Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **April 2020**
Sponsored by **Quest Software**

Focusing on the Endpoint as a Key Element of Your Security Infrastructure

Executive Summary

Endpoints used to be safely operated behind a network perimeter. However, the rapid growth of remote access to corporate resources, cloud-based applications and social media by desktops, laptops, smartphones and tablets means that the endpoint is now the new perimeter. Endpoints are being attacked in a variety of ways, including email-based phishing, ransomware, malware, and drive-by downloads from web surfing.

Given that endpoints often store large quantities of corporate data, and also contain virtually everything that attackers need to gain entry into corporate networks, robust endpoint protection is a critical element in any corporate security infrastructure.

KEY TAKEAWAYS

- Threat actors have expanded the range of attack vectors used against organizations and endpoints. As threats expand, so too must the nature of security defenses to protect against and mitigate advanced and emerging threats. Anti-virus protections alone will not protect endpoints from modern threats.

- Endpoints are attractive to threat actors for three reasons: many endpoints directly store sensitive and confidential business data that can be used for nefarious purposes, compromising an endpoint often provides access to further network resources and cloud data repositories, and newer categories of mobile endpoints have lower security defenses compared to endpoints located behind perimeter and network security defenses.

- Ransomware, malware, phishing attempts and other types of cyber attacks continue to grow in volume and complexity, with several hundred thousand new malicious programs or unwanted apps registered every day.

- New categories of endpoints with emergent business applications are finding their way into physical organizational spaces, such as Alexa for Business and Apple HomePod (in the home office of corporate executives or consultants). Equally, compromising the operational technology endpoints that power smart buildings would enable an attacker to manipulate people's movements within a building, potentially creating life-and-death situations as the building turns against its inhabitants. The security threats that might be targeted against these new categories of endpoints are unknown or only poorly understood at this stage.

- Addressing the threats unleashed against endpoints requires a prudent balancing of people, process and technology investments. All three working in synergy provides the basis for effective protection, while relying on only one or two will undermine the efficacy of the overall playbook.

Robust endpoint protection is a critical element in any corporate security infrastructure.

ABOUT THIS WHITE PAPER

This white paper was sponsored by Quest Software; information about the company is provided at the end of this paper.

Threats to Endpoints

Two statements are true about endpoints: first, they are critical to getting work done by employees, and second, they are under attack by cyber criminals. With respect to employees, a growing diversity of endpoints are used for task completion, organizational communication, team collaboration and virtual meetings, including laptops, tablets, smartphones, and new smart devices such as smart speakers. Cyber criminals, on the other hand, have diversified the range of attacks unleashed against endpoints that circumvent traditional endpoint security capabilities to gain a foothold

for data exfiltration, credential compromise, and fraud. Initial footholds lead to further attacks, including supply chain phishing attacks and lateral movement to gain control over an increasing set of endpoints, servers and other network devices in anticipation of a master stroke to cripple the organization, such as through a ransomware attack.

Security threats against endpoints include traditional and emerging attack vectors, such as:

- **Malware**
  Viruses were the early threats against endpoints, with anti-virus software the traditional mitigation. Known virus and broader malware threats could be described by a signature, enabling detection through signature matching. Newer advanced malware variants eschew static description, featuring polymorphic and multi-stage approaches to circumvent signature-based anti-virus and anti-malware protections. And even for those threats that can be described with a signature, there's an active threat window between initial release and the signature file being developed by security vendors and deployed to all endpoints, raising the specter of compromise from zero-day threats. Verizon recently noted that 30 percent of data breaches involve malware being installed on endpoints. Such threats can remain undetected for hundreds of days.

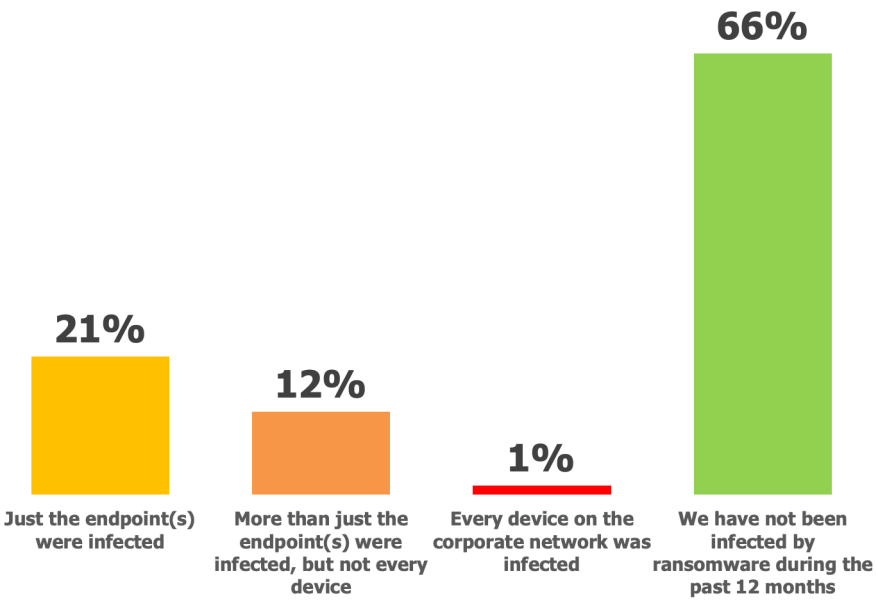
- **Fileless Attacks**.
  Anti-virus and anti-malware protections have traditionally focused on files as the threat container, but newer fileless threats use surreptitious methods to execute an attack. For example, apps that are bundled with the endpoint's operating system are leveraged to download a malicious payload into memory only, thus bypassing disk operations that can be analyzed for malicious patterns. Apps for Windows such as the command line and PowerShell are among the most frequently hijacked apps to execute malicious tasks, and the very low volume of malicious activity makes it difficult to identify and stop such threats in real-time. The lack of a file means traditional file-based security protections are blind to fileless attack threats.

- **Data Breaches**
  Stolen devices, compromised credentials and malicious apps provide cyber criminals with access to any sensitive and confidential data stored on endpoints for sale on the dark web, identity theft, and targeted spearphishing attacks. More than half of endpoints contain sensitive and confidential data that is subject to the growing body of data protection regulations around the world. Breached endpoints can result in costly fines, such as the accidentally misplaced USB thumb drive at Heathrow Airport that led to wider revelations about lax security and resulted in a £120,000 fine against the airport. In the new age of the General Data Protection Regulation (GDPR) and other similar regulations around the world, regulatory fines for data breaches will skyrocket.

- **Ransomware**
  Our recent reports on cyber security threats in the government and healthcare industries, respectively, have documented the cost of ineffective protections against ransomware. Targeted ransomware attacks have also been unleashed against other industries, including industrial infrastructure, transportation, education and financial services, with endpoints a key vector of initial infiltration. Ransomware attacks cause disruption to standard business operations (and in healthcare thus threatens human life), data loss, financial damage, reputational impacts, and even business continuity. It's the scourge of the modern cyber age. As shown in Figure 1, ransomware is quite common.

Security threats against endpoints include traditional and emerging attack vectors.

Figure 1
Spread of Infection for Successful Ransomware Attacks During the Previous 12 Months



Source: Osterman Research, Inc.

- **Phishing Attacks**
  Seemingly harmless emails that prey on people's vulnerabilities are a key attack vector for cyber criminals, leading to lost credentials and unauthorized system access and activity (e.g., through a fake password reset email), misappropriated funds (e.g., via an email purportedly from the CEO requesting an urgent bank transfer to a new joint venture partner), or as mentioned previously, a successful ransomware attack. The simplicity of sending phishing emails on a broad scale or as a targeted attack makes it the most common initial delivery method for attacks, and the lack of malicious attachments neuters traditional endpoint security mechanisms. Web links included in a phishing email may be harmless when initially clicked, but weaponized after a certain amount of time has lapsed in an attempt to circumvent once only security checks.

- **Phishing via Social Media Channels**
  New business-oriented and consumer-facing social media services have introduced new channels for phishing attacks, circumventing email-based anti-phishing protections. For example, employees can be tricked into establishing connections with cyber criminals via fake identities on LinkedIn, and then interact with their growing network through LinkedIn Messaging. Requests that would usually be subject to email-based protections bypass security checks, rendering employees vulnerable to social engineering attacks.

- **Unpatched Vulnerabilities**
  Unpatched vulnerabilities in operating systems and commonly used applications can be exploited to exfiltrate data, spread ransomware and move laterally to control more systems and applications. Over one third of security breaches are caused by existing vulnerabilities. With more than 5,000 common vulnerabilities and exposures identified each year for the top 20 client applications, there's a huge attack space ripe for the picking. While organizations often take more than three months to patch newly identified vulnerabilities (and that's the good organizations - some leave vulnerabilities unpatched for years!), cyber criminals move much faster, often developing exploits within a month of the initial notification from the vendor. Attackers, therefore, have on average at least a

Seemingly harmless emails that prey on people's vulnerabilities are a key attack vector for cyber criminals.

two-month window of opportunity to initiate attacks against ill-protected and unpatched endpoints.

- **Compromised Software Patches and Updates**
  Compromising valid software updates from a software vendor with malware magnifies the impact of cyber criminal activity. The normal distribution of compromised updates can result in immediate compromise of thousands (or millions) of endpoints, the activation of ransomware, or weakening current defenses across multiple organizations in preparation for further attacks. The global WannaCry ransomware crisis in mid-2017, for example, was initially caused in the Ukraine through compromised software updates.

- **Drive-By Downloads**
  Compromised and malicious websites can be set to automatically download malicious software to a visitor's device, without requiring any involvement or clicks from the user. The recent Webroot Threat Report found that 25 percent of malicious URLs are hosted on otherwise non-malicious domains, indicating widespread compromise of high reputation organizations and sites. Compromised ads that deliver a malicious payload via a compromised advertising network are another frequent path for spreading malicious software.

- **Infected USB Drives**
  Targeted attacks against an organization have been initiated through the apparent accidental loss of USB thumb drives that in reality contain malware and other threats. Cyber criminals distributing these infected USB thumb drives hope that they will pique employees' curiosity, and that once plugged in to see what's on the drive, the malicious payload can be executed on a trusted but now compromised endpoint. Passwords, credentials and other data can then be quietly exfiltrated, lateral movement attempted from the initial place of infection, or a ransomware attack instantiated.

- **Insecure and Non-Compliant Consumer Applications Used by Employees**
  Consumer-grade apps on smartphones and other endpoints may leak data through vulnerabilities or undisclosed backdoors created by the vendor to capture conversations and other data for sale. If these apps are used for work purposes, sensitive and confidential business data can be accessed by unauthorized individuals and entities. A similar problem is that consumer-grade apps often lack required enterprise-level controls, such as the ability to remove offensive material, redact sensitive data, and moderate conversations.

- **New Devices That Lack Strong Security**
  The skyrocketing adoption of internet of things (IoT) devices has resulted in hundreds of millions of new devices being deployed across the physical world. However, with 82 percent of IoT device manufacturers being concerned that their own devices are inadequately secured from cyber attacks, it is clear that security is an afterthought rather than a core design principle. In the healthcare industry, for example, implanted medical devices are vulnerable to cyber attack, causing significant health risks for already at-risk patients. An equal threat arises from BYOD strategies where employees are encouraged to use their own current endpoints - particularly mobile phones and tablets - for work tasks, but without the corresponding hardening of security settings found on corporate-owned devices.

- **New Categories of Endpoints That Have Undetermined Security Threats**
  New categories of endpoints with emergent business applications are finding their way into physical organizational spaces, and as of yet, the security threats that might be unleashed against these endpoints are unknown or only poorly understood. For example, digital assistants on smartphones and smart speakers from Amazon, Apple, Google and Microsoft have been subject to charges of eavesdropping from the vendors in question. As organizations embrace tools like

Consumer-grade apps on smartphones and other endpoints may leak data through vulnerabilities or undisclosed backdoors.

Alexa for Business in meeting rooms, what's the potential for malicious apps that record and exfiltrate meeting conversations? Or secretly stream the conversation in real-time to a remote location? The same challenges potentially apply for an Apple HomePod in the home office of high-ranking executives or consultants with access to sensitive and confidential business data. Can such trusted devices be used as a new vector of industrial espionage and theft of intellectual property?

Dynamics of Protecting Endpoints

Understanding the current dynamics in endpoint usage and the security threats deployed against endpoints is essential in embracing appropriate security solutions. We see the following dynamics at play.

GROWING VOLUME AND COMPLEXITY OF THREATS

Ransomware, malware, phishing attempts and other types of cyber attacks continue to grow in volume and complexity. The AV-Test Institute says more than 350,000 new malicious programs or unwanted apps are registered every day. Trend Micro documented an almost 80 percent growth in ransomware attacks in the first half of 2019, and other threat research has pegged it more than twice as high. The Webroot Threat Report found that phishing attacks increased by 640 percent during 2019, and almost 95 percent of malware was unique to a given endpoint. Other research found that 80 percent of successful cyber attack incidents on endpoints were from new or unknown threats, and that 70 percent of successful breaches begin with an endpoint. The implication is clear: in the face of advanced, emerging and unique threats, effective protections for endpoints are essential.

GROWING DIVERSITY IN ENDPOINTS

The endpoint moniker used to refer solely to desktop and laptop devices supplied by the organization. Now, however, "endpoint" covers a growing diversity of device types and form factors, such as smartphones, USB thumb drives, smart speakers, home computers, tablets and IoT devices, many of which have not been engineered with strong security in mind. Add new operating systems, ownership models and global geographic mobility in the mix, and these new categories of endpoints offer fewer protections against greater risks.

FEWER SECURITY SIGNALS

Smaller form factor endpoints, such as smartphones and tablets, are engineered to optimize every pixel, and by implication display fewer security warning signals to the user. For example, email addresses are often shown in summary form on smartphones, displaying the full name of the apparent sender but hiding the fact that it is an incorrect, impersonated, or falsified email address. Users require additional safeguards to minimize the likelihood of overlooking the obfuscated warnings.

DEALING WITH LOG DATA

Every endpoint across the IT infrastructure generates event log data. This data is critical to ensure that IT and security teams can understand all of the security-related and other events that occur across the IT infrastructure. Security analysts, threat researchers, and others access log data from SIEMs, EDR systems, firewall and other solutions for a variety of purposes, including investigating alerts of anomalous activity that could signal a cyber attack or a data breach, conducting forensic analysis to determine how an attack occurred after-the-fact, understanding who is logging into a network or accessing data, etc.

However, as necessary as log data is, there are a number of problems in using it, and even more problems in using it efficiently and effectively:

- **Endpoints create lots of log data**
  Because every event triggers a log file entry, one source estimates that a 1,000-user organization will generate in excess of 110 gigabytes of log file data per

Every endpoint across the IT infrastructure generates event log data. However, as necessary as log data is, there are a number of problems in using it, and even more problems in using it efficiently and effectively.

day. That means that if log files are kept for just 90 days (not advisable to keep them only for this long), that translates to almost 10 terabytes of data that will need to be stored over just a 90-day period. Such enormous volumes of data can make it extremely difficult for security staff members to process it effectively.

- **Log files are noisy**
  Log files contain enormous volumes of data that represent normal and acceptable events like users logging in to endpoints or applications, data sources, etc. In fact, most log data is completely innocuous and is just routine stuff.

- **There are large numbers of log files**
  There are hundreds of different types of log files generated by a large number of different endpoints across the typical enterprise. It's difficult to process log file data from so many different sources, and so to be used effectively this data must be aggregated so that it's more useful to security staffers.

In fact, log file management can become so onerous that many organizations simply won't use log files because of the difficulty associated with doing so.

INEFFECTIVE ENDPOINT SECURITY IS COSTLY

When endpoint security fails and a data breach occurs, the resulting financial, reputational and regulatory costs are high, with multiple research studies pegging the cost in the millions. But ineffectiveness extends beyond breach conditions alone, encompassing time wasted by security professionals in responding to fallacious security alerts, manually updating patch levels, and discovering and protecting unsanctioned endpoints. Current endpoint security tools are ineffective when they fail to identify and contain advanced and emerging threats, and also when they lack capabilities to support security professionals in doing their jobs.

MULTIPLE POINT SOLUTIONS FOR ENDPOINT SECURITY CREATE FRAGILE CONDITIONS

Loading endpoints with multiple agents for yet another endpoint security point solution creates degradation in device performance, atrophy in threat detection quality, and conflict in threat signal handling. Recent research concluded that two percent of endpoint security agents failed every week, and that a high number of endpoints were unprotected at any given time due to such failures.

Loading endpoints with multiple agents for yet another endpoint security point solution creates degradation in device performance.

NEW ENDPOINTS BYPASS IT SECURITY CHECKPOINTS

Although IT departments may have high-quality processes for assessing new endpoints for security threats, many endpoints circumvent these checkpoints due to overzealous employees bringing new productivity devices with poor security settings into the organization. Non-assessed endpoints weaken the security defenses of any organization, creating conditions for unknown threats to operationalize outside of the purview of security teams.

NEWER ENDPOINTS FREQUENTLY USED BEYOND THE CORPORATE NETWORK

Many of the newer categories of endpoints are designed to facilitate productive work by employees beyond the physical confines of corporate office space, meaning that the percentage of overall corporate data traffic that flows through current perimeter security protections is shrinking. For example, mobile devices that connect directly to corporate-sanctioned cloud services ignore long-standing network and perimeter security defenses, particularly if the connection is enabled by free wireless networks on the train, at client sites and in cafes.

Expectations of Changing Threat Dynamics

Are current endpoint and other security solutions effective at preventing threats from impacting corporate networks? Overall, not really, as shown in Figure 2.

Figure 2
Effectiveness of Current Security Efforts Against Various Threats

Threat	Minimally Effective	Somewhat Effective	Effective
Known malware	0%	17%	83%
Access to endpoint data by unauthorized parties	1%	28%	71%
Ransomware	2%	29%	69%
Phishing attacks that contain malicious links	2%	33%	65%
Infected USB drives	5%	37%	59%
IT-approved IoT devices on your network used to deliver attacks	3%	39%	58%
Unpatched vulnerabilities	1%	41%	57%
Phishing attacks containing malicious attachments	1%	42%	57%
Employees' IoT devices on your network used to deliver attacks	5%	38%	57%
Drive-by downloads from web surfing	3%	40%	57%
Phishing attacks weaponized post-delivery	2%	41%	56%
Living-off-the-land threats	3%	43%	54%
Advanced malware (e.g., polymorphic, multi-stage)	2%	46%	52%
Persistent and hidden threats	2%	46%	52%
Compromised software patches and updates	4%	45%	51%
Zero-day malware	1%	49%	50%
Fileless attacks	2%	49%	49%
Threats that come in via social media	5%	46%	48%
Employees' personally owned mobile devices introducing threats	5%	50%	45%
Malicious insiders stealing data	8%	50%	42%

Source: Osterman Research, Inc.

Are current endpoint and other security solutions effective at preventing threats from impacting corporate networks?

Here's where we see things changing in the endpoint security space during the near- and mid-term:

- The essential notion of a corporate network is becoming redundant, as core IT services, data repositories, and applications are outsourced across multi-vendor cloud services. An increasing proportion of corporate data traffic is bypassing network security infrastructure in favor of direct connectivity between endpoints and a plethora of cloud services. Under such an architectural approach, security has to move closer to the endpoints and each of the connected services, with a consolidated reporting and analytics layer to assess threats across a diverse data estate and enable security professionals to respond appropriately.

- Cyber attackers using ransomware are beginning to increase the pressure on compromised targets by embracing a different approach. Initially the threat was "pay the ransom or lose your data forever," but this is often ineffective at gaining a ransom payment because many organizations refuse to pay the ransom on principle. Attackers are transitioning to a more lucrative business model: "pay the ransom or we will publish your data" - and by implication, create a data breach situation that attracts regulatory investigation and inflicts financial damage through reputational loss.

- Every new device type and category introduces new security threat vectors, opening avenues for cyber attacks to cause disruption and loss. For example, compromising the operational technology endpoints that power smart buildings would enable an attacker to manipulate people's movements within a building, potentially creating life-and-death situations as the building turns against its inhabitants. Compromising the air conditioning systems to introduce weaponized air flow is a related example. We have already seen some early attempts of compromised industrial infrastructure being manipulated to cause loss of human life, and those same threat playbooks could potentially be leveraged against office buildings.

Solutions to Consider for Improving Endpoint Protection

A multitude of solutions are available for improving endpoint protection, and as a critical enabler of productivity on one hand and a growing vector of compromise on the other, having appropriate protections in place is essential. We see the following solutions as core to improving endpoint protection.

PEOPLE, PROCESS AND TECHNOLOGY

Seeking to improve endpoint protection requires giving attention to the three complementary strands of people, process and technology. The dynamic interplay between these three enables strong protections for endpoints; attempting to wing it on only one or two will be ineffective.

- For **people**, expertise is required in operating whatever technology solutions are deployed, and this requires cyber security professionals to embrace the learning curve through formal and informal training. Many current cyber security professionals are already overworked, stressed and under huge pressure, so fueling motivation to learn something new will be essential. Solutions that supplement, complement, and augment current cyber security talent with automated security methods, playbooks and mitigations will provide structural benefit to organizations and current security staff. If current staff lack the bandwidth to tackle endpoint security, consider partnering with a Managed Services Provider for security services instead.

- The **process** strand of the three enshrines new security technology and behaviors in organizational processes. Enterprise risk assessment is one example of a process, where an understanding of the nature of current threats against endpoints is matched with current solutions in order to identify the outstanding gaps between the two. Another process is focused on the approach and regularity for reviewing security alerts and warnings, along with response times for taking action on critical incidents. Incident discovery processes may be handled internally or via an agreement with a Managed Services Provider for security, and making the decision between the two - or embracing a curated mix of both - is part of defining the process. Other processes include the adoption strategy for making security part of the culture for staff, offering relevant security awareness training (see below), and policy changes to encourage good security behaviors and dissuade the risky ones.

Every new device type and category introduces new security threat vectors, opening avenues for cyber attacks to cause disruption and loss.

- Finally, the **technology** component offers a wide array of potential security protections for endpoints. It's easy to spend money acquiring new technology options, but without corresponding capability improvements in the people and process components, little value will be created. Spending anything on security protections that are poorly used and don't align with the business threat landscape is a waste of financial investment, human capital, and the already stretched energy of cyber security professionals.

ENDPOINT PROTECTION PLATFORMS (EPP)

EPPs offer an integrated collection of capabilities for protecting endpoints, covering different solution areas that were originally brought to market as point solutions. The roster of usual capabilities spans anti-virus, URL filtering, baseline endpoint prerequisites, vulnerability analysis and resolution, visibility into and control over endpoint encryption settings, and more. Endpoint Detection and Response (EDR) capabilities - see below - are also increasingly integrated with EPP solutions.

An EPP offers capabilities to:

- Monitor, protect and report on all connected endpoints, both on and off the network through agent-based capture of events on the endpoint with submission to the platform for centralized oversight and analysis. The detailed logs from endpoints combined with consolidated analysis in the platform enables early identification of abnormal behavior and emerging threats.

- Automatically resolve security incidents with minimal involvement from cyber security staff. For example, automated playbooks specify how the platform should respond to newly identified and emerging threats on a given endpoint, and how to harden security defenses across the rest. Having a security platform that will automatically deal with as much as possible enables cyber security staff to focus on the higher-level issues, critical threats, and overall strategy of ensuring endpoint protection.

- Detect and enroll newly identified endpoints across the network estate. While written security policies are essential for creating the context of expectation for the introduction of new endpoints, proactive automated discovery is essential.

Organizations are increasingly moving to cloud-based EPPs, thereby eliminating the need for deploying and managing on-premises infrastructure. In addition to the much faster time-to-protection offered by cloud-based EPPs, such services also offer the advantage of a wider set of threat signals from a huge number of global customers from which to develop threat intelligence that can be shared across all customers to thwart new threats. Organizations attempting to go it alone with an on-premises EPP will not have access to the same quality of threat intelligence.

Organizations are increasingly moving to cloud-based EPPs, thereby eliminating the need for deploying and managing on-premises infrastructure.

ENDPOINT DETECTION AND RESPONSE (EDR)

EDR solutions take a different approach to security attacks and threats, by providing visibility into current attacks and threats on endpoints, along with options for remediation across the endpoint estate. EDR doesn't primarily attempt to stop attacks - a role played by solutions under the EPP banner - but rather to analyze emerging threats and supply tools for resolving compromised endpoints and hardening the rest. EDR solutions achieve these outcomes by supplying continuous real-time or near-real-time visibility into what's happening across all connected endpoints, offering early warning signals of abnormal behaviors that betray the real intent of seemingly harmless but obfuscated emerging threats. Once new attack chains are identified, protections can be rolled out to other vulnerable endpoints to decrease the likelihood of further threats landing successfully.

ANTI-VIRUS

Protections against known viruses and malware is important - why get compromised with what's already been seen and mitigated? - but traditional signature-based anti-

virus tools alone no longer offer effective protections. As the quantity of known viruses and malware increases, there's a logistical challenge of keeping all endpoints up-to-date with the latest signatures. Theoretically, at some point, signature files would need to be streamed continuously and in real-time, meaning that any non-connected endpoints would be at risk. Behavior-based profiling of all processes - for both known and unknown viruses and malware - offers a more strategic and lighter approach to ensure threats are mitigated.

For organizations using Windows 10, one potential short-term approach to the anti-virus quandary is to rely on the default anti-virus and anti-malware protections in Windows 10. The budget that would have been spent buying best-of-breed tools can then be invested in creating protections against the newer, advanced and emerging threats that anti-virus and anti-malware are ineffective against.

Finally, while not an endpoint protection method that is deployed on the endpoint itself, cloud-based sanitization via virus and malware checking of inbound and outbound email streams is a very useful wider security protection as part of an overall security strategy.

ANTI-PHISHING

Phishing, spear phishing and CEO fraud (whaling) rely on social engineering to trick people into taking an action that will compromise their access credentials, bypass the security of their endpoint, or inflict direct financial damage on an organization, such as through a rushed payment to a fictitious vendor. All the research reports indicate phishing attempts are increasing in quantity.

With phishing being such a dominant vector for attempting a first compromise of an endpoint or initiating a chain of fraud, a robust anti-phishing solution is a must. Technology helps by analyzing for malicious links and files, impersonated email addresses, compromised supply chain partners, weird behaviors in the creation and use of email rules, and potentially compromised high reputation domains, among others.

ANTI-RANSOMWARE

Ransomware is the scourge of the modern digital age, and anti-ransomware protections on endpoints are essential. Since many ransomware attempts start with phishing emails, phishing protections that cover spam filtering, URL sanitization and deep content analysis for attached documents is a necessary first step. Vulnerability analysis across the endpoint estate and proactive patching based on threat intelligence is a second, as this reduces the attack surface available to ransomware exploits.

WEB BROWSER ISOLATION

Email is the primary delivery mechanism for phishing and ransomware attempts, and the web browser for drive-by downloads, malvertising, loading malicious pages, and more. The browser is a critical piece of end user infrastructure for gaining access to the internet and cloud services, which makes it hard to eliminate. Web browser isolation approaches, however, provide a new model for using a browser that protects the endpoint from any infection or nefarious attack attempts within a browsing session. Instead of using the browser installed on the endpoint for browsing, users connect to a virtual browser in a secured environment away from the endpoint when accessing internet and cloud resources. At the end of the browsing session, the virtual browser is destroyed. Web browser isolation approaches prevent malicious code from jumping from the internet to an endpoint.

LOG FILE MANAGEMENT

Although log files are an integral component of any security infrastructure because they enable security analysts, researchers, etc. to do their work, log files need to be managed efficiently. For example, as noted earlier, log file data can consume multiple terabytes over a short period of time, and so a tool that enables compression of this

Cloud-based sanitization via virus and malware checking of inbound and outbound email streams is a very useful wider security protection as part of an overall security strategy.

content to more manageable levels is useful. In addition, seriously consider log aggregation tools that enable multiple log sources to be consolidated and managed in a single interface, tools that enable remote log auditing, and tools that enable log management for all of the tools in use in an organization.

The latter two points are particularly important given the sudden change of work habits resulting from COVID-19-related work-at-home requirements beginning in March 2020. With almost no warning, millions of employees began working from home, sometimes using their employers' endpoints and sometimes their own, and they began using a number of new tools that they had employed before. As part of a robust security infrastructure, it's essential that remote log auditing is performed to ensure that unauthorized access and data leaks are not occurring.

APPLICATION CONTROL

Enforcing prerequisites on endpoints before being granted access to requested resources helps in two ways: first, potential threats on endpoints are minimized due to regular enforcement actions, and second, any active threats cannot move onto new hosts. Prerequisites can include defining baseline versions of applications, minimum patch levels, and the recency of on-endpoint threat scanning. Whitelisting of applications provides a complementary route for minimizing the threat surface on endpoints; whitelisted applications – subject to baseline versioning and patch levels – are permitted to execute, while everything else is blocked by default.

MULTI-FACTOR AUTHENTICATION (MFA)

Strong multi-factor authentication (MFA) of accounts constrains the ability of cyber attackers to easily take compromised credentials and get access to systems and accounts they should not have access to. Several MFA methods, such as SMS code and even app-based Authenticators, have been compromised in various attacks - making the selection of the type of MFA used critically important. The best options for MFA currently rely on a trusted hardware key, aligned with the FIDO2 standard.

PATCH MANAGEMENT

Rapidly deploying new patches for the operating system and apps on endpoints reduces the attack surface available to cyber attackers. Unpatched endpoints are an attractive first point of call to launch an attack, and from which to move deeper into the network. Automated tools that roll out prioritized patches - both proactively and when an endpoint is identified that is out of tolerance - is the only way to go; manual patching is a losing proposition.

Be aware that cyber attackers have found some success in compromising patch streams from vendors, because doing so quickly spreads compromised software across a wide swarth of endpoints across multiple organizations. Several security vendors offer centralized management of all updates for endpoints, creating and maintaining a single trusted library of verified updates.

VULNERABILITY ANALYSIS

Consolidated reporting, insight and querying capabilities across all endpoints enables proactive and automated end-to-end search for vulnerable applications. Correlating an up-to-date endpoint-wide inventory of applications with current threat intelligence highlights the in-situ vulnerabilities with the highest threat levels, enabling prioritization by security professionals of tasks to harden security defenses. Vulnerability analysis plus threat intelligence ensures the most critical vulnerabilities are resolved first, giving clear signals on where current threats are the hottest.

An emerging idea is virtual patching of vulnerabilities, in advance of actual patches being released by the application's vendor. Under this approach, the endpoint security toolkit erects protections that prevent vulnerabilities from being exploited; while the vulnerabilities themselves persist in the native application or operating system, added security defenses neutralize any attempted attacks.

Rapidly deploying new patches for the operating system and apps on endpoints reduces the attack surface available to cyber attackers.

SECURITY AWARENESS TRAINING

Provide educational resources to inform and equip executives, managers and employees to be aware of common attack methods, along with the risks of unsafe IT behaviors. Simulated phishing attacks, among others, complement this educational approach to gauge threat vulnerability levels among staff. Security awareness training has a broad role to play in strengthening security safeguards, but in context of endpoints specifically, should include topics around the risks of using consumer-grade messaging applications for work purposes, why and how to avoid free public Wi-Fi networks when on the road, and in BYOD environments, the benefit of buying smart endpoints with secure chipsets to reduce the risks of malicious on-device behavior.

BACKUP AND RECOVERY

Endpoints will get compromised, but that shouldn't mean that unique business data is irretrievably lost. Applications should be able to be re-deployed to a new endpoint, along with connections to file shares, SharePoint environments, cloud repositories, and enterprise databases. No data should be uniquely stored on an endpoint, but if that is the case, ransomware-resistant backup and recovery approaches will be essential. Connected hard drives and even network shares don't always work for this, as these are increasingly being targeted by ransomware as well. Cloud backup services with multiple restore points currently offer the best protection.

It's also important to be able to restore the entire Active Directory infrastructure down to the operating system level if a compromised endpoint leads to a total destruction of that infrastructure. A case in point for what can go wrong in the absence of an appropriate backup strategy is A.P. Møller-Maersk following its takedown from a NotPetya attack in 2018. As noted in a good article on the topic:

Early in the operation, the IT staffers rebuilding Maersk's network came to a sickening realization. They had located backups of almost all of Maersk's individual servers, dating from between three and seven days prior to NotPetya's onset. But no one could find a backup for one crucial layer of the company's network: its domain controllers, the servers that function as a detailed map of Maersk's network and set the basic rules that determine which users are allowed access to which systems.[1]

The bottom line is that the entire Active Directory infrastructure must be properly backed up to avoid potentially catastrophic results as was the case with Maersk.

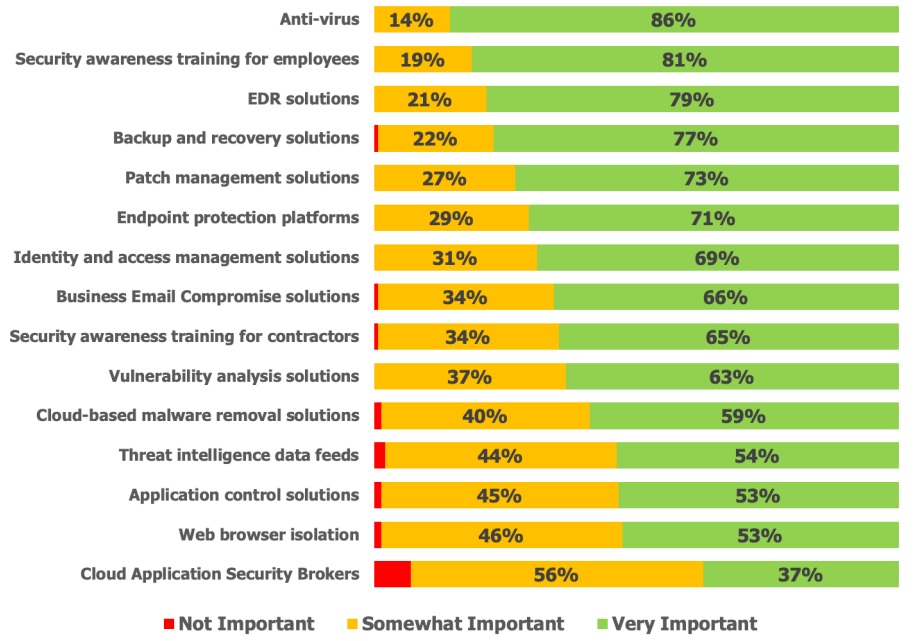
Endpoints will get compromised, but that shouldn't mean that unique business data is irretrievably lost.

WHAT'S IMPORTANT TO DECISION MAKERS?

Our research discovered that many decision makers and influencers are still focused on more traditional endpoint solutions, such as anti-virus solutions, as an important defense against threats. However, as shown in Figure 3, decision-makers and influencers are also heavily focused on newer and more innovative methods and platforms for endpoint protection, including security awareness training, EDR, backup and recovery solutions (to recover from ransomware and other infections), patch management and EPP solutions.

[1] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Figure 3
Importance of Various Endpoint Capabilities



Source: Osterman Research, Inc.

Summary

Endpoint protection must be a key component in an overall security strategy, but can only be one strand complemented with cloud security, network security, and physical security, among others. An overall security strategy should be created and defined in light of an enterprise-wide risk assessment for the organization.

Sponsor of This White Paper

Quest InTrust is a smart, scalable event log management tool that enables you to collect and store all native or third-party logs from various systems, devices and applications in one, searchable location with immediate availability for security and compliance reporting. Get a unified view of Windows event logs, UNIX/Linux, IIS and web application logs, PowerShell audit trails, endpoint protection systems, proxies and firewalls, virtualization platforms, network devices, custom text logs.

With Quest InTrust, you can even protect your workstations from modern cyberattacks, such as pass-the-hash, phishing or ransomware, by monitoring all user workstation activity — from logons to logoffs and everything in between. InTrust will watch for unauthorized or suspicious workstation activity, such as file creation beyond threshold limits, using file extensions of known ransomware attacks, suspicious process launches or fishy PowerShell commands. Real-time alerts enable you to respond immediately with automated response actions, like blocking the activity, disabling the offending user, reversing the change and/or enabling emergency auditing.

And don't worry about turning native auditing on. InTrust enables you to collect and store years of data in a highly-compressed repository, 20:1 with indexing and 40:1 without, so you can save on storage costs by up to 60%, satisfy data retention policies and ensure continuous compliance with HIPAA, SOX, PCI, FISMA and more.

Quest

www.quest.com
@Quest
+1 800 306 9329