ForeScout

Organizational Challenges

- Preserve the trust of citizens, other agencies and allies' governments by protecting data privacy
- Improve security posture without impeding government services or the free flow of information
- Comply with North American, European and international regulatory mandates and directives designed to protect sensitive information, such as FISMA, NERC, ISO/IEC 27001 and the GDPR[4]
- Facilitate streamlined network access and information sharing for trusted contractors, research organizations and the public
- Achieve continuous monitoring and mitigation capabilities that leverage existing investments

Technical Challenges

- Discover BYOD, IoT, rogue devices and other endpoints connected to government networks
- Control access to confidential data
- Prevent infected or non-compliant devices from spreading malware across the network
- Enable employees and contractors to use their personal devices while preserving security
- Guard against targeted threats that can result in stolen data and network downtime
- Measure effectiveness of security controls and demonstrate compliance with regulations

Government

Government security, privacy and compliance start at the endpoint

ForeScout Technologies helps government IT professionals protect confidential data, demonstrate compliance with regulations and provide secure network access for a wide range of devices and user populations in a cost-effective, efficient and non-disruptive manner.

The Challenge

Here's a small sampling of government agency data breaches:

- Theft of Social Security numbers and other sensitive personal information from the computer systems of the U.S. Government Office of Personnel affected roughly 21.5 million people.[1]
- British Intelligence recently revealed that ISIS hackers intercepted top secret British Government emails and were targeting information held by some of Prime Minister David Cameron's most senior advisors.[2]
- Hackers released data on 10,000 Department of Homeland Security employees and 20,000 FBI employees.[3]

It's no wonder government agencies the world over are urgently seeking advanced network security solutions. As cyberthreats increase in numbers and effectiveness, government agencies must rethink how to eliminate intrusions, protect sensitive information and mitigate exposure to cyberattacks.

As cyberthreats increase in numbers and effectiveness, government agencies must rethink how to eliminate intrusions, protect sensitive information and mitigate exposure to cyberattacks.

Traditional network security products focus on blocking external attacks with firewalls and intrusion prevention systems (IPS). However, insider threats can do an incredible amount of damage in terms of disruptions to operations, theft of sensitive data and loss of reputation. Misuse and abuse of data resources by employees and contractors are rampant, as are risks associated with the wide array of personally owned devices that are used to access networks during the workday.

Traditional endpoint security systems such as antivirus, patch management and encryption also leave a lot to be desired because they are limited to managed, user-based endpoints. Far too often, these security systems are not fully operational and up-to-date on all endpoints, leaving gaps in protection and failing to identify compromised endpoints or deter rogue wireless access points from extending your network without your knowledge.

CounterACT as a Cornerstone for Government Cybersecurity

Continuous Diagnostics and Mitigation (CDM)
CounterACT addresses key requirements for the U.S. Federal Government's CDM approach to cybersecurity and can serve as the centerpiece of your solution, ensuring continuous hardware and software visibility, monitoring and reporting for comprehensive asset management.

Continuous Monitoring and Mitigation (CMM)
CounterACT capabilities go beyond asset discovery, monitoring and reporting to address the needs of public sector agencies. CounterACT also provides advanced access control and remediation capabilities as well as a broad range of ControlFabric integrations with best-in-class network, security, mobility and IT management solutions.

> **"ForeScout improved the visibility into what was connected to the network and helped enforce security policies on devices."**
>
> **– Chief Information Officer, U.S. Federal Government**

Seeing Is Believing

CounterACT is sold as either a virtual or physical appliance that deploys within your existing network, typically requiring no changes to your network configuration. Learn more at www.forescout.com.

ForeScout

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591
Fax 1-408-371-2284

The ForeScout Solution

If there is one thing that is universal among all government agencies, it's the necessity to continuously improve security and prove compliance. Many agencies at all levels of government use ForeScout CounterACT® for both purposes.

CounterACT's military-grade security protects many of the network infrastructures of the DoD as well as those of its military contractors and suppliers. ForeScout CounterACT is certified at the Common Criteria EAL 4+ level, the industry's highest security certification for Network Access Control (NAC) solutions. It is included in the DoD's Defense Information Systems Agency (DISA) Unified Capabilities Approved Products List (UC APL) of those that have completed Interoperability (IO) and Information Assurance (IA) certification, demonstrating that it meets the government's high standards for security, ease of use and deployment, low end-user impact and interoperability with existing remediation solutions and infrastructure-agnostic requirements.

In more than 60 countries*, ForeScout helps government agencies at the federal, state and municipal levels meet the numerous access control and continuous endpoint compliance requirements with an agentless, easy-to-deploy and scalable solution. Government agencies use ForeScout CounterACT to protect their critical network infrastructure and sensitive data, measure compliance with security policies and improve operational efficiency. Here's how:

See CounterACT offers the unique ability to see devices the instant they connect to government networks, without requiring software agents or prior knowledge of the device. It sees devices other products simply can't, such as smartphones, tablets, laptops and other agency-owned and personal mobile devices as well as Internet of Things (IoT) devices, and even detects stealthy sniffer devices that do not utilize an IP address.

Control Unlike systems that flag violations and send alerts to IT and security staff, ForeScout CounterACT actually enforces network access control, endpoint compliance, mobile device security and threat control, in one automated system. As a result, citizens, contractors and government employees can access networks without compromising security. In addition, CounterACT continuously monitors devices on your network and improves the effectiveness of your security policies so you can demonstrate compliance with regulations.

Orchestrate CounterACT integrates with more than 70 network, security, mobility and IT management products* via its ControlFabric® Architecture. This ability to orchestrate information sharing and operation among myriad security tools allows you to:

- Share context and control intelligence across systems to enforce unified network security policies
- Reduce vulnerability windows by automating system-wide threat response
- Gain higher return on investment (ROI) from your existing security tools while saving time through workflow automation

1 http://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/
2 http://www.mirror.co.uk/news/uk-news/isis-hackers-intercept-top-secret-6428423
3 CNN Report—February 8, 2016
4 Regulatory legislation or standards: The Federal Information Security Management Act **(FISMA)**, North American Electric Reliability Corporation **(NERC)**, International Standardization Organization/International Electrotechnical Commission **(ISO/IEC)** and General Data Protection Regulation **(GDPR)**.
* As of January 2016

Version 9_16