The Arms Race to Stop Advanced Threats

Why traditional endpoint protection fails against today’s advanced persistent threats.
# Table of contents

IT leaders are facing more advanced threats to enterprise security than ever before ........................................3

It’s not just the Fortune 500 who are under attack .............................................................................................................4

Endpoints pose the greatest risk ........................................................................................................................................5

Traditional endpoint security catch 90% of attacks. But the other 10% pose the biggest threat ..............................................6

The 5 key problems with traditional endpoint protection ..................................................................................................7

The 2 key layers needed for advanced protection .................................................................................................................8

Determining your organization’s risk ....................................................................................................................................9
IT leaders are facing more advanced threats to enterprise security than ever before.

Today’s cybercriminals are well organized, highly sophisticated, and extraordinarily motivated. Gone are the days of battling the lone wolf hacker bent on becoming famous. Modern cybercriminals are funded, organized syndicates, with the tools and know-how to design customized attacks that sneak in, establish a foothold, then stealthily compromise an organization’s most sensitive and valuable data—syphoning everything from personal and financial information about customers to the company’s own intellectual property.

Vulnerability comes with an astonishing price tag.
Recent studies suggest that recovering from a security breach costs the average organization more than $3.8 million (Ponemon 2015). And worldwide, Symantec estimates that cybercrime accounts for $300 billion to $1 trillion in corporate losses annually. But there’s more at stake than just money: Tarnished reputations, the loss of competitive advantage, and the erosion of public confidence can exponentially compound a firm’s financial losses.

The threat is both persistent and universal.
63% of C-suite executives report their companies are under daily or weekly attack. And that number is growing.

Malware continues to increase exponentially.
Symantec estimates the number of unique malware threats at 1.7 billion, and that number is growing rapidly. Last year alone, more than 317 million new pieces of malware were created—nearly a million pieces a day—and a growing number of those are specifically designed to penetrate the core assets of an organization.

Today’s data breaches are so well written and well choreographed that they’re penetrating companies with even the most advanced tools and teams. And while big companies have a lot to lose, the truth is that cyber thieves are moving down market to smaller organizations that have information of value and are less likely to be formidable against these threats.
It’s not just the Fortune 500 who are under attack.

The astounding volume and frequency of sophisticated cyber attacks in the past year proves just how pressing the threat has become. While high-profile cases make the biggest news, there’s no doubt that small to medium-sized organizations are now seen as low-hanging fruit, increasingly ripe for attack.

Today’s cyber thieves are not just going after Fortune 500 companies, they’re moving down market to smaller organizations that have information of value and are less likely to be formidable against these threats.
Endpoints pose the greatest risk.

There’s little dispute, untethered mobility in the workplace—mobile apps, mobile devices, and worker mobility—coupled with the growth of BYOD (bring your own device) practices—creates a mind-boggling array of security challenges. Employees often mix business with pleasure, loading personal content from unsecured, sometimes infectious environments onto corporate devices. They use smartphones, tablets, and laptops to connect with each other, with the corporate network and with the outside world. And they tap into dubious public networks in coffee shops, hotels, airports, and more.

These vulnerable endpoints allow cybercriminals to slip in the back door of the enterprise, establish a foothold, and begin unfurling a low and slow attack on the organization’s most vital data.

“65% of organizations say they are experiencing more advanced persistent threats and targeted attacks.”
— 2015 Ponemon Report
Traditional endpoint security catch 90% of attacks. But the other 10% pose the biggest threat.

Most organizations use a combination of reputation- and behavior-based detection—antivirus, anti-spam, and host intrusion prevention services (HIPS)—to find and sweep up attempts to breach their systems. These traditional solutions are effective against conventional malware, but they’re not enough to prevent the kind of rapidly mutating, quietly unfolding attacks used by advanced cybercriminals.

**Reputation-based solutions only recognize known threats.**

By identifying and intercepting files based on their reputation across user groups, web crawlers, and intelligence networks, these solutions can detect up to 75% of all attempts to breach a system. They’re effective against known threats, but they can’t catch rapidly proliferating variants designed to elude detection.

**Behavior-based solutions are necessary, but frustratingly overzealous.**

These systems employ the old adage, “If it looks like a duck and walks like a duck...” comparing the behavior of an event to an established norm and tagging every deviation as a potential security risk. They’re largely effective in detecting previously unknown and zero-day threats that slip past reputation-based solutions. But, they’re intentionally paranoid systems, designed to send up a flare whenever the slightest thing doesn’t conform. That often results in a frustrating number of false alarms. And although behavior-based solutions can detect an intrusion, they can’t preempt it; once a breach is detected, it’s already in the system and likely to spread.

“68% of organizations say endpoint security is becoming a more important part of their organization’s overall IT security strategy.”

– 2015 Ponemon Report
The 5 key problems with traditional endpoint protection.

Effective security relies on two key components: First, the ability to quickly distinguish real threats from mere nuisances (prioritization). Secondly, the ability to contain anything diabolical before it has a chance to establish a toehold from which to launch a full-scale attack (resolution). That’s not easy—for a lot of reasons.

1. **Endpoint security is fragmented.** A typical IT team may use dozens of distinct and disconnected security products to protect various data control points. Without the ability to prioritize possible threats—to distinguish a weapon of convenience from a real attack—endpoint security becomes a game of whac-a-mole. When they don’t know where to look first, IT teams lose valuable time.

2. **Independent teams can’t connect the dots.** One team may be monitoring network security, another endpoints, and a third email. What’s more, the network, security, and desktop support teams may also be operating independently. That kind of disconnect makes it harder to see a large-scale attack unfolding across the enterprise, creating an environment ripe for successful cyber attacks.

3. **Detection and remediation are difficult and slow.** IT security teams are under constant pressure to accurately process data to find meaning. And that’s compounded by the fact that any advanced attack is sure to be well disguised and rapidly mutating. With data flowing in from every control point, detecting and tracing anomalies across multiple sources requires forensic expertise and painstaking focus. Once an attack is detected, it takes time to remediate it and it can be difficult to know if you’ve mopped up every last bit, until it’s too late.

4. **Tracking down false alarms diverts valuable time and effort.** When detection tools don’t prioritize alerts and every anomaly is equally dire, cautious teams end up following every rabbit hole to find the real threat and less cautious teams lower the standards to reduce the noise. Both approaches can be deadly to data security.

5. **Zero-day threats are particularly insidious.** These attacks, which exploit system vulnerabilities before they’re even known to exist, are virtually undetectable until they’ve already taken a foothold. Zero-day attacks can take security teams months, even years to detect, and much longer to quarantine, once they’re uncovered.
The 2 key layers needed for advanced protection.

Guarding against advanced persistent threats that elude traditional endpoint protection means adding additional layers of protection to work in concert with traditional endpoint security tools.

**Automated data correlation layer.**
Today’s advanced attacks are surreptitious and require that organizations evaluate activity across all control points. But even with the best security tools and forensic specialists in place, the work of correlating data from email, networks, endpoints, and advanced threat intelligence can be painstakingly slow. One solution is to add a data correlation layer to coordinate information from network, endpoint, and email events. Effective data correlation reduces the number of individual investigations required and allows teams to focus their efforts on actual threats.

Data correlation reveals what’s being replicated across the entire system.
It gives organizations a way to connect the dots across endpoints and intelligence data with greater ease. When security teams monitor one endpoint at a time, it’s far too easy to miss the big picture. Data correlation brings the big picture into view.

It prioritizes threats.
By correlating suspicious activity across all control points, a data correlation layer allows security teams to more easily distinguish critical threats from mere nuisances, providing more time to contain the attack and prevent new attacks from taking root.

It reduces the time it takes to remediate an attack.
Good data correlation replaces guesswork, the analysis, and the human interpretation with really fast-moving, agile analytics. The end result: The time it takes to fully contain an advanced attack can drop from weeks or months to mere minutes.

**Sandboxing layer.**
Creating a safe place to quarantine and test suspicious files—a sandbox of sorts—adds the missing resolution capability to a security system.

Think of it like the TSA... If your credentials are missing or in doubt, airport security has the option of pulling you into a room, interviewing you, searching your bags, patting you down, and deciding whether you’re free to get on the plane. Sandboxing is similar. If a file isn’t in the reputation database and it resembles something malicious or it originates from a source, or part of the internet, or part of the world where malicious activity is known to originate, a policy-based protocol directs the system to put it in the sandbox for a closer look.

...and a bomb squad combined. Sandboxing captures possible threats at the get-go and keeps them from spreading to other systems or users. With this layer in place, suspicious files are automatically shunted into a rubber room of sorts and then physically or virtually detonated to test their safety before they can be downloaded or passed on via email. Files that don’t pass the test remain in quarantine and the system alerts IT security to investigate.
Determining your organization’s risk.

Your particular risk depends on a number of factors, but here’s one certainty: **The threat of cyber attack is only going to grow** and being proactive is your best defense. Take the time to thoroughly assess not only your organization’s vulnerability, but also your ability to detect and contain an advanced attack.

- Are you in an industry or organization-type that’s a target for advanced persistent threats?
- Is your endpoint protection still relying only on reputation and behavior-based approaches?
- Do you have the tools, process, and team to quickly distinguish real threats from mere nuisances?
- Is your system able to detect and respond to advanced threats before they gain a foothold?
Learn how ITS can help mature your endpoint protection to identify, contain, and avert advanced threats.

productiveATP.com