WHITE PAPER

CDW PEOPLE WHO GET IT™

DEFENDING THE ENTERPRISE AGAINST ADVANCING THREATS

A new generation of cyberthreats can overcome traditional security measures, but advanced tools can minimize their danger.

EXECUTIVE SUMMARY

In today's cybersecurity climate, traditional security solutions such as anti-malware and firewalls are essential, but alone they aren't sufficient to protect against the most advanced threats. **Organizations need to implement toolkits that allow them to identify, analyze and respond to attacks quickly, even stealthy ones.** This collection of resources must be able to identify problems early — even those that are difficult to detect, such as advanced persistent threats and zero-day attacks — so that they don't become breaches. Every organization's goal is to limit the time a cybercriminal is in the environment, poking around.

The solutions that can provide this defense include network traffic analysis and forensics; payload analysis; and endpoint analysis and forensics. These tools are critical in today's security climate. Effective cybersecurity has become a necessity that enables organizations to maintain operations even in the face of advanced threats. Organizations that establish a proactive security capability give themselves a significant advantage over their competitors.

Advancing Threats

For years, information security teams have built a series of familiar controls designed to protect against familiar threats. Firewalls, anti-malware software and intrusion detection systems all successfully kept most attackers at bay. But the threat landscape has evolved significantly, with sophisticated attackers and attack techniques appearing on the scene. While enterprises should not neglect traditional security controls, they must consider technologies and measures that protect against these more sophisticated threats.

These new attackers, known as advanced persistent threats (APTs), represent a major risk to cybersecurity. APTs earned their name because they leverage advanced attack techniques in a deliberate manner, focused against well-defined targets. Unlike casual attackers who simply seek undefended targets of opportunity, APTs select their targets based on specific intelligence gathering or system disruption objectives. They then conduct reconnaissance against those targets and level precise, targeted attacks designed to achieve their objectives quickly, efficiently and stealthily.

APTs are typically well-funded efforts organized by governments, military organizations and nonstate actors, such as organized crime. They hire talented engineers and cybersecurity experts who develop customized attacks that exploit previously unknown vulnerabilities. Known as zero-day attacks, these are especially insidious for two reasons: First, because they are unknown, vendors have not yet released patches to correct them. Second, signature-based detection systems are powerless to identify them because there are no signatures for these unknown attacks.

The percentage of information security professionals who consider themselves "very familiar" with advanced persistent threats[1]

A recent study by the Ponemon Institute and the Information Systems Audit and Control Association (ISACA) provided stark statistics about the preparedness of enterprises to respond to APT attacks. While 49 percent of enterprises surveyed considered it "very likely" that they would be the targets of an APT, only 15 percent stated that they were "very prepared" to deal with an APT attack. Organizations seeking to respond to APTs need an effective toolkit in place that will allow them to quickly identify, analyze and respond to sophisticated cyberattacks. These capabilities will limit the disruptions caused by attacks, allowing organizations to get back to business quickly.

Network Traffic Analysis and Forensics

APTs typically find their way into enterprises over a network connection, making the network a fruitful source of data for security professionals seeking to identify APT intrusion attempts. Network traffic analysis assists these efforts in two ways. First, by developing models of normal network activity, network traffic analysis systems may identify deviations from those norms representing suspicious activity that requires further investigation. Second, network analysis tools may monitor the network for traffic patterns known to be associated with APT attacks, such as anomalous domain name system queries that may indicate a botnet infiltration.

Network analysis tools leverage global threat intelligence information gleaned from a vendor's deployed base of customers around the world. This information helps fine-tune threat analysis and reduce false positive reports that irritate administrators and reduce the effectiveness of security programs. These tools also use dynamic file analysis technology to block known malware, as well as files or communications that violate enterprise security policies. When the tool detects an anomaly, it may quickly get deep visibility into the activity and behavior of the threat and rapidly respond to contain an active attack.

Products such as Cisco Systems' Advanced Malware Protection for Networks offer valuable insight into potentially malicious activity on the network. AMP combines dynamic file analysis and global threat intelligence to quickly pinpoint attempted network intrusions and provide security administrators with the tools they need to conduct thorough investigations in the event of a suspected breach.

THE THREAT OF STEALTH

One of the most damaging characteristics of APT attacks is their ability to remain undetected for long periods of time. Media reports abound of large organizations that have suffered sophisticated attacks, but only detected them weeks or months after intruders infiltrated their networks and systems. These attacks are particularly dangerous because they provide the perpetrators with ongoing access to sensitive information as well as the ability to cover their tracks and disrupt security efforts that might detect the infiltration.

In May 2015, the Ponemon Institute released a research report studying APT attacks against the retail and financial services industries. The study revealed that breached retailers took an average of 197 days to identify an APT intrusion, while financial services firms took 98 days to detect an attack. Once they detected attacks, firms in both categories took approximately a month to contain the damage: 26 days for financial services firms and 39 days for retailers. That's a dangerously long period of time for a network to remain compromised.

[1]**SOURCE:** Ponemon Institute and Information Systems Audit and Control Association, "2014 Advanced Persistent Threat Awareness Study Results," January 2014

In the case that preventive controls fail and an intrusion takes place, the network also provides an effective source of information for forensic analysis. Enterprises seeking to leverage network forensics may implement tools designed to perform full packet capture and storage of network traffic. They later use this with analytics and reporting tools that support incident response, reducing the time required to respond to an incident by reconstructing flows and events that took place over a period of days or weeks. These tools also provide the detailed forensic reports required to respond to regulatory requirements.

Network forensic analysis is a highly specialized field and may place a heavy demand on computing resources because of the large amount of data that must be processed. Therefore, enterprise security teams often turn to specialized solutions to meet these needs, such as Blue Coat's Security Analytics Platform or RSA Security Analytics. Both of these tools provide the network traffic capture, analysis and reporting environment required to wage an effective security incident response effort.

Payload Analysis

Older malware detection systems rely on the use of signature detection technology that monitors systems for known patterns of malicious activity. Anti-malware vendors update massive databases with new signatures on a daily basis, attempting to stay ahead of the huge quantities of new malware strains released into the wild each day. It's simply impossible to use this technique against the zero-day exploits used by APT attackers. After all, if an attacker is using a new attack against an organization, anti-malware vendors simply haven't seen it, so they don't yet know to put it in their signature databases.

Payload analysis systems step in where traditional malware detection techniques fail. When a suspicious file enters an enterprise network, payload analysis systems quarantine it for further review, either in an on-premises appliance or in the cloud. The system then launches the suspect file in a sandboxed environment where it may execute freely but does not have access to any other network resources. The analysis system then monitors the activity that takes place within the sandbox, watching for any signs of malicious activity. Administrators may then configure responses, optionally blocking suspect files or flagging them for further review.

FireEye's Adaptive Defense platform, Palo Alto Networks' Wildfire system and Trend Micro's Deep Discovery product line all perform payload analysis on suspect content to enhance enterprise security postures. These products combine sandboxing and activity analysis with global threat intelligence to quickly identify new threats and share that information across their customer base without compromising confidential client information. Adding a payload analysis platform fills a critical gap in an enterprise cybersecurity program.

Endpoint Behavior Analysis and Forensics

In addition to analyzing network traffic and performing payload analysis, security solutions may also analyze endpoint behavior to contain application-based threats. These endpoint behavior analysis solutions leverage agents on each endpoint to directly interact with the system configuration and perform memory and process monitoring to block attacks, isolating suspect applications and files in virtual containers where they can't reach other system resources.

Endpoint behavior analysis solutions reach deep into the monitored system to intercept kernel system calls and block malicious activity, such as thread injection attacks. They can isolate web browsing sessions within containers to protect users against malicious websites, including those hosting drive-by download and watering hole attacks that target users by hosting malicious content on trusted, uninvolved third-party websites. While quite effective when deployed across an enterprise, this agent-based approach may be difficult to implement in far-flung mobile environments, particularly those that support bring-your-own-device policies.

RSA's ECAT endpoint threat detection is one example

SHOCKING TEST RESULTS

FireEye recently released a report analyzing data gathered during 1,614 proof-of-value deployments of the company's technology in enterprises around the world. These deployments installed FireEye technology behind other security defenses to gain a view of the effectiveness of existing controls. The results showed shocking lapses in enterprise security.

Almost every organization deploying these controls experienced a breach during the test period; only 3 percent successfully completed the trial without a breach. In more than a quarter of organizations studied, the breaches were consistent with the patterns used by APT actors. More than 75 percent of organizations had systems that were actively engaged in command-and-control communications with external systems, indicating an active breach possibly exfiltrating sensitive information.

The threat posed by APTs is real and widespread, and it targets a wide variety of organizations. **Government agencies** and **military organizations** might expect to come under fire by APTs, but the FireEye study found active breaches in many diverse industries, including agriculture, transportation, healthcare, entertainment, education and retail.

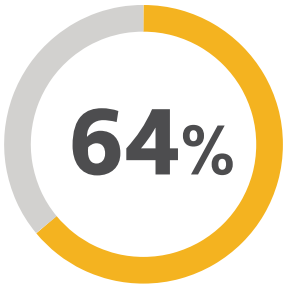
→ To learn more about dealing with sophisticated cyberattacks, read the CDW blog post "Reducing the Risks of Advanced Persistent Threats."

of an endpoint behavior analysis system. ECAT blocks zero-day attacks, provides basic forensic capabilities and protects systems from APT attacks both on and off the enterprise network. ECAT allows enterprises to detect APT attacks without relying on outdated signature detection technology.

In the event of a security incident, investigators often turn to endpoint systems to gather critical intelligence to help reconstruct the attacker's activity. Endpoint forensics tools, including the Bit9 + Carbon Black platform and FireEye Endpoint Forensics, automate incident response efforts by continuously monitoring endpoints, whether they are located on local or remote networks. These tools can quickly sweep through a large number of endpoints, remotely detecting signs of malicious activity, collecting live memory contents and other forensic data, and providing an investigation platform that yields quick answers to incident-related questions.

CDW: A Security Partner That Gets IT

CDW's solution providers are available to serve as your organization's security partner. The CDW team offers a variety of security solutions that will help you improve your security posture. CDW's account managers and solution architects are familiar with advanced threats and the latest security tools. They bring decades of cybersecurity experience to the table and hold elite security certifications. Our security staff stands ready to assist you in every phase of your project as you select and implement advanced threat protection solutions.



The percentage of security professionals who believe that technologies that isolate or sandbox malware infections are most likely to stop APTs[2]

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 telephone support

In addition to assisting with the design and implementation of security solutions through partnerships with major vendors, CDW staff are available to perform a wide range of security assessments.

To learn more about CDW's security solutions, contact your CDW account manager, call 800.800.4239 or visit CDW.com/security.

YOU and CDW

Bit9+ CARBON BLACK
ARM YOUR ENDPOINTS.

The Bit9® + Carbon Black® Security Solution is an integrated Endpoint Threat Prevention, Detection and Response solution. The solution consists of two industry-leading products and the Threat Intelligence Cloud. Independently, each product is a leader in its category. Together, they provide security and risk professionals with an advanced threat protection solution for Windows®, Mac® and Linux® endpoints and servers.

CDW.com

TREND MICRO™

At the heart of the Trend Micro™ Custom Defense solution, Deep Discovery uniquely detects and identifies evasive threats in real-time, then provides the in-depth analysis and actionable intelligence needed to discover, remediate and defend against targeted attacks.

CDW.com/trendmicro

Cisco® provides one of the industry's most comprehensive advanced threat protection portfolios of products and solutions. The threat-centric and operational approach to security reduces complexity, while providing outstanding visibility, continuous control, and advanced threat protection across the extended network and the entire attack continuum.

CDW.com/cisco

CDW® PEOPLE WHO GET IT™

[2]**SOURCE:** Ponemon Institute, "Advanced Threats in Retail Companies: A Study of North America & EMEA," May 2015