Cybersecurity in the Public Sector: Navigating the Threat Landscape

"Cyber intrusions and attacks have increased dramatically over the last decade, exposing sensitive personal and business information, disrupting critical operations, and imposing high costs on the economy."

– U.S. Department of Homeland Security

Just as businesses in banking and manufacturing, shopping and entertainment move to pervasive networks, public sector organizations face a challenging new reality when implementing today's "boundless" infrastructures: a spiraling threat to data security. Driving this growing threat are the evolving trends of mobility, cloud computing, and advanced targeted attacks, which combine to create challenges and insomnia for IT administrators.

Consider how the notion of "the network" has evolved. No longer a manageable set of communication pathways that are relatively easy to patrol, networks are now vast and virtual, integrating widely dispersed resources and users who connect from a wide array of devices.

The same innovations powering the rapid spread of information technology are presenting new challenges for protecting data. For example, cloud computing increases flexibility for scaling your infrastructure to meet mission objectives, but also increases the complexity of protecting sensitive data. Mobile devices increase convenience but often bypass traditional security measures. The nature of the threat is also changing, as thieves employ a burgeoning set of sophisticated tools to take advantage of our growing reliance on networks for critical-data exchange.

For the public sector, the stakes are high. The proliferation of hackers, inevitable human errors, bring-your-own-device (BYOD) initiatives, and the ever-broadening need to share information weigh heavily on government and education organizations, and consume substantial resources. The Pentagon, for example, has proposed to spend $23 billion on network security initiatives through 2018. This sounds like a large sum, until you consider the scope and importance of the U.S. government information resources this investment must protect.

Against this backdrop, yesterday's prevention strategies are no longer adequate for stopping advanced, targeted attacks. Today, effective cybersecurity must be multi-dimensional and tiered, as threats can originate from virtually anywhere, target numerous levels of an organization, and sometimes persist for months or years before an information security staff is aware of an attack or breach. Securing public sector networks requires a holistic approach that incorporates several elements. Best practices include:

- personnel training and awareness
- threat-centric orientation that extends beyond standard policies based on past events
- pervasive internal monitoring
- sharing of security intelligence within and between organizations

Today's heterogeneous network environments demand flexible, integrated, open solutions that evolve as quickly as the threats themselves.

Cybersecurity in the Public Sector: Navigating the Threat Landscape

Cisco: A Familiar Name Delivering Maximum Protection Against Unfamiliar Threats

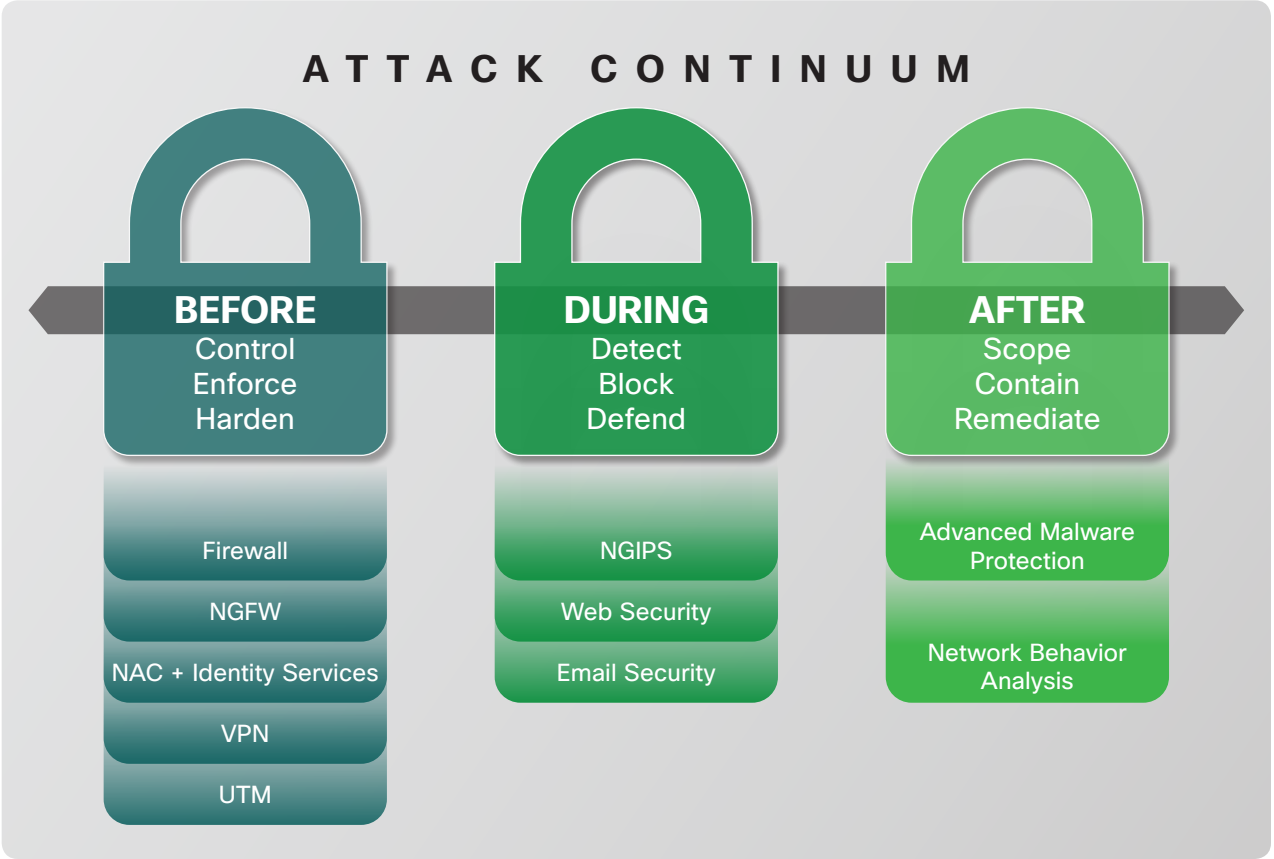
Cisco is uniquely positioned to make comprehensive cybersecurity less complicated and more practical for government and educational institutions.

Cisco® cybersecurity solutions and services provide consistent control across diverse and expansive network infrastructures. Now organizations have flexibility for deploying security in the way that best suits their objectives, and unmatched threat visualization, analysis, and mitigation.

Cisco security controls are designed and deployed at the foundation level, within and around the core network, providing an adaptive, responsive, and architectural approach. This means 360-degree protection that allows institutions and agencies to discover, defend against, and quickly remediate even the most advanced threats.

Unlike many providers that deliver point products, capable of blocking uni-directional threats, Cisco's experience and presence throughout the network infrastructure, in hardware and software from core to edge, provides unsurpassed protection.

Cisco Security Products Mapped to New Security Model



If you knew you were going to be compromised, would you do security differently?

Cisco's Cybersecurity Action Plan

Recognize that there is no Silver Bullet

The notion of a network perimeter no longer exists. Threats can enter the network in many ways, and having comprehensive protection requires a multi-tiered approach to keep threats out and detect and isolate any breaches quickly.

Defend, Discover, Remediate

Public sector IT security budgets historically have been directed at defending the network. That's no longer sufficient. Cisco's cybersecurity framework is built around the security features already embedded in its core network products. This empowers organizations to discover and thwart increasingly sophisticated information and infrastructure attacks using approaches including enhanced content inspection, behavior-anomaly detection, and advanced forensics.

Build on the Protection Already Embedded in your Cisco Network

- Take advantage of your existing investment in Cisco core network products, which comprise 80 percent of what you need to enable an effective cybersecurity posture.
- Strategically add Cisco security products based on your needs to extend your security level. You can also tap the worldwide intelligence provided by Cisco's Security Intelligence Operation (SIO) to protect your government enterprise or campus.
- Partner with Cisco's ecosystem of industry leaders to fill any gaps. Examples include Lancope Stealthwatch for continuous network-behavior monitoring, Arbor Networks for Distributed Denial of Service (DDOS) protection and Splunk for Security Incident and Event Management (SIEM): all available through Cisco channel partners.

Built-In Protection and Peace of Mind

With Cisco network solutions, public sector organizations have a strong start on creating an effective cybersecurity plan. Cisco products offer an extensive array of threat defense, detection, and remediation capabilities.

- **Secure Identity and Mobility** supports secure access from any device to selected, appropriate information resources, based on the user's identity, security access level, location, connection method, and time of connection.
- **Malware Detection and Defense** benefits from real-time threat intelligence gathered globally, enhancing local threat libraries to take a proactive stance to protecting data and networks.
- **Cisco Cyber Threat Defense** provides continuous network traffic monitoring and context information from an Identity Services Engine (ISE) to simplify and automate the detection of threats on the network, saving resources and time.
- **Secure Virtualized Data Center** extends network visibility into the virtual layer to protect the modern data center.

Learn More

Visit www.cisco.com/go/uspscybersecurity to discover how Cisco's comprehensive security solutions can help your organization protect its data and network so you can confidently achieve mission objectives.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices**.