PROTECTING THE ENDPOINT

Next-generation solutions help organizations keep pace with advanced threats against their far-flung IT assets.

EXECUTIVE SUMMARY

The world of end-user computing has undergone a dramatic transformation over the past five years. The use of mobile technology to access digital resources surpassed desktops as users embraced the convenience and accessibility of mobile devices. This diversity of endpoints creates challenges for IT security specialists who now must track and remediate vulnerabilities across smartphones, tablets and notebooks, as well as desktop computers. Today’s threat environment includes extremely sophisticated attackers who will use new forms of malware to compromise these devices and gain access to the information they store. The threat doesn’t stop at the endpoint, however. Once an attacker gains access to a trusted smartphone or tablet, that device may be leveraged to gain access to the broader enterprise network and its stores of sensitive information.

Effectively defending today’s endpoint environment requires a comprehensive set of defensive technologies that rise to the challenge of the modern attacker. Next-generation endpoint protection solutions combine threat intelligence, machine learning and behavioral analysis to combat advanced attacks and protect both the endpoint and the broader enterprise network. Organizations seeking to effectively defend themselves must integrate next-generation endpoint technology within their broader enterprise security strategy. Leveraging this new technology will bolster an organization’s security program and help keep it out of the news as the latest victim of an advanced security breach.
**Endpoint Vulnerability**

Endpoint systems are the most common targets of malicious activity in the modern enterprise computing environment. The proliferation of notebooks, desktops, and mobile devices creates a large attack surface for cybercriminals who need to identify only a single vulnerable system to gain a foothold on an enterprise network. Even as security teams recognize the importance of securing these endpoints from attacks, they find themselves frustrated by the inability of older security products to rise to the challenge. Attackers employ increasingly sophisticated weapons in their cyberwarfare arsenals, and these stealthy tools simply slip under the radar of traditional signature detection technology. Endpoints that lack additional security controls present an appealing target to attackers.

The most sensitive information held by an organization sometimes exists on endpoint devices, but is more commonly found in enterprise data centers operated by an organization or its cloud partners. However, these enterprise systems are heavily fortified against attack by a variety of security technologies deployed in a defense-in-depth strategy. Firewalls, intrusion prevention systems, data loss prevention technology, and other security controls maintain a vigilant watch over these critical systems and their troves of sensitive information. If an organization’s most valuable assets reside inside the walls of the data center, why then do attackers target endpoints?

Vulnerable endpoints offer attackers the opportunity to bypass the layered defenses designed to keep them out of enterprise data centers. By commandeering the notebook of an unsuspecting user, attackers can take advantage of the device’s trusted status on the network — and both the device and the credentials of its users — to gain access to the organization’s most valuable data. This approach has proved to be highly successful at compromising sensitive information. While security architects place extreme importance on keeping outsiders at bay, they often capitulate to the demands of convenient access placed upon them by enterprise users and leave themselves vulnerable to attacks waged through a compromised endpoint device. That’s not a condemnation of the need to balance security and convenience, but simply a fact of life in today’s complex computing environment.

User activity poses one of the gravest challenges to endpoint security. Less than a decade ago, users were accustomed to a highly regimented technology experience controlled by a risk-averse IT department that carefully managed system configurations and software installation. The rapid consumerization of IT changed these expectations, and users now expect the same instant gratification from their office technology that they experience with their personal devices. In fact, many users are able to bring personal devices onto enterprise networks through bring-your-own-device (BYOD) policies. This leads to a loss of control over endpoints by IT security teams and opens the door for inadvertent user errors that could compromise these devices. Users might fall victim to a phishing attack that encourages them to open a malware file that could compromise these devices. Users might fall victim to a phishing attack that encourages them to open a malware file or alter a system configuration setting, unwittingly allowing an attacker access to the system and a foothold on the network. It takes only a single user mistake to jeopardize the security of an entire network.

The sheer amount of software installed on the modern endpoint also creates vulnerabilities that attackers may exploit without even involving an end user. Operating systems and approved software applications all require regular security updates to patch vulnerabilities that might allow an attacker access to the system. Even endpoints that normally reside on a private enterprise network, safely tucked behind a firewall, are vulnerable to attacks as soon as they leave the security of the enterprise network. When a user connects to an airport or convention center Wi-Fi network, the device is exposed to the larger internet and becomes susceptible to attackers scanning for security flaws. An attacker might compromise that system.

**The Threat of Ransomware**

Government agencies, hospitals, financial institutions, and many other organizations suffered ransomware attacks that threatened to cripple their operations in the past year. A study by Osterman Research in June 2016 found that 39 percent of organizations were affected by ransomware during the preceding 12 months. This figure is shocking and underscores the importance of protecting against this and other malware threats to the endpoint.

Ransomware uses encryption, a widely adopted security technology, as an offensive weapon in cyberwar. Once ransomware gains a foothold on a system, it encrypts all of the user data on that system using a strong encryption key, rendering it inaccessible to anyone without the decryption key. Users then see a pop-up window demanding the payment of a ransom to regain access to their information. The Osterman study found that 37 percent of organizations wind up meeting the demands of the data kidnappers and pay the ransom.

Of those that didn’t pay the ransom, 28 percent lost access to files as a result of the attack.

Organizations seeking to protect themselves against the scourge of ransomware should combine next-generation endpoint protection technology with a consistent backup strategy that can restore lost data in the event of an infection.
and then lay low, waiting for the user to return to the office, allowing the attacker access to the private network.

Traditional endpoint protection technology is extremely effective at battling traditional threats. Simple viruses, worms and other malware don’t stand a chance against a standard signature-based anti-virus package. The host-based firewalls integrated into these products block unsolicited network connections, preventing attackers from scanning an endpoint for most vulnerabilities. Encryption technology protects the sensitive data stored on endpoints, rendering a lost or stolen device useless to someone who steals it or finds it in the back seat of a cab. However, this technology is not capable of defending against advanced threats that leverage zero-day attacks, ones that sneak previously undiscovered malware onto a system before security companies can develop effective signatures. While signature detection still plays a vital role in the enterprise security stack, it’s no longer sufficient to keep an enterprise secure.

Fortunately, security vendors now offer next-generation endpoint protection solutions that incorporate advanced technology to mitigate the rising threat posed by sophisticated attackers. These solutions use machine learning, threat intelligence, application control, behavioral analysis and other techniques to detect and respond to threats without depending on a malware signature database. These tools play an important role in enterprise security programs, either when integrated into an existing security solution or added as a stand-alone product.

Machine Learning

The machine learning capabilities of next-generation endpoint protection tools allow them to mine knowledge from vendors’ comprehensive libraries of executable files that include both files that are known to be benign and their malicious counterparts. Machine learning applies data science techniques to these libraries, developing predictive models that allow endpoint protection tools to make judgments about binary files not stored in the library.

Simply stated, machine learning takes the large databases of malware used to generate the signatures for traditional anti-virus software and extracts knowledge about the characteristics of malware. Next-generation tools may then apply this model to new situations, allowing them to detect potentially malicious objects that would easily bypass signature detection due to their novelty. This capability makes machine learning a valuable complement to traditional defensive tools.

Essential Elements of Endpoint Protection

Combating the full range of modern cybersecurity threats requires a combination of defensive techniques. This strategy, known as a defense-in-depth approach to security, is a trusted technique that implements layers of overlapping defensive controls. The principle behind this strategy is to design security infrastructure with the assumption that one or more controls will fail. Security architects following this strategy implement multiple controls designed to achieve the same objective, ensuring that the organization remains safe even if a single control fails.

In the world of endpoint protection, security architects have three main objectives. First, they wish to prevent malware and other exploits from succeeding, granting the attacker access to the system and underlying network. Second, they want to detect malicious activity if an exploit does successfully penetrate their defenses. Finally, they want to be able to remediate and contain any malicious activity that takes place on their networks.

Traditional endpoint protection tools meet these goals for traditional threats. They combine the use of signature-based anti-virus detection, host firewalls and data loss prevention technology to combat endpoint threats. Next-generation endpoint security tools complement these traditional capabilities to help organizations meet emerging security needs and keep pace with the combination of increasingly sophisticated threats and an expanding attack surface. These next-generation tools bring state-of-the-art methods to the world of endpoint protection.

Threat Intelligence

Organizations around the world come under attack by malicious individuals and groups on a daily basis. A typical business sees millions of attempts to penetrate its perimeter defenses each month. Alert administrators may notice some of these attempts and configure firewalls and routers to block inbound traffic from malicious sources, but this manual blocking is a losing game. Organizations simply face too many attackers, and once an organization detects an attack from a particular IP address, the attacker can move to a different system to continue the attack.

Threat intelligence solves this problem by correlating attacker information received from thousands of different sources. Threat intelligence vendors collect attack information from all of their customers, anonymize the data to protect customer privacy, and then use that information to automatically configure the defenses of other customers. As soon as an attacker launches an attack against a single customer, threat intelligence solutions will notice the attack, automatically reconfigure the firewall and share this information with other customers around the world. Threat intelligence brings the power of crowdsourcing to cybersecurity.

Application Control

Application control techniques invert the traditional “detect and block” model of anti-virus tools. Instead of scanning every file on a system and attempting to identify those that carry malicious payloads, application control builds lists of the executable files that...
are permitted on a system and then blocks any application that doesn’t appear on the white list of approved applications.

Administrators have the flexibility to configure application control policies as tightly or loosely as desired. For example, they might configure application control policies on a server to allow only a small set of programs expected to run on that server. At the same time, they might configure application control policies on the desktops of power users to permit them to install any piece of software from a trusted software repository. Application control limits the software that may execute on a system, stopping malware in its tracks without requiring the system to determine that it is actually malicious.

**Behavioral Analysis**

Behavioral analysis techniques step away from the model of determining whether an executable file itself is malicious or benign and instead monitor the actions taken by an application to determine whether they resemble the behavior of an attacker. Over the years, security researchers have developed a strong understanding of the patterns of activity common to attacks. For example, all of the following activity patterns might represent malicious activity on a system:

- A large number of network requests to systems on the local network or the internet might be malware engaging in network reconnaissance or attempting to spread to other systems.
- Configuration changes to sensitive parts of the operating system may be malware attempting to escalate privileges or install itself deeper into the operating system's core.
- Rapid encryption of a large number of files may be a sign of ransomware attempting to encrypt user content before making demands for a ransom payment.
- Exploit prevention techniques step in when other tools fail to prevent malicious software from gaining a foothold on a system. The exploit prevention technologies in next-generation endpoint protection solutions seek to stop malicious code from performing actions that may damage systems or grant access to sensitive information. Effective exploit prevention techniques include:

**Endpoint Protection Deployment Methods**

Security architects implementing next-generation endpoint defenses have two deployment models available to them: traditional on-premises controls and cloud-based Security as a Service. Traditional defenses provide enterprises with a familiar deployment model that works effectively within the confines of their on-premises or cloud data centers. Security specialists within the organization install, configure, maintain and monitor security solutions, allowing them deep access and control over the technology.

Cloud-based endpoint protection deployments are becoming increasingly popular as enterprises turn to service providers who build and maintain the security infrastructure used by their clients. This approach frees enterprise security teams from the burden of maintaining the endpoint protection infrastructure and allows them to focus on adding value within their own organizations by leveraging a best-of-breed product managed by the vendor.

Both on-premises and cloud deployment models offer different advantages. Organizations that choose an on-premises deployment retain a high degree of control over their security infrastructure while those that opt for cloud deployments choose to hand some of this control over to a vendor, freeing themselves of the associated maintenance burden.

Host firewalls that prevent malware from accessing other systems located on the local network
Web content filtering that analyzes code on web pages requested by end users and blocks access to pages that contain potentially malicious software
Intrusion prevention systems that monitor network traffic for signs of malicious activity and block the traffic before it reaches other systems on the protected network; these intrusion prevention technologies can be applied both at network chokepoints to prevent malicious traffic from entering the network and on endpoints to block lateral traffic that originates from infected systems that are already behind the network perimeter.

These exploit prevention techniques offer effective ways to stop malware that has already gained access to an organization’s network from spreading and carrying out malicious activity.

Threat Analysis
Unfortunately, even the most advanced endpoint protection technologies sometimes fail to prevent a successful attack. When an attack does succeed against an endpoint, security response teams require rapid access to information about the threat and its impact on endpoint and network security. Endpoint detection and response technology provides this threat analysis, rapidly collecting information about attacks while they are in progress and providing an assessment of the extent of the infection. EDR tools are the reactive component of a next-generation endpoint solution, allowing incident responders to quickly determine the extent of the compromise, evaluate the potential for data loss and restore normal operations as quickly as possible.

Next-generation security solutions provide organizations with the tools necessary to defend their enterprise endpoints against attack in today’s increasingly dangerous threat environment. The use of techniques such as machine learning, threat intelligence and behavioral analysis provides security professionals with the tools and information that they need to take an analytic approach to detecting security threats that would escape the notice of signature-based detection systems.

Integrating Next-Generation Endpoint Protection into a Comprehensive Security Strategy
There is no silver bullet when it comes to cybersecurity. No single security solution is a panacea that will meet all security needs, and next-generation endpoint protection solutions are no exception. These tools play an important role in a comprehensive enterprise security strategy but must be carefully integrated with other security technologies. This integration allows security tools to share information and work together to identify, prevent and eradicate threats that arise on the network. This collaborative approach to security enhances an organization’s ability to protect endpoints and preserve the confidentiality, integrity and availability of critical information.

The major challenge to achieving this collaborative integration is clear: Many organizations adopt security tools from different partners that do not offer native integrations. The only way to tie these disparate tools together is to feed all of their results to a security information and event management (SIEM) solution. A SIEM solution is capable of understanding the log format of each technology used by the organization, perform correlation and then instruct these tools to take appropriate response actions. This represents a major challenge for many organizations, especially those without dedicated IT security teams.

Fortunately, enterprises seeking to build a security strategy that tightly integrates information from a variety of sources have an alternative at their disposal. Instead of choosing different security products from a variety of vendors, they may choose to adopt a single-vendor approach to security, in which the enterprise identifies a preferred vendor and then implements as many security technologies as possible from that vendor. In addition to achieving many operational security benefits, this approach also tends to reduce costs by allowing the enterprise to use bundling and volume discount programs that provide reduced prices or complementary features as part of a bulk purchase.

From an operational perspective, using a single vendor provides the opportunity to leverage that vendor’s management console for the deployment, monitoring and ongoing maintenance of the vendor’s security controls throughout the enterprise.
Security analysts achieve a “single pane of glass” approach to management that allows them to view the security status of all of their systems within a single application. This improves the efficiency of security operations and increases the likelihood that analysts will spot security issues before they escalate.

Consolidating security controls onto a single platform also increases the ability of these tools to share threat intelligence information both internally and externally. Tools operating on the same platform can share information with each other about potential threats, allowing automated correlation of event data as a threat attempts to penetrate enterprise defenses.

These tools can also all benefit from external threat intelligence information that is provided by the vendor and fed directly into the management platform for shared use.

Finally, organizations that take the preferred vendor approach are likely to see a reduced false-positive rate as the different technologies available on that platform share information with each other. For example, an intrusion detection system might notice that an endpoint faces an inbound attack aimed at exploiting an operating system vulnerability that is correctable with a vendor-supplied security patch. When evaluating this threat, a consolidated platform can draw on information from agents installed on that endpoint to determine whether the required patch is present. If the system has the patch installed, administrator action is unnecessary, and the system can safely ignore the attack. In an environment that lacked this information-sharing capability, the intrusion detection system would have to assume that the endpoint was vulnerable to the attack and alert administrators to the attempt, triggering a time-consuming and annoying false-positive alert.

Enterprises seeking to take a comprehensive approach to their cybersecurity strategy should seriously consider the benefits provided by leveraging multiple security technologies from a single vendor. The improvements in management capability, information sharing and false-positive reduction allow organizations to respond to breaches more quickly and effectively. This is a critical capability in the modern cybersecurity environment where breaches are almost inevitable.

CDW: A Security Partner That Gets IT

CDW’s solution providers serve as your organization’s security partner. The CDW team offers a variety of security services that will help any organization improve its security posture. CDW’s account managers and solution architects stand ready to assist you in every phase of your project. They will guide you through the selection of next-generation endpoint security tools that will protect your organization in today’s sophisticated threat environment and then assemble the resources required to help you successfully complete your implementation project.

CDW takes a comprehensive approach to identifying and meeting the needs of every customer. Each engagement includes five phases designed to help you achieve your security objectives in an efficient, effective manner. These phases include:

- Initial discovery session
- Assessment review
- Detailed manufacturer evaluations
- Procurement, configuration and deployment
- 24/7 support

In addition to assisting with the design and implementation of security solutions, CDW security experts are available to perform a wide range of security assessments.

To learn more about how Trend Micro’s security products deliver protection for endpoints and other IT assets, visit CDW.com/TrendMicro

To find out more about CDW’s security solutions and services, visit CDW.com/security