FORESCOUT
Active Defense for the Enterprise of Things™

Securely Enable Government

Effectively monitor and manage cybersecurity risk to be combat-ready and mission-enabled

Government agencies maintain a wealth of data for effectively delivering government services, making them attractive targets for exploitation. Compounding this ever-present security challenge is the need to balance scarce labor, time and financial resources to support diverse agency missions and goals. In addition to responsibility for continuously ensuring cybersecurity and device compliance, agencies face auditing and reporting pressures due to regulatory requirements such as:

- Command Cyber Readiness Inspection (CCRI)
- Federal Information Security Modernization Act (FISMA)
- IRS Publication 1075
- CMS MARS-E

The Forescout platform helps to keep government operations available, secure and compliant

The Forescout platform actively defends the Enterprise of Things by **identifying**, **segmenting**, and **enforcing compliance** of every connected thing. The Forescout platform is the most widely deployed, scalable, enterprise-class solution for agentless device visibility and control. It deploys quickly on your existing infrastructure - without the need for infrastructure upgrades and accommodates both 802.1x and non-802.1x authentication.

The Forescout platform helps government IT and security professionals protect data, secure access to government resources and demonstrate compliance by addressing the following use cases for federal agencies and other public-sector entities.

> **"In the past it took two to three hours to find an infected machine and remediate it...With the Forescout solution we can find the right machine and shut it down within seconds."[1]**
>
> **PHIL BATES**
> **CISO, UTAH**

SOFTWARE INVENTORY

Identify unused or under-utilized software for cost savings and/or consolidation and remove outdated software that poses an increased threat due to legacy vulnerabilities. Gain visibility into authorized applications, rogue applications, operating systems, patch status and more.

Continuous asset discovery and profiling

The Forescout platform yields rich data about a variety of endpoints (IT, IoT and OT) without requiring software agents or previous device knowledge.

WHO ARE YOU?	WHO OWNS YOUR DEVICE?	WHAT TYPE OF DEVICE?	WHERE/HOW ARE YOU CONNECTING?	WHAT IS THE DEVICE HYGIENE?
• Employee • Partner • Contractor • Guest	• Corporate • BYOD • Rogue	• Windows, Mac • iOS, Android • Virtual machine • Non-user devices, IoT, OT	• Switch/Port/PoE • Wireless/ Controller • VPN • IP, MAC • VLAN	• Configuration • Software • Services • Patches • Security Agent

ACCESS CONTROL

Enforce a Zero Trust architectural framework and, through policies, limit access to information as well as service and application resources. NIST 800-207 outlines three core components of a Zero Trust (ZT) architecture: policy engine, policy administrator and policy enforcement point. The Forescout platform serves not only as the policy engine in a ZT environment, but also provides comprehensive data about connected devices that informs trust decisions.

COMPLIANCE

The Forescout platform continuously monitors for the presence of required software, unauthorized software, rogue devices and configuration changes – to help you meet regulatory requirements (e.g., CCRI, FISMA, IRS 1075, CJIS, PCI, HIPAA, etc.). The platform also provides real-time contextual updates to the asset database/CMDB, giving your teams a single source of truth for

"With the Forescout platform, we expect to save millions from exponentially faster audits that produce fewer findings and require less remediation effort."

PHIL BATES
CHIEF INFORMATION SECURITY OFFICER, STATE OF UTAH

accurate asset intelligence, governance, security operations management and reporting. Further, this visibility and control platform directly addresses or supports security controls in widely used security standards such as NIST 800-53 and the CIS Top 20 Controls, among others.

INCIDENT RESPONSE

Understand all connected devices, including unmanaged and rogue devices, to determine impact of known vulnerabilities and automate mitigation response (e.g., block, patch, etc.), saving labor and reducing time to repair. The Forescout platform provides rich device context so security teams can prioritize remediation of issues. In addition, policy-driven remediation actions can be triggered automatically by the Forescout platform.

SUPPLY CHAIN

Gain insight into embedded software and applications running on managed and unmanaged devices. NIST 800-53 Rev. 5 introduces a new "supply chain risk management (SR)" control family, which includes twelve controls and various sub-controls. Organizations should plan to implement controls related to provenance (SR-4) and supplier assessments and reviews (SR-6), among other things.

Contract Vehicles and Certifications

Contract vehicles

The Forescout platform is available through authorized Resellers and Distributors on the following contracts and purchasing schedules:

- GSA Schedules (Multiple Award Schedules and Federal Supply Schedules)
- NASA SEWP (Solutions for Enterprise-Wide Procurement) GWAC (Government-Wide Acquisition Contract)
- ITES/2H (managed and used by U.S. Army. Also used by DoD and other federal agencies)
- Encore II [managed by Defense Information Systems Agency (DISA)]
- Enterprise Software Initiative Blanket Purchase Agreement (ESI BPA) (managed by NIWC Pacific)
- Various state and local contracts (NY OGS, TX DIR, SC, NC, CA SLP, etc.)

The Forescout platform successfully identified Chinese-made surveillance cameras for removal as mandated by the National Defense Authorization Act for FY 2019.[2]

CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM)

CDM provides cybersecurity tools, integration services and dashboards to federal agencies to strengthen the security posture of the federal civilian enterprise. CDM works in four phases, each phase building upon the others: Assets (phase 1), Users (phase 2), Events and Boundary Protection (phase 3), and Data Protection (phase 4). Taking advantage of CDM phase 1 capabilities, security officials at the Department of Homeland Security found an average of 75 percent more assets than originally reported, and in some cases that number was as high as 200 percent.[3]

Forescout provides Hardware Asset Management (HWAM) capabilities to many civilian agencies. The Forescout platform can provide real-time, accurate asset intelligence across device types, organizational units and functions, and it integrates with configuration management database (CMDB) products from ServiceNow® and other leading vendors.

Certifications

Trust a solution with the highest levels of military-grade and government security certifications. Forescout has achieved the following U.S. Government certifications and compliances:

- U.S. Department of Defense Information Network Approved Products List (DoDIN APL) for **v8.X – DODIN APL LINK** (Search Forescout)
- FIPS (Federal Information Processing Standards) 140-2
- National Information Assurance Partnership (NIAP) Common Criteria Certification for **Forescout v8.1 – NIAP LINK**
- USMC ATO (Authority to Operate)
- U.S. Navy ATO (Authority to Operate)
- U.S. Army CoN (Certificate of Networthiness)

COMPLY-TO-CONNECT (C2C)

Comply-to-Connect (C2C) is a U.S. Department of Defense framework of tools and technologies that discover, identify and characterize all devices connecting to the network. C2C comprises a five-step process that begins with the ability to discover and identify assets in an agentless and non-disruptive way. Later steps of the framework include: Interrogate (step 2), Auto-remediate (step 3), Authorize Connection (step 4) and Situational Awareness and Enforcement (step 5).

Take the next step

To learn more about Forescout solutions for government agencies:

- Request a Demo
- Visit our website

1. https://www.forescout.com/company/resources/state-of-utah/
2. https://www.bloomberg.com/news/articles/2019-07-10/banned-chinese-security-cameras-are-almost-impossible-to-remove
   https://www.wsj.com/articles/u-s-government-still-uses-suspect-chinese-cameras-11571486400
3. Source: Interview with Kevin Cox, CDM Program Manager at DHS, https://www.meritalk.com/articles/cdm-the-story-so-far

Don't just see it. Secure it.™

Contact us today to actively defend your Enterprise of Things.

forescout.com/industries/government/ salesdev@forescout.com toll free 1-866-377-8771

FORESCOUT
Active Defense for the Enterprise of Things™

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

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

Learn more at Forescout.com