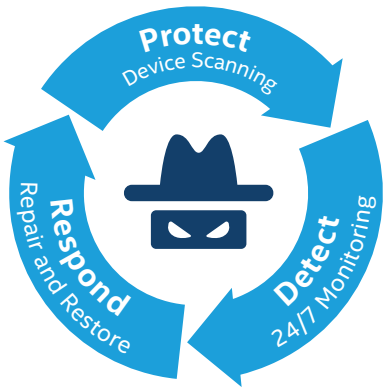
BRIEF

May 2019

IT@INTEL

Advanced Persistent Threats: Hunting the One Percent

> "The threat landscape is constantly evolving and becoming more sophisticated, which means we have to do all we can to protect our assets, plans, and data from being leaked, compromised, or stolen."
>
> **—Brent Conran, Chief Information Security Officer, Intel IT**



Executive Summary

What if a homeowner took a month to notice that a burglar was living in the extra bedroom? That seems unlikely, and yet, essentially that is often what happens when an advanced persistent threat (APT) infiltrates an enterprise. A 2018 Ponemon Institute study revealed that U.S. companies took an average of 197 days to detect an APT intrusion.[1]

Intel IT is committed to improving our ability to rapidly identify, contain, and remediate APTs—network attacks characterized by stealthy, unique malware designed specifically for the target environment. APTs constitute a small but highly destructive percentage of the information security threats that are continuously monitored.

Our approach to APTs is characterized by two important concepts.

First, we are shifting from actively watching for negative events to operationalizing the containment of such events through the use of intelligent software agents. We are building an information security architecture that we can trust to successfully contain 99 percent of the attacks that occur.

Second, operationalizing the containment of 99 percent of threats frees us to hunt for and address the one percent of them that make it through our defenses. We are using groundbreaking technology, such as machine learning algorithms for anomaly detection and pattern analysis, to identify APTs in our environment.

A typical goal of APTs is to steal data, which is one of Intel's most valuable assets. Our approach to information security is designed to protect that data to the best of our ability and in the most efficient way possible.

Table of Contents

Business Challenge

Today, the world is experiencing a tidal wave of malware: millions of pieces of malware per day, generating billions of security events and alerts.

Even more troubling is the evolution and expansion in types of threats. Increasingly, the industry is seeing more advanced persistent threats (APTs), which use sophisticated, stealthy techniques to attack well-defined targets. For example, an APT may target select high-value individuals such as corporate executives, technology leaders, or architects. APTs are often built and maintained by nation states or organized crime; these actors are typically aggressive, well-funded, and highly skilled. As a result, APTs represent one of the most difficult security threats to find and eradicate.

The data explosion fueled by cloud computing, the Internet of Things (IoT), autonomous cars, and other emerging technologies further complicates the information security landscape. For example, just one autonomous car can create 40 GB of data per day. The combination of an exponential increase in the amount of data coming into the enterprise environment and progressively sophisticated attacks requires a new approach to information security, putting new demands on both infrastructure and personnel. While traditional countermeasures or controls—like demilitarized zones (DMZs) and firewalls—are still necessary, they are not sufficient for detecting APTs.

Solution

Traditionally, Intel IT has used security capabilities like firewalls, DMZs, virtual private networks (VPNs), multifactor authentication, and signature-based intrusion prevention and detection systems to protect intellectual property, data, and other company assets. We also continually evaluate and invest in new security technology to address shifts in the threat landscape or changes in business needs. These are all effective security measures because they reduce the signal-to-noise ratio, but they are not enough.

Instead of merely watching to make sure our information security measures are working and then reacting to negative events, we are driving a significant paradigm shift. We are operationalizing and automating the traditional security architecture so that we can simply trust that it is doing its job to prevent 99 percent of attacks from succeeding. However, we assume that the remaining one percent is going to penetrate those defenses, so we create teams to hunt for positive events that indicate an active APT.

Operationalize the 99 Percent

Our traditional information security architecture (see Figure 1) is important and necessary—it helps protect Intel against external and internal hacking, distributed denial of service attacks (DDoS), vulnerability exploits, known Trojans, worms, PC and server viruses, spam, and fraud. This approach to information security successfully handles 99 percent of the threats.

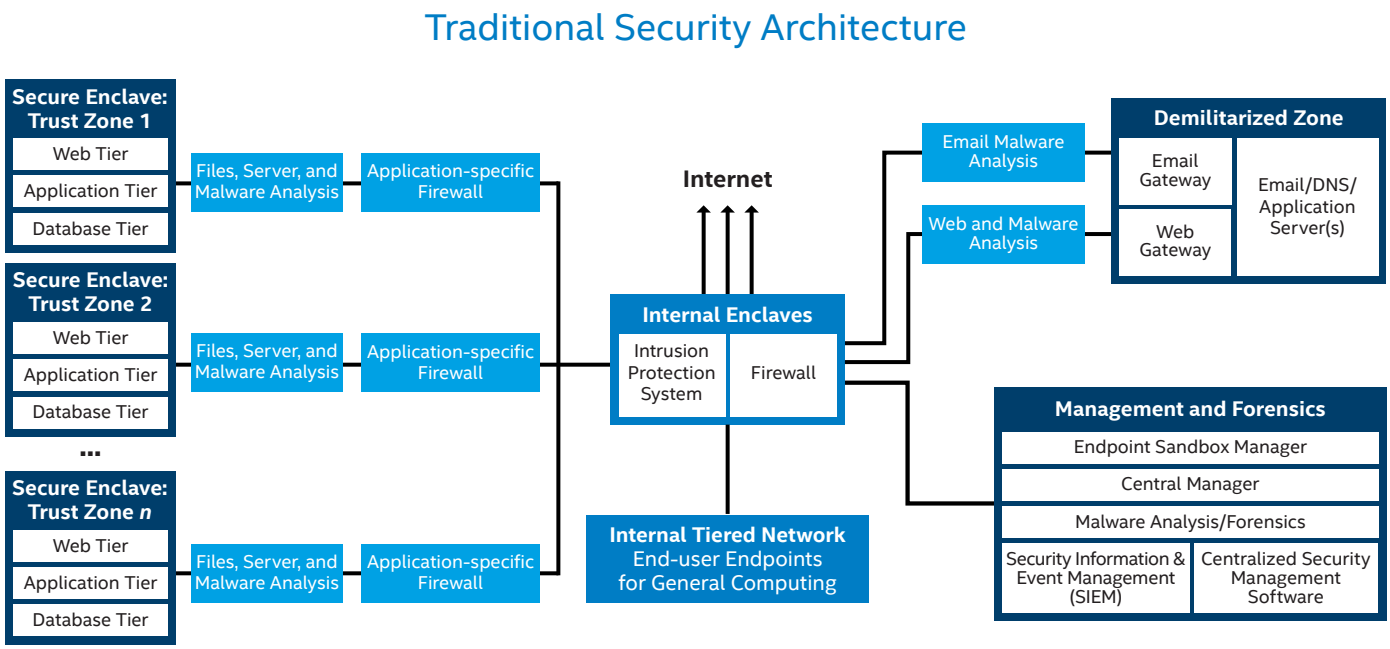


Figure 1. Operationalizing the host and network intrusion prevention systems, Web and email filtering, vulnerability management, firewalls, antivirus software, and proxies allows personnel to focus on the few but highly dangerous advanced persistent threats that may get through defenses.

While we will continue to invest in upgrades to our traditional information security architecture, we are shifting our focus: instead of continuing to have personnel watch for the negative events that these sorts of threats cause, we are working with our information security infrastructure suppliers to operationalize the monitoring of hundreds of thousands of devices using intelligent software agents that can scan, alert, and either mitigate, quarantine, or patch when problems occur.

We have found that our security information and event management (SIEM) system still has an important role. Due to the "noisy" IT environment, this system is no longer our only method of detecting attacks; however, we still use it as an important education tool. For example, cross-site scripting attacks (XSS) are still a common threat. Our SIEM system can collect and correlate data that can be used to teach security personnel about the patterns that signal an XSS attack.

Many information security solutions available today require protocol-specific appliances for each security function they perform, as well as an additional management appliance to share intelligence across different protocol-specific appliances. This costly and inefficient approach can lead to appliance sprawl. To avoid this problem, we use an information security solution that offers a centralized analysis appliance that supports multiple protocols. This consolidated approach helps lower total cost of ownership, simplify administration, and improve security posture and immediacy of protection across multiple channels through shared threat intelligence between numerous security products.

This approach to information security successfully handles 99 percent of the threats.

Use Patterns to Find the One Percent

APTs are distinct from other attacks not because of where they come from or the payload they carry but because of the unique methodology they use. APTs are "advanced" because they consist of unique malware that is well thought out and based on detailed knowledge of a specific environment and designed to bypass security controls. They are persistent because they include multiple techniques so that even if activity is detected at location A (a server, for example), other locations can carry out the attack. APTs are designed to maintain a long-term, undetected presence on the network, exfiltrating as much data as possible.

How Advanced Persistent Threats (APTs) Work

The figure below illustrates a typical APT attack scenario:

1. The hacker sets up a command-and-control (C&C) botnet to find vulnerabilities and take advantage of them.
2. APT entry points are usually internal hosts or the desktop systems of key users and corporate executives. Gaining entry is usually accomplished by an employee opening an email attachment, visiting an infected website, installing an infected USB stick, or clicking a link in an instant messaging application.
3. A loader file is downloaded and hidden, after which other malware such as key loggers, rootkits, and Trojans are installed. The infected system then connects to the remote C&C server and begins to send back data. For example, the malware may copy, compress, encrypt, and send all files with a certain file extension.
4. The malware from one machine spreads throughout the environment by taking advantage of unpatched vulnerabilities and stolen credentials.
5. The APT "camps out" for long-term data exfiltration by becoming dormant and reawakening on a set schedule to send more data to the C&C server.

Advanced actors conduct extensive reconnaissance and use knowledge of a particular enterprise environment to gain access, and then use that environment as a weapon of attack. For example, every modern enterprise must use email, the Web, and DNS. Ironically, these are all pathways to the network that advanced actors can use for an attack. APTs are tailored to a particular environment. For example, in an encrypted environment, an APT may use behind-the-scenes screen capturing to circumvent encryption and send data back to the command-and-control (C&C) server.

In contrast to the negative events that information security specialists are traditionally trained to watch for, APTs create positive events that require detective work to recognize (see Figure 2). Simply put, APT detectives learn what "normal" network, system, and application behaviors look like, and then look for changes in those patterns to identify possible APT activity. For example, if most network traffic occurs between 8 a.m. and 5 p.m., network access at 3 a.m. is a break in the pattern. It could be just that an employee is working late. Or, it could be the work of a nefarious APT.

We are making significant investments in anomaly detection solutions that use machine-learning algorithms to help determine what is and what is not normal. We are also investing in instrumentation, such as flow technology, which is an anomaly-based intrusion detection system. This sophisticated monitoring can identify nonstandard usage of data transmission protocols, adaptive authentication, and more.

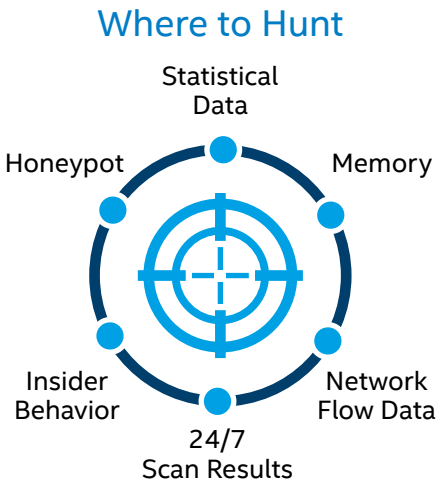


Figure 2. Hunting for advanced persistent threats requires a detective mindset, paying attention to many anomalous patterns throughout the enterprise environment.

Other techniques include the following:

- **Honeypots and sinkholes.** Isolated environments that may attract APTs, where we can learn how they behave without endangering the rest of the enterprise.
- **Layer 7 monitoring.** Detects anomalous data that leaves over the Web, instant messaging, and SSL (Secure Sockets Layer) certificates.
- **Network traffic recorder.** Enables recording of all network traffic for historical review.

Build the Right Team

It takes a different mindset to look for positive events instead of simply reacting to negative events. We are building a team that can strategically use emerging technologies to establish patterns and identify when activity deviates from those patterns. We have found that we need team members that have inquisitive minds and enjoy asking questions.

We also collaborate with fellow travelers such as suppliers, other enterprises, and government agencies. These collaborations increase everyone's threat intelligence, gaining a better understanding of indicators of compromise. We also invest in creating a security-conscious corporate culture (see the sidebar "Security College").

Security College

Intel Security's College, which offers over 100 cybersecurity courses for 12 different technical roles, improves our security posture and helps reduce costs by training our developers to write secure code from the outset. According to the National Institute of Science and Technology (NIST), it costs 30x more to fix application vulnerabilities once an application is in production.[2]

Our Security College courses are based on industry best practices, such as the NIST 800.16 security training requirements. Content can be used as Continuing Professional Education credits for existing technical certifications and is available in five localized languages.

Conclusion

Our choice of information security solutions is guided by a strategic and holistic view of the threat landscape. Investing in world-class traditional security solutions and then operationalizing those solutions frees our security teams to focus on the APTs that comprise the one percent that circumvents traditional countermeasures. We have learned that when it comes to security, if everything seems quiet, there is probably something bad going on.

We are using the latest machine-learning technology and other techniques to establish an understanding of normal network behavior and then identify when those patterns are broken. We are also investing in security training throughout the enterprise to create a security-conscious corporate culture.

Information security is a constantly changing endeavor. We continue to evaluate new techniques and technologies that reduce the signal-to-noise ratio and increase our ability to detect, isolate, and destroy APTs.

Related Information

Visit intel.com/IT to find content on related topics:

- Securing the Cloud for Enterprise Workloads paper
- Enterprise Technical Debt Strategy and Framework paper

For more information on Intel IT best practices, visit **intel.com/IT.**

Acronyms

APT	advanced persistent threat
C&C	command-and-control
DDoS	distributed denial of service
DMZ	demilitarized zone
IoT	Internet of Things
SIEM	security information and event management
VPN	virtual private network
XSS	cross-scripting attacks

IT@Intel

We connect IT professionals with their IT peers inside Intel. Our IT department solves some of today's most demanding and complex technology issues, and we want to share these lessons directly with our fellow IT professionals in an open peer-to-peer forum.

Our goal is simple: improve efficiency throughout the organization and enhance the business value of IT investments.

Follow us and join the conversation:

- Twitter
- #IntelIT
- LinkedIn
- IT Peer Network

Visit us today at intel.com/IT or contact your local Intel representative if you would like to learn more.

[1] Ponemon Institute; "2018 Cost of a Data Breach Study" (July 2018). ibm.com/security/data-breach

[2] National Institute of Standards & Technology, "The Economic Impacts of Inadequate Infrastructure for Software Testing" (2002). nist.gov/sites/default/files/documents/director/planning/report02-3.pdf