IDC MarketScape

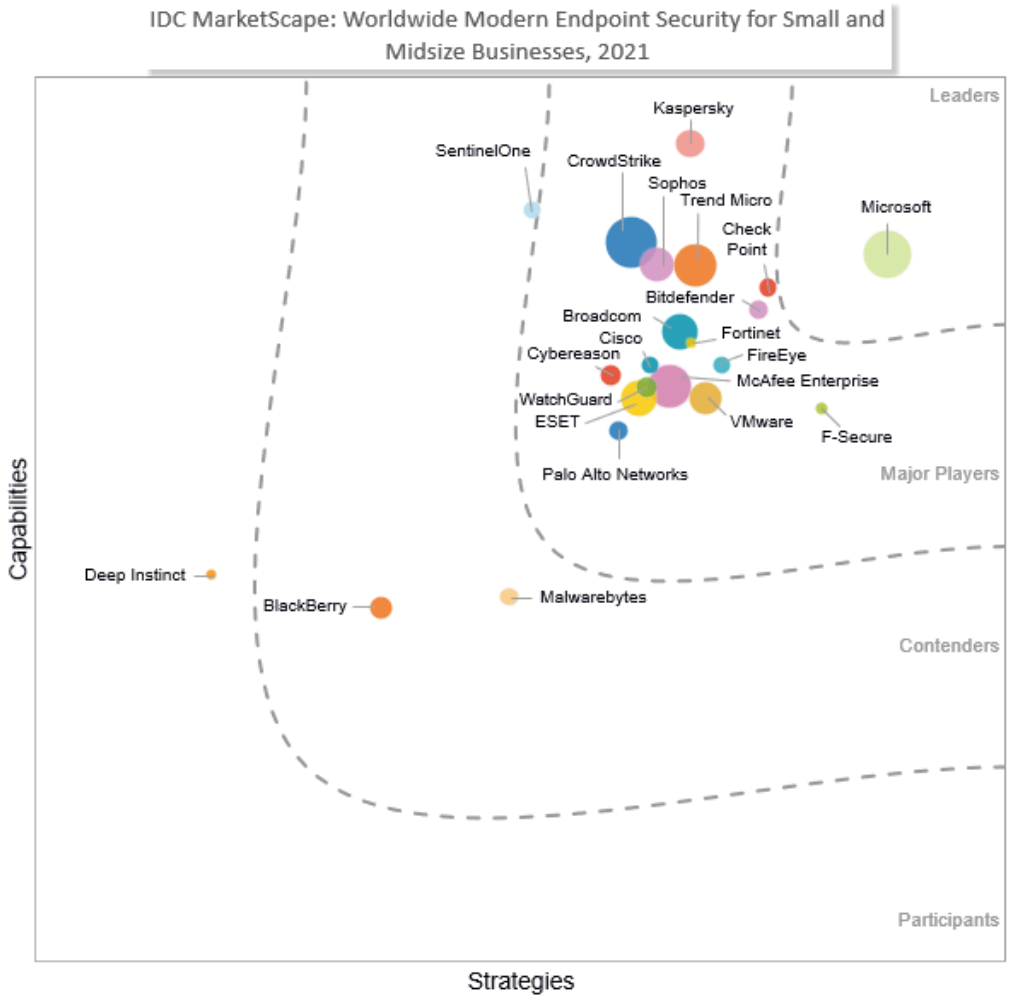
IDC MarketScape: Worldwide Modern Endpoint Security for Small and Midsize Businesses 2021 Vendor Assessment

Michael Suby

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape: Worldwide Modern Endpoint Security for Small and Midsize Businesses Vendor Assessment



Source: IDC, 2021

November 2021, IDC #US48304721

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

IDC OPINION

The endpoint security needs of small and midsize businesses (SMBs) have escalated. A decade ago, signature-based antivirus software was considered an adequate defense in identifying and removing malware from end users' devices. Times have radically changed. Threat actors no longer rely exclusively on dropping malware onto devices to carry out their attacks. Instead, they are more apt to manipulate legitimate software programs, tools, and files (i.e., living off the land attacks). Subsequently, identifying behaviors of malicious intent has become a requirement in mounting an adequate defense.

Identifying malicious behaviors, however, is no simple task. The varied, wide ranging, and complex nature of what end-user devices are equipped to do blurs the distinction between malicious and legitimate behaviors. In addition, threat actors will orchestrate a series of actions, each seemingly benign, to further disguise their presence. Assembling the trail of related actions has become essential in uncovering active attacks and then responding with speed and precision to blunt them.

While this level of attack sophistication may only seem viable when aimed at large enterprises, that is not reality. The economics of cybercrime have advanced such that SMBs are profitable targets. On the cost side, the cyberunderworld has created a marketplace of attack tools, services, and financing that in effect arm perpetrators with more capabilities for less cost.

In addition, digital transformation, while beneficial for SMBs in competing in their respective markets and serving their customers, can also contribute to SMBs' risk of being attacked. Through digital transformation, SMBs have become more digitally dependent, and this dependency spells opportunity for cybercriminals. As the rise in ransomware attacks has demonstrated, disrupting digital-dependent operations can have dire consequences to the victims and produce monetary gains for the attack perpetrators.

The endpoint footprint has changed. Spurred by the pandemic, work has also migrated from one location for many to many locations of one. Existing outside the perimeter defenses of business locations but also being online, devices used by the remote workforce and the users themselves have become more attractive as exploitable targets for cybercriminals and nation-state adversaries.

Building up endpoint security is critical. Modern endpoint security (MES) products, the combination of endpoint protection platforms (EPPs) for deterministic prevention and endpoint detection and response (EDR) for post-compromise reaction, are the latest evolution in endpoint security designed to combat threats aimed at endpoints. It is confirmed through IDC research that the demand for modern endpoint security is on the rise among SMBs.

Like enterprises, SMBs recognize that layers of complementary and compensating security technologies are essential. This is true whether the objective is to protect a location or a scattered inventory of endpoint devices. But unlike enterprises, SMBs often lack the financial and security talent resources necessary to effectively utilize layers of security technologies and engage with multiple security vendors. Simplicity without sacrificing security efficacy in thwarting today's and tomorrow's threats is what SMBs require.

The vendors included this IDC MarketScape offer modern endpoint security solutions that serve this objective.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Participating vendors met the following criteria:

- From a single endpoint software agent, the vendor's modern endpoint security product supports both endpoint protection platform and endpoint detection and response.
- End-user personal computing device platforms supported by the modern endpoint security product must, at minimum, include the latest versions of Windows and macOS.
- Vendor began selling modern endpoint security products to customers from January 2019 or earlier.
- Sales to commercial and governmental customers of EPP (also referred to as antivirus or next-generation antivirus), EDR, and modern endpoint security products must, at minimum, totaled $30 million (following generally accepted accounting principles [GAAP]) in calendar year 2020.

ADVICE FOR TECHNOLOGY BUYERS

SMBs are fortunate in that there are many capable vendors offering MES products. In addition, all vendors are actively enhancing their products. What these products deliver in the future will be more than what they deliver now. This is reassuring as threat actors will continue to advance their tradecraft and the cost and availability of security talent will remain ongoing challenges. SMBs, in essence, need and should select a vendor that can effectively adapt to a changing threat landscape while minimizing the additional time and operational duties borne by SMBs' limited security staffs. IDC offers the following advice for modern endpoint security buyers.

- **Focus first on MES fundamentals:**
  - **Protection efficacy.** IDC buyer analysis shows that SMB's top consideration in choosing a MES vendor is its research into never-before-seen threats and attack tactics. But buyers are not content with just research, they want results. There is no better result than automatically and deterministically blocking new forms of attacks. Independent evaluations on protection efficacy are useful guides in this regard but are not the panacea. IDC recommends conducting proofs of concepts (POCs). We further recommend that EPP POCs should become a routine activity. With existing vendors evolving their EPP capabilities and new vendors emerging with "next generation" approaches, comparative analysis in your environment is the best litmus test. Keep in mind that other SMBs started their search for a more effective MES product after they suffered a serious security incident. Better to avoid this circumstance by making EPP POCs a routine practice and then acting on your assessment (e.g., augmenting with another vendor's product or replacing an existing product). This practice will assist in lessening the likelihood of attacks escalating into serious security incidents and in curbing the alert and incident inflow into EDR.
  - **EDR automation.** Second on the list of buyers' vendor selection criteria is incident investigation's speed and ease. The unfortunate reality is some attacks will evade the immediate preventions of EPP and establish a footprint on endpoints. Security teams need to be prepared. But just having EDR functionality is not enough, human engagement is

required. Concentrating human engagement more on decision making and less on investigatory processes is vital in lessening threat actors' dwell time and the time required of your security personnel. Therefore, automation is essential and is present in various forms, such as assembling and cross-correlating relevant data, visualizing attack sequence, devising risk-rated responses, and executing on the chosen responses. In addition, SMBs cite automated threat hunting as a highly important factor in considering a MES vendor. Conducting a POC is the most effective means for evaluating the vendor's level of automation and usability fit with your security personnel.

    - **Device support.** MES products can only deliver EPP and EDR capabilities on endpoint device types and operating systems (OSs) that their software agents support. Obviously, you will want to confirm support for the device types and OS platforms that are in your environment. All vendors in this IDC MarketScape support recent OS versions of Windows and Mac. But Windows and Mac PCs are not the only device types attacked. Mobile devices, physical and virtual servers, and cloud workloads are also targeted. While vendors' datasheets list supported device types and OSs, IDC recommends digging deeper into feature parity and feature distinction to ensure the vendor's product is adequately equipped for all of your devices and provides unified management.

- **Examine cross-function integration.** Endpoint security and endpoint management functions are intertwined. Unpatched and out-of-date software applications and OS versions are targets of exploitation by threat actors. When exploited, EPP and EDP become the next two layers of compensating security. Logically, systematic patching reduces exploitability. However, budget for a dedicated patch management product and/or personnel to oversee patching may be lacking at your firm. An alternative that may be less costly, less administratively taxing, and can natively integrate patching into attack mitigating or remediating responses is the patch management capabilities offered by MES vendors in their solution suites. In addition, patch management is one of several functions that reduces an endpoint's attack surface and, consequently, exploitability. Other functions include device control, host firewall management, vulnerability assessment, microsegmentation, and application blacklisting, whitelisting, and process-level allow listing. In your consideration of MES vendors, comparing their collection of attack surface reduction capabilities with those of dedicated products may reveal an effective and possibly a more affordable approach to strengthening your security posture.
- **Evaluate eXtended Detection and Response (XDR) frameworks.** Reaching a complete and speedy understanding of attacks affecting endpoints may require more than telemetry gathered from endpoints running a MES software agent. Telemetry from other sources (e.g., network sensors, perimeter defenses, email and web gateways, cloud access security brokers, and identity management services) can bring in beneficial context. Many of these sources can also be control points for applying attack-mitigating responses and in refining security policies. An oversimplified description, this is the realm of extended detection and response. Nearly all vendors in this IDC MarketScape have an XDR framework that encompasses their non-endpoint security product portfolios, ecosystem partners, or a combination of both. As part of your assessment of MES products, evaluate the vendor's current state of XDR, future developments, and incremental security value and what a transition from EDR to XDR will entail (e.g., additional cost, technology upgrades, and staff training and augmentation).
- **Question ransomware defenses and recovery options.** The consequences of ransomware incidents are a top-of-mind concern for business leaders, and for good reason. According to IDC's July 2021 *Future Enterprise Resiliency and Spending Survey, Wave 6,* 75% of IT decision makers with organizations that experienced one or more ransomware incidents in the past 12 months indicated that significant extra resources beyond what internal staff handled were required to rectify. Ransomware, like other forms of malware, frequently enters business

networks through endpoint devices. Subsequently, endpoint security products, like MES, are a vital line of defense. But just as ransomware has evolved to evade detection and ultimately increased the likelihood of payment and amount of ransom payment, MES products must also evolve to detect ransomware and prevent its execution (e.g., data exfiltration and file encryption) and propagation to other endpoints and critical systems. IDC recommends that you query MES vendors about their ransomware defenses and incident recovery options for returning affected files and endpoint configurations (e.g., changes to registry keys) to their previous known good state. As you do, assess these capabilities within the context of your overall business cyber-resiliency plans.

- **Gain perspective on incorporation of built-in device security capabilities.** Worth repeating, threat actors will evolve how they conduct attacks. They will continuously probe for new avenues to enter and takeover endpoints. While not yet a mainstream avenue, attackers compromising the device's firmware is a possibility. Rather than react to this possibility once it becomes reality, ask MES vendors about their approach to confirming firmware integrity and restoration. Also ask about leveraging the device's chip-based processing features in conducting or augmenting MES functions. Eventually, the measuring stick for endpoint security solutions may entail the collaboration of built-in device security with overlay on-device security software augmented with cloud-powered features. To make security-maximized decisions on device and MES product purchases, ask MES vendors about their current and planned approaches to leverage built-in device security features.
- **Consider managed services options.** Although MES vendors have and will continue to automate and simplify the use of EDR, experienced security professionals are needed to produce maximum return on EDR's capabilities. IDC recommends that you consider the managed service options offered by MES vendors and/or their channel partners. As service needs vary by level of engagement (e.g., from on-demand collaboration to around-the-clock outsourcing) and tasks performed (e.g., threat monitoring, threat hunting, and threat response), seek a managed services arrangement that best aligns with your current needs and budget but is also flexible to adjust for changing circumstances.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Bitdefender

Bitdefender is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

Established in Romania in 2001, Bitdefender provides security solutions to businesses and consumers. A research-driven vendor, Bitdefender states that more than half of its 1,600 employees are focused on research and development (R&D). This R&D-heavy focus has contributed to the company's early incorporation of AI into its prevention stack, late 2017 introduction of EDR, a steady expansion in GravityZone features and capabilities, and high marks from customers on manageability. Although Romania based, the company competes globally, with the majority of its business segment's revenue derived from organizations based in Western Europe and North America. Although competing against much larger competitors operating with more recognizable brands, IDC estimates Bitdefender's market share in modern endpoint security materially increased in 2020.

Strengths

Bitdefender's endpoint protection capabilities are frequently tested by third-party labs. While beneficial in promoting its protection effectiveness (i.e., comprehensiveness, accuracy, and low-performance impact), this testing is also part of the company's ongoing improvement cycle. Customer references confirm Bitdefender's efficacy. Customers surveyed by IDC were very satisfied with Bitdefender's ability to detect attacks early in the attack chain and block zero-day attacks.

Preventing attacks is also part of the Bitdefender's capabilities and is included in all GravityZone versions (Business Security, Elite, and Ultra). Those capabilities include patch management, device control, application control, full disk encryption, and risk analysis. These capabilities are notable as not all vendors offer as extensive of a range of preventive capabilities and/or do not offer them fully integrated into their endpoint security product.

With ransomware attacks being a prominent concern among SMBs, Bitdefender includes Ransomware Mitigation as a product feature. Not reliant on shadow copies, Bitdefender automatically and in real time creates backup copies of user files and will restore these files after the malware has been identified and blocked from further execution.

The company's financial state is solid and at a level that has allowed Bitdefender to increase its software development talent pool, which, in turn, feeds feature and capabilities expansion.

Challenges

Bitdefender's XDR progress is not as advanced as other vendors. Many of the functional building blocks do exist (visibility, analytics, and automated response) but are not as comprehensive or mature. Nevertheless, with its track record of product expansion, we anticipate Bitdefender will be a competitive fast follower in its transformation from EDR to XDR. As for initial evidence of this, Bitdefender introduced eXtended EDR (XEDR) in July 2021 as an automatic XDR upgrade to GravityZone Ultra, Bitdefender EDR (a standalone EDR offering), and Bitdefender MDR. Key features include multisource correlation and detection, organization-level attack visualization, and automated and guided response selections. Network telemetry, collected through Bitdefender network sensors, is the initial new telemetry source included in XEDR. XEDR customers will have free use of network telemetry through the end of 2021. Starting in early 2022, network telemetry will be a fee-based (per endpoint) add-on.

Hardware integrations to monitor firmware integrity and remediate are not included in Bitdefender's modern endpoint security product. Although firmware attacks are not prevalent today, IDC's expectation is that this will change over time as attackers pursue new avenues to covertly take control of end-user devices.

Consider Bitdefender When

Bitdefender is a solid choice for SMBs that are looking for proven, comprehensive, and tightly integrated modern endpoint security that they can manage themselves. For SMBs that are new to EDR and/or lack hands-on talent, Bitdefender offers managed detection and response services. Indicative of the growing adoption of its MDR services, the company's number of MDR-dedicated personnel has been increasing.

BlackBerry

BlackBerry is positioned in the Contenders category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

BlackBerry's entrance into MES was through its February 2019 acquisition of AI-powered security vendor, Cylance. At the time of acquisition, Cylance's principal products and services were CylancePROTECT (EPP), CylanceOPTICS (EDR), CylanceGUARD (MDR), and ThreatZERO (delivery and training). Cylance also offered incident response (IR) and compromise assessment services. All these products and services have continued under the BlackBerry brand. Cylance also had a consumer product, Cylance Smart AV, that utilizes the same AI-powered engines as Protect. Even though this product remains, BlackBerry is not aggressively cultivating its presence in the consumer segment.

Commercially, the Cylance products and services are components of the broader BlackBerry Unified Endpoint Security suite. New products in this suite include BlackBerry Persona, Protect Mobile, and Gateway. BlackBerry Persona conducts continuous user authentication and assessment of network risk based on real-time monitoring of user and device dynamics. Originally offered for mobile devices, Persona has been extended to PCs with near feature parity. BlackBerry Protect Mobile was introduced in 2020 and provides mobile threat defense capabilities for smartphones and tablets. BlackBerry Gateway repurposed Cylance's AI engine to provide cloud-hosted zero trust network access. This product was introduced in 2021.

Strengths

Compared with the new vendor challenges of simultaneous funding product and market development as Cylance, the acquisition by BlackBerry opened the aperture on funding and the brand recognition associated with the larger BlackBerry.

BlackBerry is one of a small subset of MES vendors that is currently leveraging Intel's Threat Detection Technology (TDT) for malicious process detection.

Staffed internally, BlackBerry Guard is the company's MDR service. In addition to the aforementioned IR and compromise assessment services, BlackBerry has also introduced a virtual CISO service. All of these services are offered on a retainer basis.

BlackBerry has not participated in as many independent EDR evaluations as other vendors but has participated in most.

Although its consumer business is small, BlackBerry can still fold consumer telemetry into its AI engine's data pool. Not all MES vendors have a consumer business.

Challenges

BlackBerry's participation in independent EPP evaluations is considerably lower than other vendors. This circumstance is unfortunate as a principal reason for acquiring Cylance was for its signature-less, local-operating EPP. Increased participation could be an effective means to showcase the robustness of its AI-powered approach.

Similar to other vendors included in this IDC MarketScape, BlackBerry does not have a rollback remediate feature.

BlackBerry's security portfolio is exclusively for endpoints, encapsulating telemetry from multiple sources including network and user behavioral analytics. Consequently, BlackBerry is not positioned to offer native integration with other security technologies (e.g., messaging, web, cloud access, and network). Instead, BlackBerry will need to rely on a multivendor ecosystem, which it has been actively building. Where BlackBerry is positioned to provide native integration is with its unified endpoint management (UEM) products. Currently, however, it is separate product sets.

Consider BlackBerry When

BlackBerry's endpoint security strategy is to lead with a prevention-first approach, which differs from many of the other vendors in this IDC MarketScape. Although it offers EDR, it adheres to a prevention-first approach. Logically, the more reliable EPP is in automatically removing malware files and stopping malicious processes, the number of security alerts generated and security incidents are fewer. EDR remains an important security layer, but one that is less likely to be overloaded.

BlackBerry is also not approaching the market with the promise of unifying a suite of security technologies together.

BlackBerry should be considered by SMBs that prefer a best-of-breed approach in choosing vendors and products and appreciate the value of EDR but not as a counterbalance to inferior EPP. BlackBerry Persona and Gateway are distinctive products that are also worthy of consideration. While both mitigate risk emanating from users and their endpoints, operational and security synergies through integration with BlackBerry Protect and Optics (e.g., single agent and single administrative console) have not yet been put forward by the company.

Broadcom

Broadcom is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

An endpoint security vendor with a lengthy history, Broadcom's incumbency via its November 2019 acquisition of Symantec, broad feature set, and global operations has contributed to the company remaining among one of the most deployed vendors. However, customer loyalty and stability in channel partner relationships suffered following the acquisition. With a tightened focus on strategic customer relationships and targeted product development, Broadcom is transforming to become a more formidable competitor.

Strengths

Broadcom, like other well-established endpoint security vendors, has a large base of customers that use an on-premises administrative console. With the prevailing trend to cloud-based administration, Broadcom has integrated on-premises and cloud-based options to ease migration and support hybrid instances.

Embracing the principle that endpoint security should reduce the likelihood of compromise as part of prevention, Broadcom is among the top tier of vendors with a broad set of native attack surface reduction capabilities in its MES product, Symantec Endpoint Security Complete.

With the incorporation of Symantec into Broadcom and refinement in its strategic direction and narrowing of its go-to-market reach, Broadcom is in an improved position to surgically fund future MES development.

Broadcom's material market positions in email, web, cloud access, identity, and data security place the company in a favorable position to offer enterprises a natively integrated, cross-technology XDR value proposition.

Broadcom maintains one of the largest threat intelligence networks, with over 30 years of experience in categorizing and analyzing threat intelligence from a global footprint. Even though the consumer and enterprise businesses split at the time of the Broadcom acquisition, Broadcom continues to gather consumer telemetry from NortonLifeLock. Few MES vendors have the volume and diversity of endpoint telemetry as Broadcom.

Challenges

Market momentum is Broadcom's most significant challenge. As other MES vendors have been gaining market share, a portion of their gains have come at Broadcom's expense. The customer perception that forms frequently forces Broadcom into a defensive position in customer retention. With progress in working through its post-acquisition challenges, the company maintains it will regain market share.

Although its principal MES product, Symantec Endpoint Security Complete, has host-based capabilities that other vendors do not have (e.g., deception, active directory defense, network firewall, and intrusion prevention), other vendors have host-based capabilities that Symantec Endpoint Security Complete does not. Those include rollback remediation and hardware-based detection capabilities (e.g., use Intel TDT).

Consider Broadcom When

SMBs currently using older versions of Symantec's endpoint security product should consider Broadcom for its Symantec Endpoint Security Complete product. With this upgrade, SMBs gain a material expansion in relevant security features and be on the endpoint security product that will gain the concentration of Broadcom's endpoint security innovation. A recent example of this is the introduction of Adaptive Protection. Adaptive Protection provides process-level policy control in an automated fashion to Symantec Endpoint Security Complete's already extensive attack surface reduction capabilities.

Check Point

Check Point is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

Pivoting from its lengthy history in endpoint security and by aligning its product strategy with growing customer appetite for integrated product suites over independent point products, Check Point rebranded its SandBlast Agent endpoint security product as Harmony Endpoint in 2020. Harmony Endpoint Basic, the narrowest but functionally robust Harmony Endpoint package, includes antimalware, antiransomware, zero-day phishing, advanced threat prevention, and EDR. The next package size, Harmony Endpoint Advanced, augments Basic with threat emulation (sandboxing) and threat extraction (file content disarm and reconstruction). The most comprehensive package, Harmony Endpoint Complete, adds data security (full disc and media encryption) to Advanced. All technologies in Harmony Endpoint are originally designed or acquired by Check Point.

With an objective of providing customers with choice and combinability across endpoint, devices, and access, Harmony Endpoint is one product set within the broader Harmony suite. Other product sets in

the Harmony suite are Harmony Connect (Secure Access Service Edge), Harmony Browse (web gateway functionality delivered within the end user's browser via a nanoagent), Harmony Email and Productivity Suite (email and phishing security specifically for Office 365 and G Suite), and Harmony Mobile (mobile threat management).

Harmony, itself, is one of three suites in Check Point's full product portfolio of SMB and enterprise products. The other two suites are Quantum (network security) and CloudGuard (cloud security). Like Harmony, there are multiple product sets in the Quantum and CloudGuard suites. Check Point also sells an endpoint protection product named Zone Alarm, which is targeted at the consumer market.

Bringing all suites and product sets together into unified management is Infinity-Vision. Combined with access to Check Point's library of threat intelligence and equipped with similar SOC tools used by Check Point analysts, Infinity-Vision is Check Point's answer to XDR.

Strengths

With a limited number of exceptions, Check Point is in the upper tier of MES vendors in all of our comparisons. Key strengths for Check Point include:

- **Profitable.** A consistently profitable company for over 15 years, Check Point has a history of reinvestment in core security technologies, threat research, new and enhanced products, system management, and sales channel.
- **Broad and integrated product portfolio** As outlined previously, Check Point has a comprehensive and integrated portfolio of security products that the company has assembled into mix-and-match suites and product sets. From those, Check Point is well positioned to engage with customers as they seek to reduce their vendor relationships while strengthening their security readiness.
- **Distinctive MES product capabilities.** Check Point is in a limited subset of MES vendors with rollback remediation and hardware security integration features. Threat emulation and threat extraction are also distinctive MES product features.
- **Consumer business.** Check Point is active in the consumer segment through its ZoneAlarm brand. In addition to threat intelligence gathered from millions of consumer endpoints, ZoneAlarm provides Check Point with an additional segment to test its core endpoint security technologies.

Challenges

Compared with the MES vendors included this IDC MarketScape, Check Point's participation in independent product evaluations is modest. Check Point is similar to other MES vendors that have long-term customers using their non-endpoint products. As an incumbent vendor, the need to participate and promote independent product evaluations from multiple testing firms and through a variety of tests is not as great in gaining consideration of its MES product.

Check Point's range of attack surface reduction features is modest but not as expansive as a subset of MES vendors. Support for patch management is currently missing, although we are aware that Check Point is working with a third-party vendor to address this within the next year.

Consider Check Point When

While Harmony Endpoint is a viable solution for new Check Point customers, it is particularly well suited to SMBs that are already Check Point customers in non-endpoint security products and have

already become familiar in the use of Infinity-Vision. This familiarity will shorten the learning curve of an additional security product and add to cross-product benefits in visibility and policy coordination. Check Point's Harmony Endpoint is also a standalone MES product consideration due to its robust feature set and emphasis on automated protections. In making this consideration, best to weigh the implications of a separate vendor relationship and administrative console for MES versus a MES product from an existing security vendor that is intended to remain in place long term.

Cisco

Cisco is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

Not new to the endpoint security market, Cisco ramped up its game over the past few years through product enhancements and cross-product integrations. In addition, leveraging its large commercial customer base and sales channel, Cisco has become a legitimate vendor in the broader endpoint security market and specifically for organizations selecting a MES product. Based on IDC estimates, Cisco has grown slightly faster than the worldwide MES market over the past two years.

Strengths

With customer interest for cross-product integration and centralized platforms, Cisco is well positioned across its product lines at several junctures. At the agent, the software agent supporting Cisco's MES product options, Cisco Secure Endpoint Advantage and Cisco Security Endpoint Premier, also supports AnyConnect VPN, Umbrella (cloud-based DNS security), and Duo (multifactor authentication). For product administration, policy management, security operations (e.g., threat hunting), product trials, and orchestration functions, Cisco SecureX centralizes all of these functions within a single, cloud-hosted platform. SecureX's product reach is designed to encompass all Cisco security products (endpoint, network, web, email, cloud access, and identity) and Cisco infrastructure products.

A profitable company with market momentum in security, Cisco's continuing investments in Cisco Endpoint Security and its integration into a broader XDR solution set are highly probable.

Owing to and contributing to its global footprint, Cisco's local language support is among the most extensive of MES vendors.

Among MES vendors, Cisco has an extensive portfolio of attack surface reduction capabilities (vulnerability assessment, patch management, device control, and host firewall).

Supporting SMBs with staffing alternatives or augmentation, Cisco offers managed services in threat hunting, EDR, and incident response.

Not as well known, Cisco is active in the consumer segment through a free version of Cisco Secure Endpoint offered through Immunet, a malware and antivirus protection system. Over 2.2 million Immunet community members have deployed Cisco's consumer product. Incremental to Cisco Talos threat intelligence, Cisco folds in consumer telemetry in support of global outbreak control (i.e., see once and protect globally). Cisco also occasionally uses Immunet to pilot new capabilities on consumer devices.

Challenges

One of Cisco's challenges is in matching SecureX capabilities with customer expectations. Customer interviews conducted for this IDC MarketScape surfaced some disappointment in the cross-product integration and single console experience currently present in Cisco SecureX.

Cisco's participating in independent evaluations of security efficacy is modest, specifically in EPP evaluations. Cisco's participation in independent evaluations is at the low end relative to other MES vendors.

Consider Cisco When

Cisco is a distinct consideration for SMBs that want an MES product that is integrated with other security capabilities relevant for remote and hybrid workforces. With a series of feature-building packages (Cisco Secure Endpoint Essentials, Advantage, and Premier) and managed services options, Cisco provides SMBs with a logical progression. They can start with Essentials and then upgrade as their security needs warrant without changing agents or familiarizing themselves with a new administrative interface.

CrowdStrike

CrowdStrike is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

CrowdStrike has steadily expanded its prominence in the modern endpoint security market. Several factors have contributed to the company's market success. Architecturally, CrowdStrike's cloud platform, Falcon, and lightweight sensory agent have done well with enterprises that are under attack and must deploy rapidly across a large and diverse endpoint footprint. Directly related, the company's marketing tagline of stopping breaches, product packaging options that range from DIY to product-integrated managed services (e.g., managed detection and response and managed threat hunting), and its incident response and proactive services have also worked in CrowdStrike's favor in catching the attention of cybersecurity-stressed SMBs and in demonstrating value over and above their current endpoint security vendor or vendors. Also contributing to stress for SMBs is their accumulated technology and operational debt as their security technology stacks and vendor relationships have grown to unsustainable levels. Alternatively, SMBs can become stressed due to their lack of cybersecurity technology expansion. They, in essence, are underequipped to defend against sophisticated attackers. Funding and concern over the additional operational investments have restrained their technology expansions. Through a combination of platform extensibility spanning CrowdStrike modules, integrated technology partnerships, and telemetry-sharing CrowdStrike Store vendors, CrowdStrike provides multiple pathways for SMBs to reduce their technology/vendor debt or fold in overdue capabilities.

Strengths

The extensibility and hive benefits (e.g., combined and shared telemetry and cross-technology interconnectivity hub) of CrowdStrike cloud-native Falcon platform underpins CrowdStrike's strength in the modern endpoint security market and in adapting to the evolving security and IT technology needs of SMBs. Although CrowdStrike cannot claim uniqueness with a cloud-native platform, the company's early and aggressive embrace combined with managed services has produced gravitational pull for CrowdStrike among current and future strategic partners and Store vendors as it expands and deepens a CrowdStrike-centered ecosystem.

Challenges

With its market ascension, CrowdStrike is frequently considered. The resulting challenge in the highly competitive modern endpoint security market is that CrowdStrike has become a principal target for other vendors. Amid many distractions, CrowdStrike should focus on remaining steadfast in its mission, strategy, and growth initiatives, particularly as the company seeks to expand its penetration among SMBs.

IDC believes that the most significant architectural challenge for CrowdStrike is its lightweight agent. Although beneficial in deployment speed and low-performance impact, other vendors with denser agents will argue that they have an advantage in offline prevention, autonomous operation, and single-agent extensibility. In addition, separate endpoint agents still exist for some of CrowdStrike's strategic partners with solutions that utilize the endpoint as an autonomous enforcement/control point. This runs counter to SMBs' desire to reduce their number of endpoint agents. IDC contends that CrowdStrike would further improve its competitiveness by increasing the speed with which partners integrate with the CrowdStrike agent architecture.

CrowdStrike also lacks the breadth and maturity of a SMB sales channel and SMB product portfolio that have existing SMB positions in non-endpoint cybersecurity and network technologies and/or business applications.

Consider CrowdStrike When

CrowdStrike has proven to be among the go-to vendors when organizations are under attack and initial indications are that the early stage of the attack sequence involved a compromised end-user endpoint or multiple endpoints. CrowdStrike should also be under consideration as renewal dates of existing endpoint vendors is on the horizon, especially when SMB customers rank strength of a cloud-based ecosystem a critical factor.

Cybereason

Cybereason is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

With a defining focus on equipping defenders to offset cyberadversaries' advantage in stealth and complexity, Cybereason applies a data and operation-centric approach to modern endpoint security. Collecting and analyzing relevant data from Cybereason-protected endpoints in real time, Cybereason presents a comprehensive and concise view of attackers' string of operations. This string of operations Cybereason labels as malicious operations or MalOps. From this MalOps view, continuously refined through the company's behavioral-based engines and fed by Indicators of Compromise (IOCs), Indicators of Behavior (IoBs), and additional context-enhancing collections, defenders can take action to stop threats, previously seen and new, before real damage occurs. Cybereason recommended response actions are also an integral part of the end-to-end MalOp view.

Founded in 2013, Cybereason is a private company with funding of $664 million.

Strengths

Publicly demonstrating its EDR capabilities, Cybereason has been active in independent EDR evaluations.

Cybereason offers tiers of MDR, IR, and security assessment services staffed internally. Managed services are also offered through the company's channel partners.

Cybereason provides choice and flexibility in its administrative console. Customers can conduct their administrative, analytics, and policy setting duties from cloud based or on premises, or an integrated combination of the two.

Cybereason is one of the limited number of vendors that is expanding its detection reach via hardware integrations. Cybereason has partnered with Intel to use its Threat Detection Technology to detect ransomware attacks.

Cybereason's XDR prospects grew stronger with the Google partnership announcement made in October 2021. Early XDR customer wins will likely come from Google's existing customers of the company's cloud, productivity, and identity services.

Gaining momentum in the MES market, Cybereason, based on IDC estimates, has gained material worldwide market share over the past two years.

Challenges

Vendor choice in the SMB segment is diverse with new-age endpoint security vendors such as Cybereason, established endpoint security vendors, and vendors for whom endpoint security is one of many security products they offer. A principal challenge for Cybereason in competing for SMBs is positioning itself favorably against multiproduct vendors. Their existing customer and sales channel relationships and cross-product integration and packaging will be a barrier to overcome. This barrier, however, has the potential to evaporate with existing Google customers. Google's services become Cybereason's multiproduct advantage, with Cybereason prevention and detection capabilities spanning Google services.

Unlike more tenured security vendors that can cycle profits into development, Cybereason's ability to fund product development, expand geographically, and grow sales and customer support is dependent on the company's ability to attract external funding. So far, the company has been successful in attracting funding: $275 million in cross-over funding in July 2021 and an undisclosed amount of funding from Google as part of the October 2021 Google–Cybereason partnership announcement.

Emphasizing early detection and response with its MES solution, Cybereason does not offer similar rollback remediation capabilities as some of the other vendors.

Consider Cybereason When

Cybereason is a consideration for SMBs that prioritize best of breed in their selection of MES. And in keeping with Cybereason's focus on equipping defenders to operate at higher levels of productivity and proficiency, Cybereason is also a good, shortlist consideration for SMBs that view EDR as essential to their endpoint security arsenal and have already tired EDR from another vendor and are dissatisfied with the results in terms of operational overhead and ability to confidently detect threats early in the attack sequence.

Deep Instinct

Deep Instinct is positioned in the Participants category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

Founded in 2015, Deep Instinct is approaching the MES market with a new approach to an old challenge. That challenge is detecting and preventing zero-day attacks with comprehensiveness, accuracy, and speed. The common approach to this challenge by MES vendors has two parts: periodically upgrade their automated EPP detect and block mechanisms and augment EPP with EDR to detect and respond to the attacks that were not detected and blocked by EPP and complete the response before tangible harm has occurred.

The limitation with this two-part approach is adversaries gain the benefit of time. Since their exploits were not detected and blocked in real time by EPP, time passes as security personnel equipped with EDR assemble threat artifacts to reach a verdict on what happened, where, how, and when. Then, unless there is an automated process to remediate and recover, these steps consume additional time.

Deep Instinct's approach is to lessen this challenge by using AI-based deep learning to predict threats and prevent their operation at the pre-execution stage and minimize the burden on EDR by reducing the overall number of alerts. Expressing confidence in its technology, the company backs its claims with a pair of warranties underwritten by Munich Re: a $3 million warranty against damage from a ransomware attack and, potentially an industry first, a false-positive warranty that pays out when the false-positive rate exceeds 0.1% over a defined period. The company also states its pre-execution prevention on known and unknown malware on files, scripts, and macros occurs in less than 20ms, with a prevention rate for never-before-seen attacks of over 99%. Updates to its prevention engine are only required one to two times per year. Deep Instinct integrates with other security solutions such as EDR, SIEM, and SOAR via REST API; syslog; and SMTP to improve the overall efficiency of the entire security stack.

Strengths

A purpose-built deep learning framework applied to cybersecurity, adversarial AI protection, and prevention capabilities is tied to its prediction engine.

Deep Instinct's offers depth of prevention with multiple layers of static analysis for file- and script-based attacks and dynamic, behavioral, and reputational analysis to prevent fileless code injection attacks and other advanced attacks such as adversarial AI.

As previously noted, update frequency to maintain maximum security efficacy of Deep Instinct's prediction engine (i.e., Deep Instinct Brain) is low, only 1-2 times per year. Following a design principle concentrated on autonomous operation, Deep Instinct states that the efficacy of its prediction engine is nearly equal between connected and disconnected devices.

The company has secured private investment of over $240 million to fund product development and its go-to-market initiatives. Noteworthy in its go-to-market approach is a shift to 100% channel, an approach that has been successfully used by other MES security vendors in their efforts to build scale and reach profitability.

Deep Instinct offers extensive OS support for endpoint device platforms including Windows, macOS, Linux, iOS, and Android.

Support for agentless use cases is also present, particularly in preventing malware propagation. Relevant use cases include scanning in-transit files for web gateways, cloud storage, and custom-built applications. Deep Instinct functions as an inline malware filter preventing malicious files containing known or unknown malware from downloading from a web gateway or uploading to or downloading

from cloud storage (e.g., AWS S3, Azure Blob, and Google Cloud Storage) and preventing malicious files from uploading to or downloading from custom applications and workflows.

Challenges

Deep Instinct's principal challenge is in gaining mindshare in a crowded and highly competitive market. Adding to this challenge is the battle in convincing prospective customers that the company's technology is materially different from other vendors' prevention technologies and unlikely to be replicated. Countering this challenge is a very high renewal rate among Deep Instinct customers. Note that this is self-reported and on a small customer base relative to many of the other vendors included in this IDC MarketScape.

While Deep Instinct historically has had very low participation in independent EDR and EPP evaluations, circumstances are changing. The company recently completed a SE Labs test, expects to be incorporated into VirusTotal, and will complete the current MITRE ATT&CK Evaluation by the end of the year. Of note, independent evaluations do have inherent limitations in testing for a vendor's detection of zero-days and never-before-seen attacks. Consequently, Deep Instinct and other vendors with detection engines designed to prevent the unknown cannot be fully evaluated.

Like other vendors with private investment funding, Deep Instinct does not have the same latitude as vendors with profitable operations to organically fund their growth initiatives. Deep Instinct is also disadvantaged relative to other MES vendors that have multiple security product categories that they can natively integrate and package together.

Consider Deep Instinct When

As threat actors constantly change and advance their tactics, such as weaponizing machine learning to circumvent endpoint security defenses, SMBs should periodically examine promising alternatives. Deep Instinct should be considered a promising alternative. Examining alternatives and switching out an incumbent vendor's product, however, are not effort-free tasks. Nevertheless, the potential of suffering through a business-disrupting ransomware attack is a very good reason to reexamine. Another logical time to examine alternatives is when debating the upgrade from EPP only to a MES product.

ESET

ESET is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

Approaching 35 years since its founding and serving both the corporate/commercial and consumer segments, ESET is among the most tenured vendors included in this IDC MarketScape. From its origins in Europe, the company has diversified geographically, and its commercial customer base is evenly spread across sub-100 endpoint companies to firms with thousands of endpoints. Constant throughout its history is a research and technology-driven culture and stable leadership.

Strengths

A private company, ESET is profitable and reinvests its profits into the disciplines that directly contribute to advancing its products, namely, software development, core threat research, and threat hunting.

Tailoring the company's support of its expansive base of customers across western, central, and eastern Europe, ESET engages with its customers in the prevalent languages of their countries. Local language support, either directly or through partners, applies to the other regions where ESET has a material presence, namely, North America, Japan, and Latin America.

Willing to put its endpoint security products to the test, ESET's participation in independent EPP evaluations is among the upper tier of vendors. With its EDR capabilities introduced in 2018 via ESET Enterprise Inspector, ESET's participation in EDR evaluations did not start as early as other vendors, but the company has since been highly participatory in EDR evaluations involving multiple testing firms.

With a security product portfolio that includes email, cloud-hosted business apps, cloud access, data, and identity, ESET has a solid position relative to other vendors to offer a broad and natively integrated cross-product platform solution.

Assisting customers in overcoming their skill gaps, ESET with its in-house talent and through its partners offers MDR and managed threat hunting services.

As previously stated, ESET offers security to the consumer segment. As with other vendors that are active in the consumer segment, ESET benefits from the unique threat data it collects and analyzes.

Challenges

There are just a few capability areas where ESET is lacking. ESET does not have rollback remediation features, for example, to return ransomware-compromised user files and settings to preattack state. The company's focus, however, has been noticeably present in ransomware prevention through a pair of ESET-developed technologies: Network Attack Protection and Ransomware Shield. ESET is also limited in its hardware-based security capabilities. Not the same as hardware based but related in protections below the application layer is preboot monitoring. In that regard, ESET added UEFI scanning as a standard feature. Its UEFI Scanner scans for threats that could launch prior to a device booting up.

ESET's set of capabilities directed toward attack surface reduction are not as expansive as some other vendors in this market. ESET offers device control and host firewall management natively within its product. Vulnerability assessment and patch management are currently not part of ESET's solution set, either natively or through third-party integrations.

Although ESET's MES business is steadily growing, on a worldwide basis, ESET's growth trails the overall market. The risk to ESET is larger worldwide vendors crowding out ESET in POC invitations.

Consider ESET When

Existing ESET endpoint security customers should trial ESET's EDR capabilities and consider upcoming road map functionality. ESET's long history of feature expansion will likely narrow potential differences between the company's capabilities and those of competitors and, conversely, ESET is also apt to have capabilities that other vendors do not. In addition, ESET, as previously stated, has security products in other disciplines that provide useful telemetry for threat detection and represent additional control points for policy enforcement (preventive and reactive). This is beneficial for enterprises that want to unify their security stack with fewer vendors and are also comfortable with separate vendors for vulnerability assessment and patch management. In evaluating unification, do pay attention to centralized management and its contribution to improving security staff's productivity.

The administrator and analyst experience and actual cross-product integration versus claimed integration matter. In addition, compare ESET's partner ecosystem with your multivendor environment to ensure cross-vendor telemetry exchange and response orchestration meets your requirements.

FireEye

FireEye is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

FireEye, the company, is on the verge of a transitional split. Announced earlier this year, Symphony Technology Group (STG) will be acquiring the FireEye products portion of FireEye, with the close anticipated for later this year. The Mandiant services portion of FireEye will become a standalone entity. In July 2021, STG acquired McAfee's enterprise business. For the purposes of this IDC MarketScape, strengths and challenges are based on current FireEye. Given the gravity of the FireEye product acquisition by STG and the potential modern endpoint security product optimization with McAfee, the Consider FireEye When section includes IDC's opinion on the combined FireEye and McAfee.

Strengths

Attack surface reduction (i.e., vulnerability management, patch management, device control, and host firewall management) is a strength of FireEye. The company is in the upper tier of vendors with natively integrated capabilities.

Not present among all vendors, FireEye offers on-premises and cloud-based options for its administrative console, and the two are integrated. Integration helps alleviate time, effort, and potential missteps for organizations in their migration from on premises to cloud or in maintaining hybrid administration.

Intentionally, Mandiant MDR services were designed to leverage FireEye's products. As with other vendors that support MDR with in-house talent and in-house product, FireEye has a direct feedback loop on feature refinements and additions from the Mandiant services team in its real-world product usage.

Another avenue for gaining constructive feedback on its EDR capabilities, FireEye has participated in all MITRE Engenuity Evaluations.

With a product portfolio that spans network, messaging, and endpoint security, FireEye has a good vantage point from which to build a natively cohesive, multi-technology XDR solution. Missing in FireEye's product set is cloud security gateway (i.e., cloud access security broker) and identity management.

Challenges

FireEye's current lack of support for mobile device platforms (i.e., iOS and Android) is a notable gap in the company's modern endpoint security product.

Also, rollback remediation capabilities, beneficial in recovery from ransomware attacks and in removing lingering artifacts from other attacks, are not as advanced as other vendors. FireEye customers, however, do have options. If the customer has established procedures for backing up files locally or into cloud storage, Helix playbooks can be triggered to restore files. Scripting is another option for conducting remote recovery actions. Exclusively focused on the commercial/corporate

market segment, FireEye is not a recipient of threat intelligence nor has the means to evaluate its product's effectiveness on devices owned and operated by consumers. Other vendors in this market do. Nevertheless, FireEye has an indirect approach to improve its security efficacy through consumer engagements. That approach is by licensing Bitdefender's malware protection engine. As Bitdefender updates its engine for consumer threat observations, FireEye's corporate customers also benefit.

Consider FireEye When

FireEye entered modern endpoint security with EDR and then incrementally built out its EPP capabilities. That strategy has worked for the company as FireEye has been growing on par with the worldwide modern endpoint security market over the past two years. As for FireEye as a good fit for SMBs, IDC contends the best fit is with SMBs that maintain a SOC and want capabilities that align well with the operational needs of SOC analysts. Following the acquisition by STG and the melding of modern endpoint security capabilities with McAfee, our recommendation is to look for post-acquisition product announcements that convey EDR ease of use and a high level of EPP efficacy.

F-Secure

F-Secure is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

F-Secure is one of the smaller vendors included in this IDC MarketScape. Based on IDC estimation, F-Secure's market share in the worldwide modern endpoint security market is less than 1%. This 1% on a worldwide basis, however, masks the company's business concentration in western, central, and eastern Europe and SMB-tailored solution set, which accounts for over 100,000 customers. In addition, the company has a material and growing business in the consumer segment that adds an element of strength.

Strengths

A principal strength of F-Secure in the modern endpoint security market for SMBs is its holistic solution set. Easing vendor, administrative, and agent sprawl for SMBs, F-Secure's solution set includes context-based vulnerability management and patch management. Extending its core capabilities in endpoint protection for prominent cloud applications, F-Secure adds a complementary layer of security to the native security features of Office 365 and Salesforce.

F-Secure also offers managed detection and response and threat hunting. A 24 x 7 operation conducted from three geographically separate locations, F-Secure's threat hunters drive new discoveries, which form new automated detections and protections in its EDR and EPP, respectively. Through the company's "Elevate to F-Service," customers can engage directly with F-Secure's threat hunters.

F-Secure's recently introduced usage-based security subscriptions further illustrate the company's alignment with SMBs needs. SMBs with variable or seasonal endpoint security requirements may reduce their security costs as they are charged based on actual device usage rather than a fee structure based on a fixed number of registered devices.

F-Secure is also thoroughly tested by third parties. In our assessment of vendor testing, F-Secure is in the highest tier based on number of testers it is evaluated by, variety of tests conducted, and testing frequency. Unequipped to run in-house tests, SMBs benefit from a collection of independent tests.

Representing 45% of its total business, F-Secure's consumer segment is a rich source of threat telemetry. In addition, F-Secure's success in the consumer segment is a testament to its attention to the multiple aspects of execution that contribute to channel partner success. This experience and know-how have a parallel in the SMB segment where channel partners are a prominent means to market.

Finally, the company is profitable. This provides SMBs a measure of assurance that F-Secure's investments in product upgrades and new product introductions will not waiver in the future.

Challenges

In a market in which scale matters, F-Secure's small overall market size and its European concentration limit buyer awareness of the company in the larger North America market and F-Secure's growth and, therefore, scale-altering prospects.

The company's platform support is not as extensive as other vendors. While it supports Windows, macOS, Android, iOS, and Linux, support for older versions of Windows, macOS, and iOS lags other vendors. Pertaining to feature parity, F-Secure maintains feature parity across all the platforms and their versions it supports. Conversely, Microsoft, as an example, favors its Windows 10 operating system in feature depth.

Consider F-Secure When

F-Secure should be a strong consideration for SMBs that want a holistic solution set, are reluctant to rely solely on Microsoft for security, or face the prospect of a higher-tier licensing agreement and their platforms run recent OS versions. F-Secure MDR and 24 x 7 on-demand services add appeal to resource-constrained SMBs that want around-the-clock, enterprise-grade security operations.

Fortinet

Fortinet is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

Fortinet entered the endpoint security market in a meaningful manner with a next-generation antivirus product in early 2017. Two and half years later in October 2019, Fortinet entered the MES market with the acquisition of enSilo. Also in 2019, Fortinet added pre-execution prevention through integration with FortiSandbox and added application discovery, assessment, and virtual patching to its endpoint security feature set. Fortinet's MES product is FortiEDR.

Strengths

A globally operating and mature security vendor, Fortinet is a profitable entity. The company has parlayed this profitability into expanding its security portfolio into MES and other security disciplines via organic development and acquisition. With its internal funding source and demonstrated intent to deepen its MES market presence, Fortinet is solidly positioned to compete in a MES capabilities arms race and equip its extensive channel partnership to market and support FortiEDR.

Fortinet's broad security portfolio and investments in cross-product integration (i.e., via Fortinet Security Fabric) and XDR (FortiXDR) enable Fortinet with a strong foundation in serving customer objectives in vendor consolidation and in maturing from EDR to XDR. FortiEDR is currently integrated with FortiGate, FortiNAC, and a host of third-party vendors in support of intelligence sharing and

coordinated responses, with FortiSandbox for real-time file assessment and with FortiSIEM in support of security operations.

FortiEDR features and capabilities are comparable with those of much larger MES vendors. Its range of device support and administration flexibility (on premises, cloud, and hybrid) are among the top.

Fortinet's ransomware rollback approach occurs in real time. Upon detecting attempted file access and write operations, FortiEDR redirects those operations to a copy of targeted files efficiently created in a mirror memory location. If post-operation is determined to be safe, the operations are permitted on original files, otherwise the operations are blocked on the file copy.

Supporting channel partners and customers globally, Fortinet's local language support is extensive.

MDR is available through Fortinet personnel and through an increasing number of certified channel partners.

Challenges

Fortinet's demonstration of the company's EPP and EDR functionality and performance through independent evaluations is limited relative to the rest of the market. Increasing its participation would benefit Fortinet in bolstering its creditability, especially among non-Fortinet customers.

Fortinet's attack surface reduction capabilities are modest. Missing from its capabilities is patch management. Fortinet does mitigate system and application vulnerabilities via virtual patching. Having native patch management would provide customers with flexibility in choosing how to mitigate vulnerabilities and automate the workflow from virtual patching to actual patch deployments.

Consider Fortinet When

Fortinet is a natural consideration for existing Fortinet customers. Given Fortinet's product-development history, future and deeper integrations with other Fortinet products and feature enhancements to FortiEDR should be expected. Greater availability of partner-led MDR services will also follow.

Kaspersky

Kaspersky is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

A prominent security vendor operating worldwide, Kaspersky has expanded its security product suite beyond its endpoint security roots. Its current product suite includes inline security for the common threat vectors of email and web. The company also offers security products for ICS, IoT, and network attached storage and offers fraud prevention. Kaspersky is not solely products, it has an expanding suite of services spanning assessment, training, threat intelligence, incident response, and detection and response. Focused on cross-product and service integration and reuse of a common technology base, Kaspersky's approach to new product introduction, feature expansion, and service process design and staffing is from within rather than through acquisitions.

Strengths

Capabilities of Kaspersky's modern endpoint security product are very competitive with no material deficiencies.

The company is among the most tested for EPP capabilities.

With its expanding and internally developed product suite, the company is well positioned to offer SMBs a natively integrated cross-product solution.

Kaspersky also offers a comprehensive set of attack surface reduction management functions natively integrated into its MES product (vulnerability, patch, device, and host firewall) and administrative console.

Platform support is expansive and includes cloud workloads. On personal computing device, the only gap is lack of support for Chromebooks. However, Kaspersky is not alone, only a small subset of MES vendors currently support Chromebooks.

Kaspersky offers a range of endpoint security products distinguished by different feature sets and not all meeting IDC's strict definition of MES. Nevertheless, with double-digit annual customer growth with its non-MES products, Kaspersky is building a strong pipeline of upgradable customers to its MES products.

Representing an additional and real-time source of threat intelligence, Kaspersky is a major provider of digital life protection products for consumers.

Kaspersky leverages its profitable operations to fuel product expansion and enhancement.

Challenges

Missing from Kaspersky's product portfolio is cloud security gateway (Cloud Access Security Broker). Consequently, SMBs that rely on this gateway as one of their security policy control points must engage with another vendor's product.

A subset of vendors utilizes Intel's Threat Detection Technology for firmware integrity monitoring; Kaspersky does not. It contends its technology delivers similar if not better security benefits.

With a customer footprint concentrated in EMEA, LATAM, and APAC, Kaspersky is at a disadvantage to larger vendors with greater U.S. presence in catering to United States-based SMBs.

Consider Kaspersky When

SMBs dissatisfied with the security efficacy of their current EPP product and are looking to step up their endpoint security capabilities into EDR and reduce their number of standalone products (e.g., vulnerability and patch management), Kaspersky is a solid contender. In addition, Kaspersky's managed detection and response service and tiered packaging allow SMBs to strengthen their security operations without needing to change or add vendors.

Malwarebytes

Malwarebytes is positioned in the Contenders category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

Building off its remediation technology, Malwarebytes introduced its MES solution (Malwarebytes Protection and Malwarebytes Endpoint Detection and Response for PCs and servers) in mid-2017. With this introduction, Malwarebytes gains new MES customers in two motions. One motion is as an endpoint security product replacement following a security incident. In this motion, Malwarebytes is

initially deployed to locate and remove all attack artifacts on compromised endpoints. Following this, Malwarebytes becomes the SMB's principal MES product. The second motion is part of a SMB's cybersecurity planning process, and Malwarebytes is chosen over other vendor's products.

Strengths

Malwarebytes is a profitable private company. This has allowed the company to internally fund feature enhancements and new product introductions and expand its go-to-market initiatives.

The same core technologies that have contributed to its remediation capabilities are used to support rollback remediation. A safety valve, Malwarebytes' rollback remediation returns user files and settings to their preattack state.

Demonstrating its EDR capabilities in a public forum, Malwarebytes has been an active participant in independent EDR evaluations over the last two years.

Providing customers choice and flexibility, Malwarebytes offers on-premises and cloud-hosted administration that are integrated together to facilitate migration (e.g., on premises to cloud hosted) and hybrid situations.

Malwarebytes is growing at the market pace. This is noteworthy as Malwarebytes' MES product features and product suite are not as broad as vendors Malwarebytes is competing against. In addition, many of the vendors in the SMB segment have an existing customer base in non-endpoint security products from which they can sell into. The fact that Malwarebytes is growing at the market pace, given these limitations, is a testament to a product that consistently delivers on its principal objectives and, as cited by customers IDC interviewed, superior customer support.

Malwarebytes also operates in the consumer segment. This segment provides Malwarebytes with an additional source of threat telemetry that it can recycle into improving the security efficacy of its business endpoint security products.

Challenges

As previously stated, Malwarebytes' MES product features and product suite are not very broad. This situation limits Malwarebytes long-term market potential among SMBs that rate vendor consolidation and an XDR strategy as important criteria in choosing a MES vendor. The company is working to improve its competitiveness. Malwarebytes is expanding its product portfolio to meet the changing needs of the market and has brought on top talent to lead the company's transformation.

At the time of writing of this document, product features Malwarebytes lack are mobile device support, hardware-based security integrations, breadth in attack surface reduction capabilities (i.e., vulnerability assessment, patch management, and device control), and a MDR service. IDC anticipates that this situation is changing.

In other gaps relative to other MES vendors, Malwarebytes does not offer security products beyond endpoint security. This limits the company's product bundling options and foundation to create cross-product-native integrations. As SMBs expect additional sources of telemetry to bolster detection of multivector attacks and choice in control points to affect security response, Malwarebytes will be reliant on other vendors' APIs. This situation places Malwarebytes at a disadvantage to vendors with products that span multiple security disciplines (e.g., web security, email security, firewalls, cloud access, and identity management).

Consider Malwarebytes When

Malwarebytes is a consideration for SMBs that have grown frustrated with the diminishing level of security efficacy of their current EPP products and have heightened concerns about the business-debilitating effects of ransomware attacks. Moreover, since Malwarebytes' rollback remediation operates locally on end-user devices, Malwarebytes appeals to SMBs that have a remote workforce and do not have a SOC. The alternative of reimaging a ransomware-attacked remote endpoint versus local rollback causes remote information workers to be partially or fully out of commission for multiple consecutive days or longer. Malwarebytes has also gained a sizable customer adoption among state and local government agencies.

McAfee Enterprise

McAfee Enterprise is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

McAfee Enterprise business as of July 2021 became part of STG. Anticipated later this year, STG will complete its acquisition of FireEye's product group. With both McAfee Enterprise business and FireEye products under the same ownership, IDC anticipates the one-time direct competitors will combine forces and deliver a modern endpoint security product suite that blends the best of both companies' current capabilities and those in near-term development. Under this context, the Strengths and Challenges sections focus exclusively on current McAfee and the Consider McAfee Enterprise When section includes IDC's opinion on the combined FireEye and McAfee Enterprise.

Strengths

A flagship brand over decades in endpoint security, McAfee Enterprise has one of the largest bases of EPP customers. Having this large EPP customer base to upgrade to a modern endpoint security is a competitive advantage for McAfee Enterprise versus newer vendors that must build a modern endpoint security customer base from scratch. McAfee's proactive threat intelligence capabilities, delivered by MVISION Insights, provide early warning signals on threat campaigns and emerging threats. In addition, with a security product portfolio that includes XDR, actionable threat intelligence, cloud security gateway, cloud workload security, network sandboxing, web content security, IDS/IPS, and DLP, McAfee has a strategic and product bundling advantage over single-product vendors. Crossing across its entire product portfolio, McAfee's Advanced Threat Research team is a key source of intelligence.

McAfee Enterprise has put its EDR capabilities on public display. The company has participated in all MITRE Engenuity Evaluations.

In recovery of local files encrypted in a ransomware attack, the company's rollback remediation is a distinctive capability.

McAfee Advanced Threat Research team is a key source of intelligence in supporting the company's entire product portfolio. Although not part of STG's acquisition of McAfee Enterprise, McAfee's massive consumer business has been a source of threat intelligence for McAfee Enterprise in support of its business endpoint security products. IDC anticipates that intelligence sharing will continue over the foreseeable future between McAfee Enterprise and McAfee consumer business.

As previously mentioned, McAfee Enterprise has a security products portfolio that spans network, messaging, data protection, and cloud services access. Native integration across its portfolio is a strength for McAfee in its competitive XDR approach.

Challenges

Although its lengthy tenure and large customer base are strengths for McAfee Enterprise, the company has nevertheless been susceptible to competitive inroads. IDC's market analysis shows McAfee's worldwide market share in modern endpoint security is trending downward. Contributing to this market share decline is loss of nonstrategic accounts, such as customer accounts that have not upgraded from older versions of McAfee Endpoint Security (ENS). These account departures should diminish as McAfee Enterprise states 80% of its current customers have deployed the current, more advanced version of ENS. In addition, customer wins and upgrades to MVISION EDR are also countering customer departures.

McAfee Enterprise is among the top tier of vendors in its participation in independent EDR evaluations. Conversely, McAfee Enterprise's participation in EPP evaluations relative to other vendors included in this IDC MarketScape is not as extensive.

Consider McAfee Enterprise When

SMBs need EPP to conduct the function it was designed to do: automatically block the maximum number of attacks that begin at endpoints with the highest level of confidence. Layering on EDR or MDR as a compensating control, while an option, is a questionable endpoint security strategy. With this thought in mind, IDC's recommendation for McAfee Enterprise's existing SMB customers is to pay close attention to product announcements that follow STG's acquisition of FireEye. Tune into realistic announcements that speak to improvements in EPP efficacy and automated attack surface reduction.

Microsoft

Microsoft is positioned in the Leaders category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

With Windows, the most prevalent end-user device operating system, Microsoft has an inherent vantage point no other modern endpoint security vendor can match. And the company has leveraged this vantage point to its advantage. The company has its endpoint security capabilities from hardware (via chip and device manufacturer partnerships) up through the application layer. Within its modern endpoint security solution, the combination of Microsoft Defender Antivirus and Microsoft Defender for Endpoint, Microsoft employs a hybrid local and cloud architecture to maximize its range, speed, and accuracy across all stages of endpoint security: prevention, protection, and post-compromise detection and response.

Strengths

Microsoft's strategic vantage point is more than its Windows operating system. Directory service of Active Directory, web browser of Microsoft Edge, and the ubiquitous business productivity apps of Office 365 provide Microsoft native visibility and control across common endpoint attack vectors. These security building blocks available through Microsoft licensing agreements (E3 and E5) and as standalone options have contributed to Microsoft's market strength and momentum in modern endpoint security.

For many organizations, security products are no longer sufficient. They need on-call talent to assist in exercising threat intelligence and conducting threat hunting. Through its licensing agreements, Microsoft offers services to assist customers in their security functions.

Microsoft's momentum in the modern endpoint security market is undeniable and that lends to more customers considering and trialing Microsoft Defender Antivirus and Microsoft Defender for Endpoints. Based on IDC's estimates, Microsoft's market share has increased by 8 percentage points from 2018 to 2020 in the high-growth modern endpoint security market. Over this same two-year period, the worldwide modern endpoint security market expanded by 32%.

As telemetry is the rocket fuel for AI- and ML-infused endpoint security solutions, Microsoft's breadth and volume are unequalled geographically and across customer segments (enterprise, small and midsize businesses, and consumer). With the support of macOS, iOS, and Android, Microsoft's telemetry pool is expanding and diversifying. Microsoft's expanded platform support also chips away at the long-standing advantage of endpoint security ISVs.

Challenges

The most prominent challenge Microsoft faces is customer reluctance to extend its Microsoft software dependency into security. While Microsoft has been gaining customer converts in modern endpoint security and in other security technologies, customer interviews conducted in support of this IDC MarketScape confirm there are security decision makers that are solidly opposed to using Microsoft. They will continue to use an ISV as their principal means for protecting their endpoints.

Manageability is also an area Microsoft needs to improve upon. Also cited by security decision makers, manageability across Microsoft's security portfolio has not kept pace with its expansiveness. For SMBs, however, the recently announced public preview of Microsoft Defender for Endpoint Plan 1 holds promise in reducing management complexity.

Cross-platform support in endpoint security is a recent development for Microsoft. Consequently, functional parity remains a gap and one that plays to ISVs' advantage. Nevertheless, IDC anticipates that Microsoft will make progress in cross-platform parity.

Consider Microsoft When

Microsoft Defender Antivirus and Microsoft Defender for Endpoint (current and Plan 1 in the future) should be a consideration for SMBs that have a concentration of Windows endpoints and view Microsoft licensing agreements favorably. SMBs that have a diverse set of platforms or are concerned about manageability pause for now but revisit when Microsoft Defender for Endpoint Plan 1 enters generally availability and Microsoft announces additional strides in cross-platform parity.

Palo Alto Networks

Palo Alto Networks is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

Pivoting from its success in next-generation network security and with ambition to radically improve cybersecurity practices through comprehensive visibility and cross-technology integration, Palo Alto Networks approached the MES market with holistic intent. Rather than principally compete in endpoint security, Palo Alto Networks positions its EPP and MES products, Cortex XDR Prevent and Cortex XDR Pro, respectively, as stepping-stones to XDR. Starting early and continuing, the company's

aggressive pace of technology acquisitions and enhancements in its Cortex security operations platform are demonstrations of the company's all-in XDR focus.

Strengths

Palo Alto Networks welcomes the opportunity to put its EDR capabilities on public display. It has extensively participated in independent EDR evaluations.

Reflecting the diverse platforms of its customers, Palo Alto Networks is in the upper tier of vendors in device platforms supported and in-synch compatibility with new OS releases.

Investing in high-skill talent, Palo Alto Networks supports customers with managed threat hunting and incident response services through its Unit 42 organization and incident response services through its Crypsis unit. MDR is offered to customers through partners, and Palo Alto Networks' MDR partners have expanded from 5 in 2019 to currently 42.

Palo Alto Networks' security product portfolio is extensive, spanning endpoints, cloud instances, network, web, cloud access, and security analytics. This product range contributes to Palo Alto Networks' foundation in building a comprehensive, natively integrated XDR solution.

Challenges

Relative to a subset of vendors in the MES market, Palo Alto Networks does not have hardware-based threat monitoring (e.g., the use of Intel TDT) and rollback remediation as product features. However, Palo Alto Networks does automatically provide remediation suggestions, such as allowing analysts to restore damaged or deleted files and registry keys with a single click.

Missing opportunities to test and promote its EPP effectiveness, Palo Alto Network's participation in independent EPP evaluations is less than other vendors.

With a singular focus on addressing the cybersecurity needs of businesses and governmental agencies, absent from Palo Alto Networks' collective threat intelligence is telemetry from the consumer segment, which a subset of other endpoint security vendors has. Conversely, Palo Alto Networks has telemetry other vendors may not, for example, outside-in visibility on internet-exposed assets, which the company recently gained through its 2021 acquisition of Expanse. In addition, Palo Alto Networks gathers threat intelligence from the cloud-delivered Palo Alto Networks WildFire malware prevention service. This service has over 35,000 enterprise customers and has analyzed over 16 billion unique malware samples.

Consider Palo Alto Networks When

Palo Alto Networks' Cortex XDR Pro is most applicable to SMBs that view EDR as a starting point in fulfilling on an XDR strategy and prefer a software suite approach to building out their cybersecurity technology stack in support of XDR.

SentinelOne

SentinelOne is positioned in the Contenders category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

Founded in 2013, SentinelOne's initial offering of next-generation antivirus occurred in 2017, followed the next year with the launch of its managed detection and response service. A useful training ground,

feedback gained in use of its EPP and EDR capabilities by its MDR team were incorporated into the product launch of ActiveEDR in 2019. This MDR-to-product improvement cycle remains in place today. Joining the multiuse platform trend, SentinelOne's Singularity Platform was introduced in late 2019. Prepping for the transformation of EDR to XDR, SentinelOne acquired Scalyr in 2021 for its cloud-based data analytics platform.

Strengths

Among SentinelOne's principal strengths is the company's third-party evaluations of both its EPP and EDR capabilities. SentinelOne is among the top tier of vendors that has subjected its products to as many independent evaluations.

SentinelOne has proven the applicability of its agent with its range of device platforms supported and responsiveness to new OS versions is also among the top tier of vendors.

Since the company's pre-EDR entry into MDR, SentinelOne has expanded its menu of managed and professional threat mitigation and response services and tools and represents another SentinelOne strength in meeting customers' evolving needs with a mix of product and services. Also noteworthy is SentinelOne's remote script orchestration tool. SentinelOne's incident response partners utilize this "power tool" in serving SMBs to conduct forensics, rapidly contain attacks, and manage configurations at scale.

An effective local endpoint recovery feature following a ransomware attack, SentinelOne's base product includes file and configuration rollback capabilities.

As expected with a relatively young security software company and one that recently bolstered its balance sheet through an IPO, growing its software development talent is integral to its growth strategy.

As the market as a proof point, SentinelOne has steadily gained MES market share.

Challenges

Compared with security vendors with broader product portfolios spanning security disciplines in email, web, network, cloud access, and identity, SentinelOne's product portfolio is centered on endpoint. This places SentinelOne at a disadvantage relative to vendors that can demonstrate operational and security efficacy benefits of native integration across their broader product portfolios.

SentinelOne's attack surface reduction capabilities are modest as they do not include patch management. Several other vendors have this popular feature in their MES product sets. The company, however, is advancing its attack surface reduction capabilities. In September, SentinelOne announced a partnership with Automox, a cloud-native IT Operations platform provider, to automate and accelerate the process of vulnerability discovery and remediation.

Consider SentinelOne When

SentinelOne is a consideration for SMBs that are dissatisfied with their current EPP product and also recognize that EPP alone is no longer a sufficient endpoint security product strategy. They need a MES product that effectively pairs EPP and EDR together to deliver improved security with minimal extra operational requirements. For SMBs that need extra assistance from trained security specialists, SentinelOne's services and the services of SentinelOne's expanding ecosystem of managed security service providers are available to serve this need.

Sophos

Sophos is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

Sophos is among the most tenured vendors in this IDC MarketScape, with over 35 years of experience in offering cybersecurity solutions. During its tenure, the company has steadily broadened its product portfolio and service suite through organic development and acquisitions, expanded its channel, and diversified its geographic footprint. The company's cybersecurity product portfolio spans endpoint (PCs, mobile, and servers), network, email, and cloud workloads. The company introduced EDR in November 2018, and current modern endpoint security packaging is tiered based on feature set and inclusion of managed threat response.

Strengths

The company has a history of demonstrating its EPP prowess through independent evaluations. Among modern endpoint security vendors, Sophos is in the highest tier based on number of testers it is evaluated by, variety of tests conducted, and testing frequency.

Sophos is also distinguishable in its long-tail support for aging operating systems (PCs, mobile, and servers) and in supporting new OS versions rapidly after introduction.

The company caters to customers and partners in their native languages. Sophos is among the top one-third of vendors in the number of languages supported by its customer- and partner-facing technical agents.

The company's rollback remediation feature is comprehensive, returning files and systems settings to their precompromised state.

Constrained in security talent, Sophos addresses this deficient for its SMB customers with two options: Sophos-staffed MDR and partner-staffed MDR.

Challenges

There are just a few areas of capabilities in which Sophos is not in the top one-third of vendors. In attack surface reduction, Sophos does not offer patch management natively. Hardware-based integrity checks on firmware is also not present in Sophos' solution set.

A bit behind, Sophos' participation in independent EDR evaluations is less relative to other vendors.

Consider Sophos When

With its long and decorated history in EPP, Sophos is a solid consideration for SMBs seeking a replacement to their existing EPP vendor. Combined with Sophos' MDR service option, SMBs are better equipped to reduce their exposure to attacks that initially compromise user endpoints.

Trend Micro

Trend Micro is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

Trend Micro is the largest vendor in the worldwide corporate endpoint security market and among the largest in modern endpoint security. Its market presence is the result of uninterrupted focus on

customer endpoint security needs today and the needs of tomorrow. The same applies to the company's threat research. Trend Micro operates 15 threat research centers globally, and through its TippingPoint acquisition and founding of Zero Day Initiative, Trend Micro has consistently led industry efforts to discover and understand software vulnerabilities.

Strengths

As telemetry is the currency of threat detection, Trend Micro sits on an immense and diverse set of sources. In addition to the telemetry the company attains through its massive footprint in both corporate- and consumer-protected endpoints and physical servers, Trend Micro also gathers unique perspective from its mature IDS/IPS and email products. Last but not least, among established endpoint security vendors, Trend Micro was among the first to recognize and act upon the cloudification of enterprise datacenters and entered the cloud workload security market half a decade ago.

Attack surface reduction is another of Trend Micro's strengths. Differing from other vendors that rely on scanning for vulnerabilities, prioritizing, and then facilitating patching, Trend Micro takes a preventive approach. Its approach starts from its active perch on top of vulnerability knowledge via its deep involvement in the Zero Trust Initiative program. Combining this vulnerability knowledge with real-time knowledge of OS and software applications present on endpoints, Trend Micro actively deploys virtual patches to prevent attacks aimed at exploiting long-standing vulnerabilities and those recently discovered. This allows SMBs flexibility in rolling out official patches issued by software vendors.

Further demonstrating a proactive focus on attack surface reduction, Trend Micro introduced Zero Trust Risk Insights in September 2021. Zero Trust Risk Insights correlates data from endpoints with other sources to continuously monitor the threat and risk posture of identities and devices. Its functionality prioritizes vulnerabilities based on local and global threat intelligence, detects account compromises from anomalous user activity (e.g., logins, email usage, and file transfers), tracks user access to unsanctioned and risky cloud applications, and measures an organization's overall risk posture.

With a lengthy history of serving a worldwide customer base, Trend Micro speaks the local languages of its customers. Its local language support is among the top tier of vendors in this IDC MarketScape.

Other notable features and attributes of Trend Micro's MES product includes its rollback remediation feature (i.e., reversing changes to files and settings) and rapid agent compatibility with new OS releases.

Bridging talent gaps of its customers, Trend Micro offers MDR services staffed internally and co-managed through its partners.

Finally, Trend Micro is a sustainable company. Its profitable operations have and continue to be a source of reinvestment in product and customer support and an assurance of stability. In addition, its large base of EPP customers is an incumbent source of customers to upsell to MES and further contribute to Trend Micro's scale and profitable.

Challenges

There are only a couple areas that Trend Micro is not in the upper tier. Hardware-based firmware integrity monitoring and visibility (e.g., via the use of Intel's TDT) are not in Trend Micro's product. Trend Micro's third-party evaluations have not been as extensive as other vendors, particularly in EPP.

As one of the largest endpoint security vendors, Trend Micro is a frequent target for customer take-aways by competitors. Defending its position against the many competitors in the MES market will be an ongoing challenge. Although Trend Micro has been more successful than other large, incumbent endpoint security vendors, its market growth over the past two years modestly trails the overall market.

Consider Trend Micro When

Trend Micro's lengthy tenure in endpoint security, the breadth of threat intelligence and research, financial stability, and technical fluency across multiple security disciplines contribute to Trend Micro's consideration among SMBs. With a security product portfolio that spans personal endpoint devices, physical servers, email, web, network, data, and cloud workloads, Trend Micro represents a stronger consideration for SMBs that are seeking to reduce vendor relationships but also want the assurance of proven cross-product integration and manageability.

VMware

VMware is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

Making its entrance into the MES product market and simultaneously broadening its security suite of products, VMware acquired Carbon Black in late 2019. With a strategy to secure organizations' end-user devices, critical applications, and data independent of location, VMware through a combination of acquisitions and internal development has assembled a product suite that spans endpoints, access, network, cloud, and workloads. The Carbon Black Cloud is a cloud-based platform with security capabilities in NGAV/EPP, EDR, device control, vulnerability management, live query and response, threat hunting, and incident response.

Strengths

A strength for Carbon Black with the acquisition by VMware is the funding capacity of a much larger and profitable company, a base of customers to sell into, and the VMware brand. Although Carbon Black was already growing its MES market share prior to the acquisition, its market share under VMware continued to expand in 2020.

Another attribute of Carbon Black that also continued post-acquisition is its participation in independent EPP and EDR evaluations.

Supporting enterprise transition from EDR to XDR, VMware is positioned to natively integrate telemetry from multiple vantage points. Those vantage points include endpoints (PCs, servers, cloud workloads, and containers), Lastline's network detection and response (NDR) platform, VMware Cloud Web Security service hosted in VMware SASE points of presence (PoPs), VMware NSX network security products, and endpoint system status from VMware Workspace ONE. Many of these same vantage points do double duty as security policy and incident response control points.

Only a few of the vendors included in this IDC MarketScape have security integrations with device hardware, and VMware is one of them. The VMware Carbon Black Cloud can validate the BIOS image on Dell devices. Although not occurring at boot time, this check can generate an alert whether the BIOS image has been modified in an unauthorized manner.

VMware Carbon Black's native attack surface reduction capabilities include vulnerability management and device control. There are other add-on products from VMware that broaden attack surface

reduction capabilities. They include VMware Carbon Black App Control for high-risk endpoints in preventing unauthorized changes to applications and files and VMware Workspace ONE for patch management.

As most of the MES vendors, VMware also offers MDR. The VMware Carbon Black's MDR service is designed for organizations that want assistance in incident-led threat hunting.

Challenges

VMware Carbon Black does not have a rollback remediation feature to return compromised files and settings to preattack state (e.g., as part of recovery from a ransomware attack). VMware does offer an alternative. By partnering with VMware Cloud Disaster Recovery, endpoints can be recovered or rolled back to a healthy state while still remaining covered by the VMware Carbon Black agent. Through this partnership, the agent is retained and VMware Carbon Black's EDR capabilities can ensure a healthy time to failover to. Languages supported by customer-facing agents and in technical documents are limited to only English and Japanese. Placed into relative context, the average number of languages supported by vendors included in this IDC MarketScape is 10.

VMware Carbon Black is not sold into the consumer market. Compared with other vendors that are active in this market, VMware Carbon Black is not receiving threat telemetry from consumer devices.

Consider VMware When

VMware Carbon Black should be considered by SMBs that currently rely on cloud infrastructure for critical business operations or are moving in this direction. Providing an integrated ribbon of security from endpoints to cloud infrastructure, IDC contends, will be where VMware Carbon Black's future product investments will be concentrated.

WatchGuard

WatchGuard is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

WatchGuard entered the MES market by acquiring an established endpoint security vendor, Panda Security, in June 2020. Panda Security introduced its MES product in 2015. At acquisition, Panda Security's principal MES products were Panda Adaptive Defense 360 and Cytomic EPDR. The new WatchGuard Endpoint Security solutions were launched in June 2021.

Strengths

As mature security vendors in their respective security disciplines and each with a lengthy history of internal product development, the combined company has a solid foundation to organically fund development in cross-product integration and MES feature enhancements and market and channel-expanding initiatives.

With an existing integrated security product portfolio spanning network, messaging, and Wi-Fi security; multifactor authentication; and DNS-level protection, the acquisition and integration of Panda Security will strengthen WatchGuard's position in competing among vendors with similarly broad product portfolios. Missing from WatchGuard's portfolio that is present with a subset of MES vendors is cloud access security (aka cloud access security broker).

Among MES vendors, WatchGuard has a robust set of attack surface reduction (vulnerability assessment, patch management, device control, and host firewall) capabilities. Its Zero-Trust for Application Service adds another attack surface reduction capability. This service classifies each encountered executable as trusted or untrusted and denies execution of untrusted executables. Having launched this service in 2015, the company has six years of real-world experience in building out its vetted library of trusted executables and managing false positives downward.

Having a geographically concentrated endpoint customer base in Europe, WatchGuard supports its customers and partners through the native language of their countries.

Among the most responsive in the MES market, WatchGuard commits to have its agent compatible with new OS releases the same day they become available.

Bolstering its detection capabilities, WatchGuard's MES product routinely integrates a set of indicators of attack (IoAs) curated by its team of threat hunters. These IoAs are beneficial in detecting malwareless/living-of-the-land attacks.

WatchGuard (Panda Security) has a lengthy history in serving the consumer segment. From this segment, WatchGuard gains a stream of threat telemetry and visibility of a large set of distinct applications across very heterogeneous environments that other MES vendors without a consumer focus do not have.

Challenges

Although Panda Security joined WatchGuard with a well-rounded set of EPP capabilities and added EDR back in 2015, Panda Security's participation in independent EPP and EDR evaluations is low among MES vendors. This circumstance places WatchGuard at a comparable disadvantage in gaining market mindshare relative with vendors that have been more participatory.

Panda Security's support for a variety of device platforms is expansive up to a point as iOS is not supported. In comparison, three-fourths of MES vendors state they support iOS.

While not supported by a majority of MES vendors, WatchGuard is among the vendors that also does not offer file recovery as part of its remediation options, although this feature is expected for early release in 2022.

Consider WatchGuard When

Existing WatchGuard customers should consider the WatchGuard MES product. The Panda Security acquisition fits the profile of past WatchGuard acquisitions and product expansions of enterprise-grade security without enterprise-size operational requirements. As a single, cloud-based administrative console that crosses WatchGuard and Panda Security products is a work in progress, best to examine current progress and future commitments to full integration. IDC also recommends conducting a POC involving a diverse sample of PCs (i.e., users in different roles or departments in your business) to determine if malicious files are instantly discovered that your current EPP product did not detect. For SMBs seeking a MDR service, that service will be delivered by a WatchGuard channel partner. IDC also recommends assessing the certification and experience of your WatchGuard's channel partner in use of the Panda Security product.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

Modern endpoint security products protect personal computing devices (PCDs) (such as workstations and laptops) from cyberattacks through the detection of malicious code and behaviors present or operating within the PCD and then facilitate a counteracting response (e.g., block, remove, or isolate). Modern endpoint security products contain two detect and response mechanisms differentiated based on elapsed time and human involvement. Endpoint protection platforms (EPP) reach detection verdicts and initiate responses in real time and autonomously (i.e., without human involvement). Endpoint detection and response (EDR) is a second stage of detection and response for cyberattacks that have evaded EPP detection. With EDR, the time to reach detection verdicts and initiate responses can span minutes to days. How fast the cyberattack unfolds, its sequence of steps, and its sophistication and uniqueness are factors that affect the elapsed time in detection and response. Automation and predefined workflows assist in reducing the elapsed time. Security analysts (humans) are typically involved, at minimum, to confirm detection and/or authorize response.

Strategies and Capabilities Criteria

Tables 1 and 2 provide key strategy and capability measures, respectively, for the success related to the worldwide modern endpoint security for small and midsize businesses.

TABLE 1

Key Strategy Measures for Success: Worldwide Modern Endpoint Security for Small and Midsize Businesses

Strategy Criteria	Definition	Weight (%)
Functionality or offering strategy	The vendor's strategy for improving the security efficacy of its modern endpoint security products	50.00
Growth	The vendor's market momentum	30.00
Financial/funding	The vendor's capability to organically fund its operations and market expansion	15.00
Delivery	The vendor's complementary engagement in market segments outside modern endpoint security	5.00
Total		100.00

Source: IDC, October 2021

TABLE 2

Key Capability Measures for Success: Worldwide Modern Endpoint Security for Small and Midsize Businesses

Capability Criteria	Definition	Weight (%)
Functionality or offering	Breadth of vendor's product functionality and device support	55.00
Software development	The vendor's investment in software development and engineering talent	20.00
Portfolio benefits	The vendor's product features that facilitate post-infection response including remediation	10.00
Range of services	The vendor's ability to support varied customer circumstances	10.00
Customer service delivery	The vendor's capabilities to engage with a geographically diverse market	5.00
Total		100.00

Source: IDC, October 2021

LEARN MORE

Related Research

- *Top Technology Integration Opportunities for Unified Endpoint Management* (IDC #US48266821, September 2021)
- *Market Analysis Perspective: Worldwide Tier 2 SOC Analytics, 2021 – Where the Puck Is Going* (IDC #US47394921, September 2021)
- *Market Analysis Perspective: Worldwide Corporate Endpoint Security, 2021* (IDC #US48208121, September 2021)
- *IDC's 2021 Ransomware Study: Where You Are Matters!* (IDC #US48093721, July 2021)
- *Which Criteria Rank Highest in the Evaluation of Modern Endpoint Security Products?* (IDC #US48053021, July 2021)
- *Worldwide Corporate Endpoint Security Forecast, 2021-2025: On a Higher Growth Trajectory* (IDC #US47957021, June 2021)
- *Worldwide Corporate Endpoint Security Market Shares, 2020: Pandemic and Expanding Functionality Propelled Market Growth* (IDC #US47768021, June 2021)
- *Insights from IDC's EDR and XDR 2020 Survey: Operational Challenges and Initiatives Are Abundant* (IDC #US47357921, January 2021)

Synopsis

This IDC study represents a vendor assessment of providers offering modern endpoint security for small and midsize businesses through the IDC MarketScape model.

"Modern endpoint security products, the combination of deterministic protections and post-compromise detection and response, are rapidly becoming an essential component to small and midsize businesses' cybersecurity arsenals," states Michael Suby, research vice president, Security and Trust at IDC. "Reliance on a basic endpoint security product is a risky proposition with today's advanced threats and the business harm that can inflict. Favorably for SMBs, there are many vendors with capable modern endpoint security products. Selecting a modern endpoint security product and optimizing its use, however, can be a challenge for SMBs due to their acute budget, time, and talent constraints. To alleviate these constraints, IDC's recommendation for SMBs is to first focus on the fundamentals of what a MES product is designed to accomplish and then assess ease of use, integration, and collaboration with other security technologies that strengthen security posture and the option of managed services. Finally, modern endpoint security products are continuing to advance in their capabilities. While a time-consuming effort, SMBs should conduct proofs of concept routinely to ensure their limited security budgets are well spent."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com