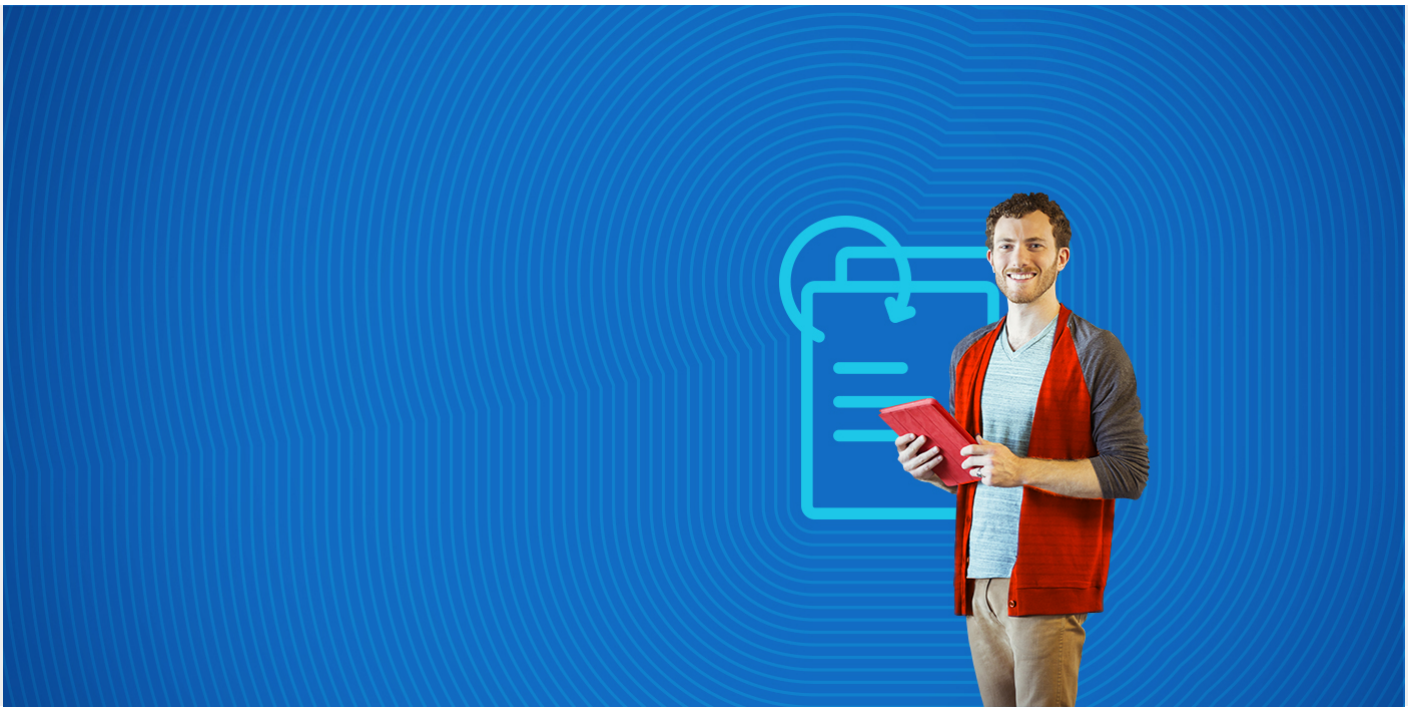
ADVANCED PERSISTENT THREATS



How to resist persistent threats in the digital economy

We live in an increasingly digital world and keeping organizations secure in this environment is more demanding than ever before. IT infrastructures have not been built to support this rapid transformation. In the race to provide more types of features and faster access to consumers, there are often gaps in code that can lead to vulnerabilities. These vulnerabilities and attacks seem to be coming out of nowhere and they need to be prevented. They are such a growing concern that based on BMC research with Forbes Insights, 97% of the execs interviewed expect a rise in data breaches in the next 12 months.

As we looked deeper into this issue, we've discovered that data breaches occur even when vulnerabilities are identified. Frequently, the data losses could have been prevented by a patch that was available, but not deployed, at the time a vulnerability occurred. According to Rob Joyce, head of NSA's Tailored Access Operations, " any large network, I will tell you that persistence and focus will get you in, will achieve that exploitation without the zero days," he says. "There's so many more vectors that are easier, less risky and quite often more productive than going down that route. This includes, of course, known vulnerabilities for which a patch is available but the owner hasn't installed it."

Fast track security with TrueSight Vulnerability Management for Third-Party Applications

[Explore TrueSight Vulnerability Management for Third-Party Applications ›]
See how you can accelerate vulnerability resolution, lower costs of remediation and avoid major security incidents.

- Prioritize and remediate vulnerabilities with TrueSight Vulnerability Management for Third-Party Applications
- Reduce time spent logging changes in CM system
- Improve systems stability through granular, role-based access
- Explore the security view to see predictive SLAs and burndown with TrueSight Vulnerability Management for Third-Party Applications

What is a persistent threat?

Persistent threats have hidden and continuous computer hacking processes that target a specific entity. These threats are covert, focus on accomplishing a specific task, and can happen continuously over time. They are considered persistent because an external system continuously monitors and extracts data from the target. If these threats are advanced, they can also involve planting remote administration or exploit software in the target's network that allows access to the victim's network and acquires administrator privileges on the victim's computer. Ultimately, hackers can steal data from the victim's network.

Persistent threats involve general attacking in areas that you may not realize are vulnerable. For example, a major retailer was attacked through their heating and cooling system for their building infrastructure, which became a gateway for hackers. The vendor had opened up the network to make fixes to a related system. A hacker was looking for that network, saw a hole, exploited it, and compromised customer data that had a price tag of more than $250 million and damaged the company's reputation.

What's the cost of being vulnerable?

The Office of Personnel Management breach that affected more than 22 million people could be the single most damaging breach to US national security of all time. Those who have access to some of the most sensitive information in the world had the contents of their entire background checks stolen by an unknown hacker. Imagine if a hacker knew exactly which buttons to push in order to blackmail someone into turning over vast swaths of sensitive or classified data. A hacker could also use this information for identity theft. More than 22 million government workers and contractors on government projects are now vulnerable. Also, OPM is providing credit monitoring services to some of the people affected by the hack. With the average cost of a monitoring service being $20 per month per person, the cost of this hack is as high as $440M per month and $4.88B per year.

Many breaches are avoidable

Security and Operations executives acknowledge that their organizations face unnecessary risks. The problem is deploying those available patches throughout a complex IT environment in a reasonable timeframe. WhiteHat Security says that it takes 193 days on average – more than six months – to resolve a vulnerability.

One reason it takes so long is the complexity of modern IT environments. Virtualization and cloud computing have made it difficult to control the creation of new systems. It's not uncommon for teams to build their own IT services outside the IT department ("Shadow IT"), which makes it harder to track and identify vulnerable systems.

The increasingly complex nature of modern applications makes it hard to isolate and secure parts of the supporting infrastructure. Administrators may be afraid that an action on one component may have cascading consequences elsewhere.

Even though a vulnerable system has been identified, users are often reluctant to accept downtime of services that they require. Often, easily understood business concerns trump seemingly abstract security concerns and there's a disconnect between the role and priorities of the Security team, which needs to protect the enterprise, and the Operations team, which is focused on ensuring performance and availability. This disconnect can lead to a gap between the organizations, known as the SecOps Gap, which may result in neither priority being satisfied unless the organization is governed by a policy that can close the gap.

Automate to close the SecOps Gap

Enterprises can address challenges created by persistent threats through effective and timely remediation. They can shrink and close the SecOps Gap by taking into account the different priorities and concerns of those two roles, and enabling both teams to achieve what they need. This includes having a governance strategy that integrates and automates discovery, definition, auditing, and remediation to ensure a level of continuous and vigilant compliance. Vigilant compliance is based on managing by policy, and not just by alert.

The Security team wants to close the window of vulnerability, the period of time during which a bug or vulnerability can be exploited to penetrate a company's defenses, by deploying patches and fixes as quickly as possible. They are usually very aware of how long it takes to make these changes, and vice versa, of how quickly attackers can move to exploit a new weakness. Security teams are judged by how well they block and remediate threats and not on how installing a new security patch impacts uptime.

The main concern of the Operations team is to reduce both scheduled and especially unscheduled downtime. A leading industry analyst reports that 80% of downtime is due to misconfigurations – errors in manual data entry, incorrect or incomplete targeting of activities, or incomplete execution. The Operations team aims to minimize this risk with procedures, but these have the unfortunate side effect of introducing delay into the process.

BMC research indicates that 60 percent of executives say Security and Operations teams have only a general or little understanding of each other's requirements. Conflicting priorities, mounting pressure, and little understanding of each other – what can organizations do to improve this situation before it is too late?

Strategies for ensuring Security

To stay on top of today's complexities, threats and opportunities, large enterprises are developing SecOps strategies that focus on three core areas:

1. **People—** Security and Operations professionals share accountability for making business systems more secure and reliable
2. **Processes—** Guide and integrate the activities of key stakeholders in Security and Operations
3. **Technology—** Heighten security by replacing error-prone manual processes with automated tools.

In the digital era, with more and more internet-visible services, persistent threats are the most dangerous type of attackers because they keep looking for gaps in security. To improve the cadence of rapidly closing security vulnerabilities, organizations need to recognize and balance the needs of Security and Operations. This will help digital organizations move faster, while maintaining availability and keeping their customers happy.