



TAKE CONTROL.

## Cyberwar Threats

NEW SECURITY STRATEGIES FOR GOVERNMENTS

WHITE PAPER ○



# Introduction

---

Cyberwar fundamentally changes how government must handle security. Faced with increasingly sophisticated attacks from gangs of cyber criminals and foreign governments probing U.S. systems for sensitive data, threats frequently go undetected for days, weeks, and even months. Unfortunately, the traditional fortress approach no longer suffices. Firewalls, intrusion detection systems and other security devices can stop the average hacker, but new threats use stealth techniques that these defenses cannot detect on their own.

Faced with the certainty that attackers will get into their systems, government organizations must take a more proactive approach to risk management. This approach includes focusing security efforts on protecting mission-critical data. To focus those efforts, government organizations need situational awareness. They must know the location of critical data, identify the characteristics of the systems that carry the data, understand the vulnerabilities of those systems, and detect changes in activity that signal potential threats. Government organizations must also know what security controls they have in place throughout the IT infrastructure, and whether these controls protect the infrastructure against the potential threats.

However, the sheer size and complexity of the government infrastructure makes gaining that awareness difficult. The US government boasts thousands of uniquely configured systems strewn across hundreds of offices and government departments. And thousands of security devices throughout the government IT infrastructure generate such huge quantities of valuable data that the IT departments in these government organizations get overwhelmed when faced with collecting and analyzing it.

Government organizations urgently need solutions that provide automated, continuous, and end-to-end monitoring of that infrastructure to isolate vulnerabilities and risk and help overwhelmed security professionals immediately identify and mitigate any damage from existing and potential threats. Only with these solutions can government agencies defend themselves against the threats and consequences of cyberwar.

## Evolving Threats Require New Cybersecurity Strategies

The attack that compromised Google's systems in December, 2009 demonstrates just how the new generation of adversaries can effectively take down an Internet giant.

Google said that the Chinese government launched the attack to access the email accounts of Chinese human rights activists, but that some 20 other organizations fell victim to the attack, including several U.S. defense contractors. The attackers got past all of the defenses installed by Google, and managed to stay hidden for days while they hunted for the activists' data.

In testimony to the Senate Select Intelligence Committee in February 2010, Denis Blair, the director of national intelligence, said that these kinds of advanced persistent threats (APTs) result in the theft of sensitive information from government networks every day. The technology balance currently favors the attacker, he said, and may do so for some time.

Deloitte, in its 2010 CSO Cybersecurity Watch Survey, found that most organizations it surveyed lacked awareness of these kinds of attacks, or felt overconfident that their current security measures and technology could protect them. More than two-thirds still considered hackers the biggest threat.

Unfortunately, these non-agile security tools and processes don't work against APTs. The Deloitte report noted that intrusion detection, signature-based malware and anti-virus solutions provide little defense, and rapidly become obsolete against attackers who use such strategies as encryption technology to mask their efforts.

Cyber attackers typically exhibit much more patience than the traditional hacker. When rebuffed, they keep probing until they find a way in. Once past the defenses, they call on their assets time and again to extract data. You would not classify these attackers as opportunists; they have a mission and remain focused on it until they succeed.

# Identifying and Managing Risk

Given the tactics and tools of cyberwar, IT can no longer simply man the barricades and plug whatever holes develop in their defenses. Instead, government must proactively identify the data most at risk and secure the systems that contain that data. The desired end? Agencies continue to operate and missions remain uncompromised. When it comes to national security, defense and essential parts of the country's IT infrastructure, that's the ultimate goal.

The National Institute of Standards and Technology (NIST) is responsible for drawing up the guidelines for certifying and accrediting the security of government IT systems. NIST puts risk management at the center of its most recent revision of those guidelines.

The guidelines emphasize building solid security into those critical government systems as early in their life cycle as possible. Doing so makes it easier to identify what vulnerabilities and weaknesses remain, which makes it easier to manage them within the standard risk determination and acceptance process.

That's certainly something that the Department of Defense (DoD) counts on to keep its Global Information Grid, the worldwide collection of computers and networks that drives its operations, up and running, and its most important data safe. Of all government organizations, cyber attackers consider the DoD the prize target.

In order to manage risk, however, you must know the security status of all of the systems throughout the enterprise. Any weakness can be exploited by the opposition. That's the essential visibility that all agencies will be looking for.

In an interview with GovInfoSecurity.com, Ron Ross, the head of the team that drew up the NIST guidelines, said continuous monitoring "is critical" for making sure that agencies know the security state of their systems on an ongoing, day-by-day, hour-by-hour basis. "That is the up tempo that our adversaries are working in today as they launch these very sophisticated cyber attacks against our critical systems," he said.

## Still a Long Way to Go

Most of government still remains far from having the kind of visibility and situational awareness it needs to manage risk.

One of the basics of good security, for example, is systems that are correctly configured according to a baseline of policies and controls that are known to be good. Next is knowing promptly when those systems become misconfigured and then fixing them.

As part of their annual FISMA report to the Office of Management and Budget (OMB), agencies must show they have both an agency-wide security configuration policy, and provide evidence on how well they have implemented various security configurations on their systems.

In a July 2009 report, the Government Accountability Office (GAO) said all 24 of the major federal agencies it investigated claimed they had a security configuration policy in place. But almost all of them had weaknesses in their information security controls, and over 21 had configuration management weaknesses.

Several agencies did not implement common secure configuration policies across their systems, the GAO said, and many did not ensure that system software changes had been properly authorized, documented and tested.

John Gilligan, a former chief information officer for both the Air Force and the Department of Energy, told a recent cybersecurity forum that if government organizations deployed and enforced security measures such as configuration controls, these organizations could block some 85 percent of attacks.

Devices in the network that record security-related events offer another source of useful security information. Collecting those logs and having some way of analyzing them can help flag potential threats. Unfortunately, most agencies can't do that right now; however, many are starting to realize what those logs offer. In a recent study, the DoD said that log management ranked among the highest value controls that could be used to block attacks.

# Tripwire VIA Solutions: Visibility, Intelligence, Automation

The suite of Tripwire® VIA™ solutions deliver the real-time, continuous monitoring organizations need to counter modern cyberwar threats, so agencies see the data that matters no matter how much noise the IT infrastructure generates. Armed with this visibility, security professionals detect weaknesses and vulnerabilities, and make fixes before attackers can exploit them. Tripwire VIA solutions include Tripwire® Enterprise for industry-leading configuration audit and control, and Tripwire® Log Center for next-generation log and event management.

Tripwire Enterprise helps organizations focus on the changes that matter with change detection, compliance policy management, real-time intelligence that identifies changes that introduce risk or non-compliance, and instant access to remediation advice.

With over 200 out-of-the-box policies, Tripwire Enterprise covers just about any security, regulatory and operational policy needed for assessing and managing configurations. Specific to government organizations, Tripwire Enterprise includes policies for NIST SP 800-53 Rev 3, DISA STIGS and FISMA requirements. These policies include weighted tests that help IT managers focus on the configurations that pose the greatest security risk or most impact system performance.

Tripwire Enterprise also allows organizations to capture secure or operationally optimized configurations developed in-house so these configurations can be re-applied as needed. And Tripwire Enterprise offers remediation of issues for both physical and virtual environments.

Tripwire Log Center, a next-generation log and event management solution, captures and stores tens of thousands of events per second to meet the log management requirements of many standards and regulations. It also enables Google-like searches of log activity data for deep forensic analysis. Because Tripwire Log Center supports the most popular log transmission protocols, it immediately collects logs from just about any source. In addition, Tripwire Log Center detects and alerts to events that may indicate suspicious activity. The solution's graphical tools help correlate events, and pinpoint those parts of the infrastructure that could be open to attack.

As part of the Tripwire VIA suite of solutions, Tripwire Enterprise and Tripwire Log Center integrate with each

other to provide a single solution for complete IT security and compliance. With Tripwire VIA, IT can investigate suspicious events related to a change that introduces risk or noncompliance. Combined, these solutions also support incident investigation, reveal patterns of activity that indicate threats, and help identify downstream impacts of a given change. The combination also enables organizations to gain instant audit logging capabilities across the entire IT infrastructure without installing additional code.

With the Tripwire VIA suite of solutions, organizations gain end-to-end visibility across the enterprise, intelligence to help them make better and faster decisions about threats and risk, and automation to address the millions and billions of changes and events that occur in today's IT infrastructure.

## Conclusion

Cyberwar and its sophisticated, persistent threats is forcing government agencies to move away from an all-or-nothing approach to security. These organizations must now focus on protecting essential data and ensuring continuous availability of critical systems—all without interrupting the ability of these agencies to conduct the day-to-day business activities required to fulfill their missions. As a result, security becomes a strategic necessity rather than activity that simply complements the other activities of government agencies. Agencies must now apply risk management practices that ensure systems stay up and running.

To do that, security professionals have to shift from their traditional reactive stance to a more proactive one. Because they can't manually plug the holes fast enough, they need a way to get ahead of the threats. Key to this is being able to get a clear view of the existing vulnerabilities through the noise created by the overwhelming number of systems and configurations that make up today's IT enterprise.

Tripwire VIA solutions provide that end-to-end, in-depth visibility of all activity and events across the enterprise so users can identify potential threats in real-time. These leading solutions also deliver actionable intelligence so managers know where misconfigurations, and therefore vulnerabilities and non-compliance, exist. And Tripwire VIA solutions provides the automated response needed to deal with today's round-the-clock threat environment.

#### ABOUT TRIPWIRE

Tripwire is the leading global provider of IT security and compliance automation solutions that help businesses and government agencies take control of their entire IT infrastructure. Over 7,000 customers in more than 86 countries rely on Tripwire's integrated solutions. Tripwire VIA™, the comprehensive suite of industry-leading file integrity, policy compliance and log and event management solutions, is the way organizations proactively prove continuous compliance, mitigate risk, and achieve operational control through Visibility, Intelligence and Automation. Learn more at [tripwire.com](http://tripwire.com).

