White Paper

Adaptive Protection, a Critical Capability in Disrupting Sophisticated Attacks

Sponsored by: Symantec (a Broadcom division)

Michael Suby
June 2021

IDC OPINION

End users' devices have been and will continue to be primary targets for threat actors. Not only are these connected devices a stepping-stone to high-value assets, but they are also soft targets. Soft because there are multiple conduits into these devices (web, email, physical media, software updates, remote administrator access, and peer-to-peer applications). In addition, end users, as humans, can be manipulated, and applications, configurations, and patterns of use are as unique as each end user and subject to change. Standards of work are also evolving. Cast into the unprecedented remote working experiment of the pandemic, the location of work has forever changed to be more virtual and dynamic. Moreover, the devices of work will increasingly be influenced by end-user preferences, often in the spirit of convenience. All of this provides threat actors a broad attack surface and range of motion that are challenging to surveil with comprehensiveness and certainty.

Endpoint security solutions have evolved with high-tech protection and detection mechanisms to mitigate this ever-present risk. But, as history has shown, malware still lands on end-user devices, threat actors tweak their techniques to evade detection (e.g., living-off-the-land tactics), and false positive alerts plague security analysts. Consequently, security breaches originating from an infected endpoint still occur.

IDC's perspective is that organizations have over relied on protection and detection mechanisms in endpoint security at the expense of strengthening security posture and reducing the attack surface. There should be a more equal balance in organizations' endpoint security arsenals. Yet solutions designed to enhance security posture and reduce the attack surface at enterprise scale, with precision and individuality while automatically adapting to changing circumstances, have not existed. Moreover, concerns of disrupting business operations and employee productivity have added to organizations' hesitancy in defining and enforcing deny lists for all but legitimate activities.

Symantec's recently launched Adaptive Protection rebalances enterprises' endpoint security arsenals by limiting threat actors' range of motion. Leveraging Symantec's global threat intelligence on behaviors involving trusted processes (e.g., a legitimate executable processing a download) and combined with artificial intelligence (AI) modeling and machine learning (ML) engines, Adaptive Protection automatically produces a real-time heatmap of process behaviors and offers preventive recommendations (e.g., deny or monitor) based on the prevalence of behaviors within the organization. By denying specific behaviors that Symantec has identified, bona fide attack tactics immediately reduce attackers' range of motion, without disrupting routine processes. What are preemptively disrupted are attack chains that attempt a denied behavior. Those chains are immediately broken.

Persistently, attackers will attempt additional process behaviors, some that have occurred within the enterprise. Adaptive Protection is responsive to the uniqueness of each enterprise to thwart these attempts. Drilling into heatmap details, Adaptive Protection administrators can quickly see which uncommon behaviors have occurred at each endpoint and their prevalence. Armed with this knowledge, Adaptive Protection administrators can tailor deny and monitor rules for an individual device, organizationally grouped devices, or devices clustered by Symantec as exhibiting similar behaviors.

Adaptive Protection is also dynamic. With both attack tactics and enterprise environments continuously evolving, Adaptive Protection's heatmap and recommendations are designed to automatically adjust. The upward drift in risk brought on by changes in attack techniques and the enterprise environment becomes more preventable.

Complementary to Symantec Endpoint Security, Adaptive Protection reduces the potential of attacks advancing beyond the first infected endpoint by selectively closing down uncommon process behaviors within and among enterprise endpoints. Endpoints, however, are just one attack vector and illicit process behaviors are just one indicator of risk. The combination of business essentialness and threat actors' refined capabilities to covertly manipulate endpoints has contributed to the popularity of websites, email, text, and file sharing for delivering malicious code to endpoints and coaxing end users to divulge sensitive information.

Like process behaviors, websites, peer-to-peer communications, and file sharing volumes are extreme and circumstances vary and change rapidly. Legitimacy can change instantaneously and cannot be assumed at face value. Gathering broadly and interpreting granularly the latest threat intelligence are essential in adaptively assessing risk and enforcing risk-mitigating rules tailored to each enterprise's employees' web, communication, and file sharing activities. Beneficially, Symantec has a head start. The adaptive techniques used to preempt uncommon process behaviors at endpoints will be extended to the full protection stack.

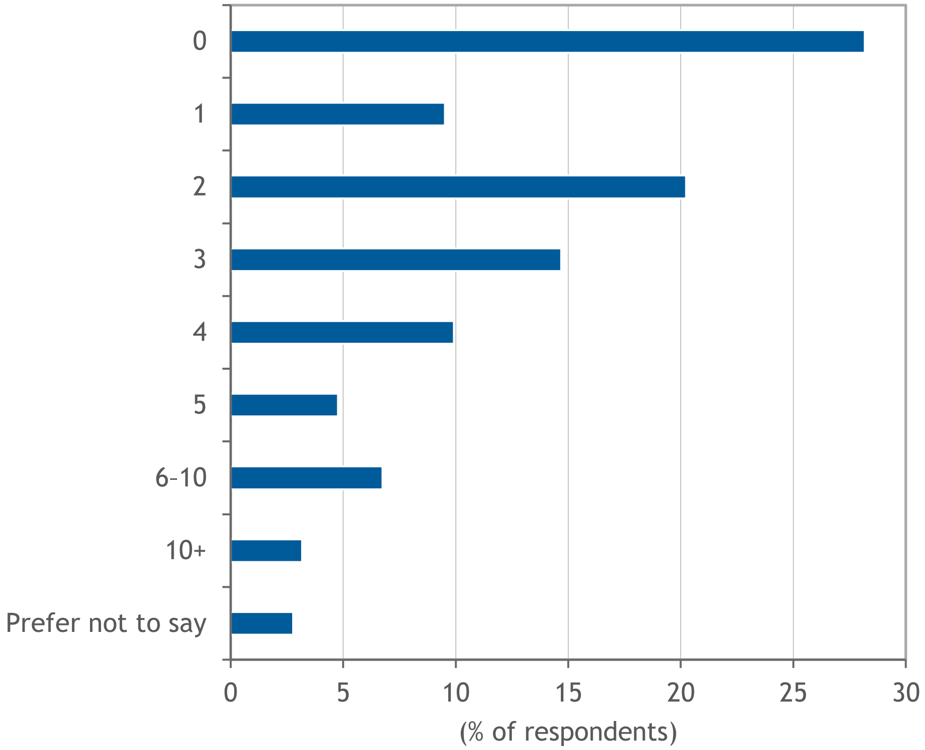
Protection and Detection Technologies Are Not Enough

For many organizations, current cybersecurity solutions and practices fall short on meeting their risk mitigation objectives. In a recent IDC survey, 60% of surveyed organizations with 5,000+ employees suffered at least one major security breach annually. Less than one-third of surveyed organizations claim to have avoided a major security breach in the past two years (see Figure 1).

FIGURE 1

Major Security Breaches in the Past Two Years

Q. *Approximately how many major security breaches has your organization had in the past two years that involved spending significantly extra resources to rectify?*



n = 252 (organizations with 5,000+ employees)

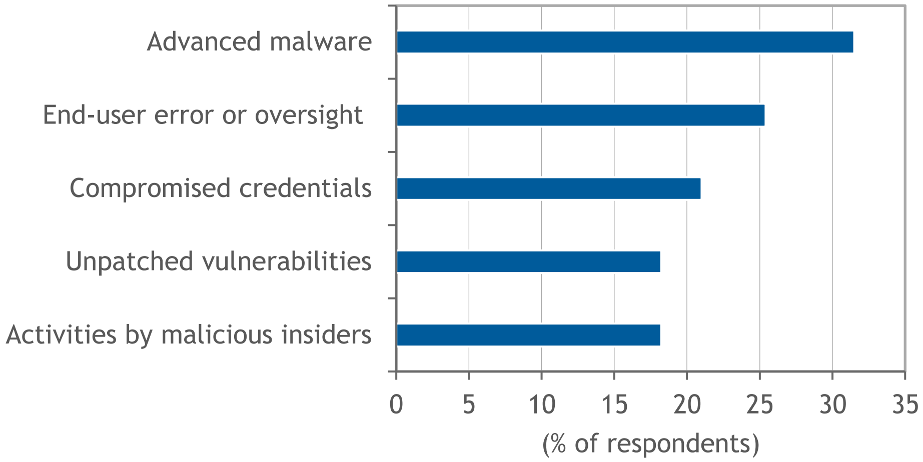
Source: IDC's *EDR and XDR Survey,* December 2020

Although the vast majority of organizations use endpoint security products and some use products from multiple vendors, advanced malware is a common contributor to security breaches followed by end-user error and compromised credentials (see Figure 2).

FIGURE 2

Most Frequent Contributors to Security Breaches

Q. Which of the following were the most frequent contributors to security breaches? (Select up to 3 contributors from the list of 12.)



n = 181 (organizations with 5,000+ employees)

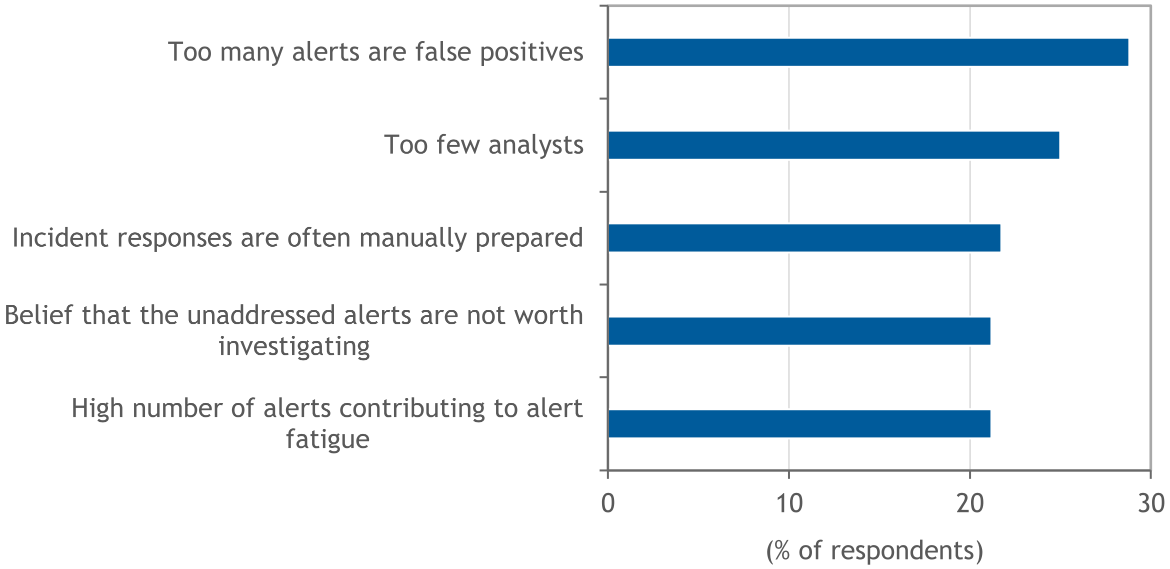
Source: IDC's *EDR and XDR Survey,* December 2020

As confirmed by IDC's survey, there is also a positive correlation between the number of security breaches and the number of uninvestigated alerts and the elapsed time in investigating alerts. Moreover, contributing to uninvestigated alerts and investigation time is the number of false positive alerts (i.e., triggered by benign activity) and alert fatigue (see Figure 3).

FIGURE 3

Reasons That Prevent Organizations from Investigating and Responding to Suspicious Alerts

Q. What is preventing your organization from investigating and responding to all suspicious alerts each week? (Select up to two reasons from list of nine — top 5 reasons shown.)



n = 184 (organizations with 5,000+ employees)

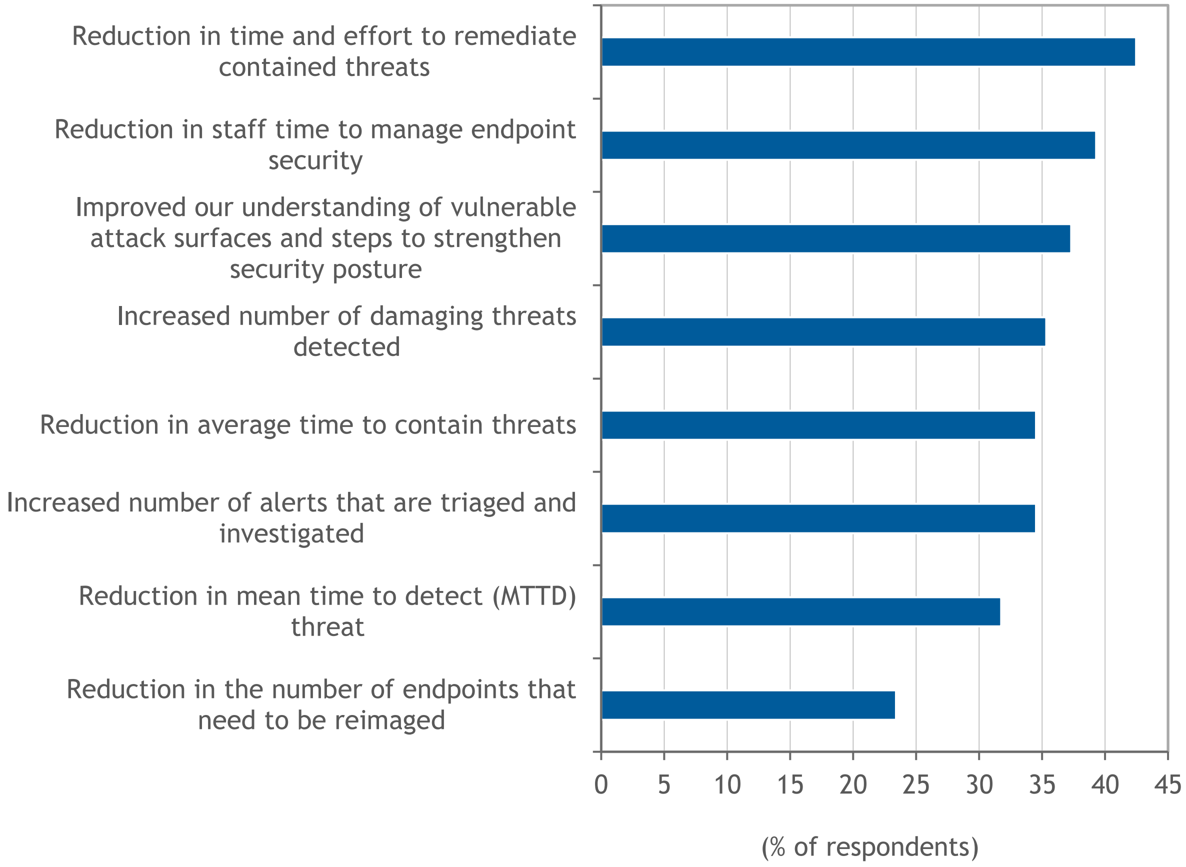
Source: IDC's *EDR and XDR Survey,* December 2020

As organizations have turned to endpoint detection and response (EDR) to improve their defenses, they report a range of benefits (see Figure 4). Not all of the benefits, however, are in EDR's core mission of detect and response. Understanding vulnerable attack surfaces and gaining insights on strengthening security posture were among the most frequently cited benefits. Although beneficial, this understanding is occurring after a threat actor has already penetrated the organization's environment. Nevertheless, this EDR benefit is demonstrative of organizations recognizing the value in preemptively reducing their attack surfaces and strengthening their security posture.

FIGURE 4

Benefits Delivered by EDR

Q. *Which of the following are the most important benefits EDR delivered to your organization? (Select up to four benefits among the eight listed.)*



n = 252 (organizations with 5,000+ employees)

Source: IDC's *EDR and XDR Survey,* December 2020

EDR is not the only means to aim a spotlight on vulnerable attack surfaces. Periodic blue and red team exercises and penetration tests also add to understanding. Yet these approaches have limitations:

- **Rearview mirror staging:** Exercises and tests conducted on current threats attempting to exploit current vulnerabilities are an incomplete assessment of readiness to thwart the next attack technique or gauge vulnerabilities attributed to future changes in the enterprise environment. That will have to wait until the next scheduled assessment.
- **Expertise required:** Experience and talent are essential, but many organizations are inadequately equipped or funded to conduct exercises and tests tailored to their enterprise's circumstances.
- **Not a closed-loop system:** Exercises and tests identify security gaps and vulnerabilities and may recommend steps to improve the security posture. Unfortunately, the recommendations may be too complex and time consuming to operationalize rapidly, leaving the enterprise bidding time in a heightened state of exposure awareness.

Adaptation Is Essential in Turning the Tide on Adversaries

Taking a critical look at how security is practiced, there is ample room for threat actors to maneuver and succeed. Security, whether as endpoint security, intrusion detection, message content filtering, or web security, is constructed to block threats that are instantly identifiable as malicious or unwanted with a high degree of confidence. This is true whether the mechanisms that power automatic detection and blocking use hashes, signatures, reputations, categories, behavioral analysis, ML/AI, or some combination.

While advancements in automated detections have expanded the range of threats identified and blocked with high confidence, experienced threat actors vary their techniques to avoid detection. As IDC's survey called out, advanced malware is the most cited contributor to security breaches. Experienced threat actors also educate themselves on how security products operate. By reverse engineering these products, conducting reconnaissance, and trial-and-error experience, they hone their ability to evade automatic detections.

There are, however, supporting reasons to continue to use general-purpose, one-size-fits-all security products. From a business perspective, broad categories of attack types are thwarted without impacting the normal flow of business (i.e., business transparency) or taxing security personnel.

In addition, security teams have the option to define and enforce customized deny rule sets to block specific activities. This supplemental approach, however, has drawbacks. First, balancing security risk and business transparency is still a consideration. More rules and rules more granularly defined make this balancing act more challenging. Second, life-cycle rule set management is necessary and is generally a manual effort and, therefore, not inherently scalable. Third, changes in the threat landscape can lessen rule set efficacy. Inevitably, persistent threat actors will seek to circumvent customized rules.

Faced with the limitations of general-purpose security products and customized rule sets, plus threat actors continuously pushing forward, organizations have elevated their post-compromise detection and response capabilities – a justifiable security layer, but also a layer that is, at its core, reactionary. To succeed, the actions of threat actors within the organization's IT environment must be detected and the threat contained with both speed and comprehensiveness before damage has occurred. Containment, at its best, should also be business transparent. Considering the ever-expanding and transformative state of organizations' IT environments, threat actors have more new space to maneuver in, making detect and respond a challenge of escalating proportion.

IDC contends that, to turn the tide on threat actors, prevention needs to become more central to security practices. Of course, the general concept of prevention is not new. It has been a long-held foundational element. Nevertheless, prevention has not evolved to be as effective in today's circumstances as it was in the past. To become more effective in today's hyperdynamic threat landscape and IT environments, IDC believes prevention should be optimized on the following attributes:

- **Adaptive:** As the threat landscape and IT environment change, so too must the prevention mechanisms adapt to retain and, even better, improve their efficacy in narrowing threat actors' ability to enter, infect, and progress.
- **Customizable:** Each organization's mix of IT environment, security technologies, and risk tolerance is unique. Consequently, prevention must be tailored for each organization.

- **Automated:** Threat actors succeed by exploiting gaps in security defenses before organizations can put countermeasures in place. To optimize the effectiveness of prevention, adapting and customizing must be facilitated through automation to narrow threat actors' window of opportunity and, equally important, minimize demand on security personnel's time and talent.
- **Extensible:** With multiple inbound and outbound vectors that threat actors exploit, organizations employ multiple forms of security technologies. Adaptive and customizable prevention should be extensible to complement as many security technologies as feasible.
- **Business transparent:** The effectiveness of prevention demands functioning in real time, and that requires operating within the flow of business. So not to hinder the flow, the potential adverse effect of prevention must be assessable with a high level of accuracy and comprehensive before enforcement is turned on and continuously monitored thereafter to gauge for unforeseen impacts.

Optimized on these attributes, prevention can deliver the following additional benefits:

- **Increase threat actors' costs:** By being adaptive and customizable, the organization's security defenses differ from every other organization. Repeatable playbooks and techniques used by threat actors to evade standard security configurations are, consequently, less likely to succeed. To overcome this, the threat actor would need to step up their attack method from automated and repeatable techniques to bespoke techniques designed for a single target. The one-to-many return the attacker prefers is no longer viable and this may convince the attacker to direct their resources on other, less well-defended targets.
- **Lower detect and response workload:** With avenues for attackers to use reduced via prevention, the number of alerts, benign and serious, are poised to be reduced and the same for security incidents. In a volume-driven operation, security teams could see their reactionary, detect-and-respond workload diminish, allowing them to concentrate on fewer incidents and possibly redirect their energies to security initiatives of strategic importance.

Solution

The first of Symantec's adaptive solutions, Adaptive Protection reduces an enterprise's attack surface and enhances an enterprise's security posture by limiting attackers' range of motion within and from compromised endpoints. The building blocks of Adaptive Protection are Symantec's global threat intelligence, AI modelling, and ML engines. In concert, they automatically create and refresh a real-time collection of trusted process behaviors that have been utilized in attacks and provide comprehensive visibility of the enterprise's processes and behaviors. Combined, Symantec presents a heatmap on the actual prevalence of these behaviors involving trusted processes.

For the behaviors that have not occurred within the enterprise, this is a low-risk deny decision. If there are future occurrences of these behaviors, they will automatically be blocked. In other words, the uncommon behavior has been isolated and treated separately from other behaviors associated with the same trusted process.

Taking Adaptive Protection further with ranking of the behavior frequency and the endpoint devices involved, security administrators can activate deny, monitor, and allow decisions for each behavior for an individual device, devices grouped organizationally (e.g., finance, HR, IT, or marketing), or Symantec-clustered devices based on behavioral commonality. This granular understanding can also assist security administrators in prioritizing their investigations into the legitimacy of the behaviors involving trusted processes.

Encouraging security administrators to conduct their investigations and increase deny enforcements is the customization Adaptive Protection produces in their security defenses. The greater they push distinctiveness in their security defenses, the less attractive their organization is as a target relative to organizations that are less distinctive. In addition, the security posture of their endpoint devices strengthens as the denied behaviors no longer represent a security risk since they are blocked from occurring.

Adaptive Protection also introduces the Quick Tune setting. Quick Tune identifies all zero-prevalence behaviors (i.e., behaviors not present in an environment) and configures them to deny. This greatly simplifies an administrator's workflow, needing only the administrator's approval to enable these settings to take effect in the product. Quick Tune further reduces the time to value and ease of adoption of Adaptive Protection.

OPPORTUNITIES

IDC believes the market opportunity for Symantec Adaptive Protection is strong and further strengthened when Symantec extends the adaptive and customization capabilities of Adaptive Protection into additional Symantec security technologies and platforms.

Starting with Adaptive Protection is a logical first step in Symantec's Adaptive Protection capabilities. As we stated previously, end users and their devices are frequently targeted. As such, endpoint security is widely accepted as a critical first line of defense in cybersecurity.

This criticality of endpoint security became amplified with the COVID-19 pandemic as large swaths of information workers were suddenly cast into work-from-home arrangements on a full-time basis. In parallel, organizations accelerated their migration to cloud services. This dispersion in the IT environment, while essential during pandemic lockdowns and also aligned with organizations' strategic digital transformation plans, made endpoints even more targeted as they operated outside the protections of enterprise network defenses and end users gained greater and frequently direct internet access to more cloud resources. Neither remote working nor cloud usage will return to pre-pandemic levels, so the importance of effective endpoint security will not diminish.

Adaptive Protection is also well aligned with the concept of zero trust. As security administrators progress in their use of Adaptive Protection, the behaviors allowed with trusted processes will become increasingly restricted to only behaviors that are commonly used in the organization's environment. All other behaviors are disallowed.

For security teams struggling to make tangible progress in zero trust, Adaptive Protection provides a drop-in, practical means. IDC anticipates that as Symantec extends Adaptive Protection's functional capabilities into other Symantec security platforms, the alignment with zero trust will continue, providing security teams with a unified approach to put zero trust more broadly into practice.

Endpoint security as practiced today with endpoint protection platforms and endpoint detection and response continues to be highly dependent on knowing how threat actors operate, attempting to predict how they may operate, and detecting and responding to compromises with comprehensiveness and speed. While essential in a multilayered defense, Adaptive Protection offers a complementary, robust, and business-transparent approach for reducing endpoint's attack surface, strengthening the security posture, and restricting threat actors' range of motion, including lateral movement. And as we previously stated, Adaptive Protection could have a positive impact on incident responders' workflow volume.

Finally, large enterprises have long been first adopters of new security technologies. However, over time their stacks of security technologies from multiple vendors have become too broad and complex to deliver the security outcomes they require. The desired remedy is to reduce the number of security vendors while gaining tighter cross-product integration and holistic manageability. They also need demonstration that their strategic security vendors will continue to innovate to combat a threat landscape that will become even more sophisticated, targeted, and relentless over time. Symantec's internally developed adaptive product line initiative is a demonstration that Symantec is continuing on the path of innovation.

CHALLENGES

The key challenge we believe Symantec will face is in winning over a skeptical buyer community. Stung by other replacement or additive security technologies that did not deliver on expectations on risk mitigation and/or operational ease, they are not going to be easily won over by either an incumbent or a new vendor. Greater up-front demonstration of value, particularly ease of use, will be needed. In Symantec's favor, Adaptive Protection is included in the Symantec Endpoint Security Complete (SESC) agent. With no additional software agents to deploy, broad-based proof of concepts with existing SESC customers should be feasible. With the first instantiation of security value shown in heatmap visibility of behaviors among trusted processes that have been utilized in attacks, perhaps enabling customers to quantify an aspect of risk they previously could not assess, that too should work in Symantec's favor.

CONCLUSION

Too often threat actors have held the upper hand. With a broadening and diversifying IT environment, they need to find just one unguarded or lightly guarded entry point. From that original infection, they span outwardly to other devices and systems. Always seeking ways to disguise their movements, threat actors have turned to hijacking trusted processes as they are less likely to be restrained so not to disrupt legitimate business operations.

Symantec Adaptive Protection offers a new approach to prevent illicit use of trusted processes. Combining knowledge of uncommon behaviors and visibility into all behaviors and processes that have occurred, security administrators are equipped to confidently place restraints on legitimate processes without restraining the business. In addition, the custom preventions produced by Adaptive Protection make each environment uniquely defended, one that is less susceptible to attackers' standardized and repeatable tactics. From IDC's perspective, Adaptive Protection is a technology that is long overdue and worthy of adding to organizations' endpoint security arsenals.

MESSAGE FROM THE SPONSOR

A division of Broadcom Software, Symantec is a global leader in cyber security and helps organizations and governments secure identities and information wherever they live. Symantec's Integrated Cyber Defense approach simplifies cyber security with comprehensive solutions to secure critical business assets across on-premises and cloud infrastructures. Symantec Endpoint Security, Network Security, Information Security, and Identity Security solutions are uniquely integrated and infused with rich threat intelligence from the Symantec Global Intelligence Network, as well as advanced AI and machine-learning engines to protect data, to connect authorized users with trusted applications, and to detect and respond to the most advanced targeted attacks.
For more information, go to https://www.broadcom.com/products/cyber-security.

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

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.