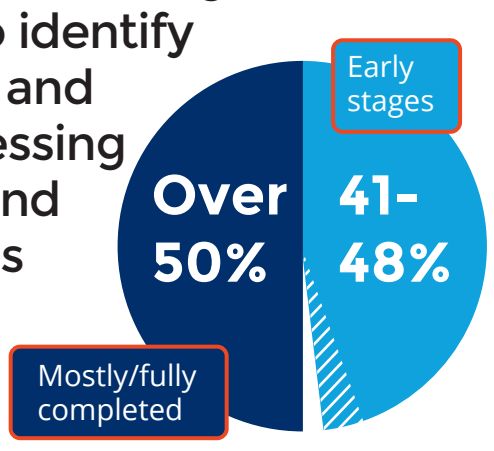
FORESCOUT

Ensuring Your Agency's ZERO TRUST Approach Reaches Every Network Device

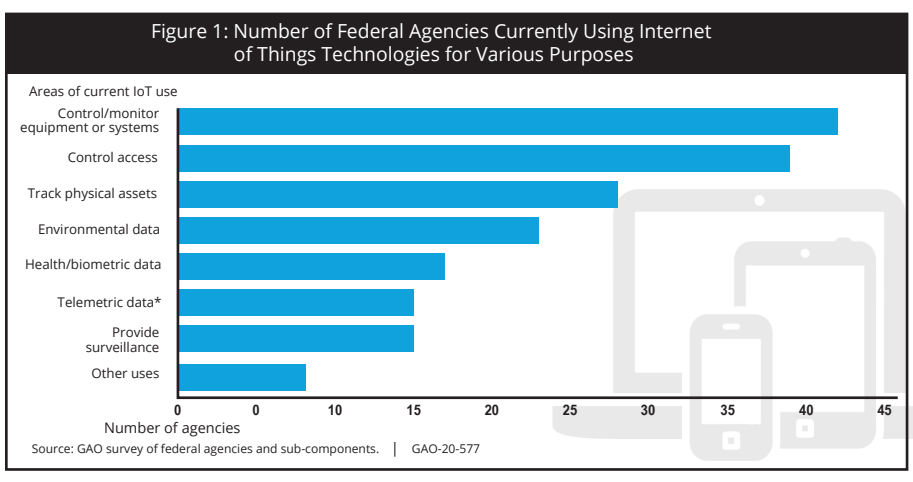
A Zero Trust approach to all government network devices is critical for cybersecurity

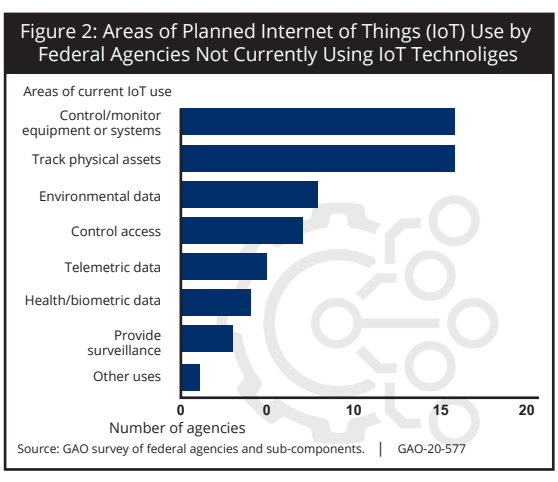
Agencies are making progress to identify the people and things accessing networks and applications



Source: https://www.fedscoop.com/government-agency-embrace-identity-access-strengthen-cybersecurity-study/

Top uses of IoT at government agencies





Global volume and diversity of connected devices

- Gartner predicts 25 billion by end of 2021
  (source: https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends)
- IDC predicts 41.6 billion by 2025
  (source: IDC, Worldwide Global DataSphere IoT Device and Data Forecast, 2019–2023, May 2019)

Work from anywhere

- 60% of U.S. government officials say pandemic has accelerated digital transformation
- Teleworking capacity increased by 800%
- Federal remote work to continue at least 3 days/week

Major IoT cyber-risks

- Smart buildings
- Medical devices
- Networking equipment and printers
- Outdated Windows workstations
- Security cameras
- VoIP phones

Focus your investments in 7 key areas

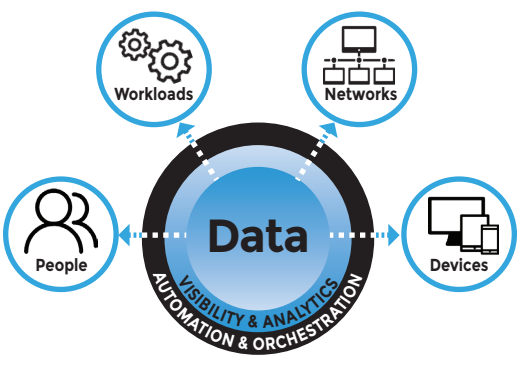


Figure 3: The seven dimensions of Forrester Research's Zero Trust eXtended Ecosystem Framework

"Visibility is the key in defending any valuable asset. You can't protect the invisible."
- Forrester

Forrester's Zero Trust eXtended (ZTX) Ecosystem

- Network isolation, segmentation, and security
- Data categorization, isolation, encryption, and control
- Protect workload application stacks
- Protect the users of network and infrastructure resources
- Automate/orchestrate Zero Trust controls and processes
- Provide visibility and analysis
- Comprehensive device visibility across the network

Continuous Diagnostics and Mitigation is a Zero Trust building block

The Department of Homeland Security's CDM program provides a phased set of capabilities and tools to address burgeoning cybersecurity threats:

- Continuously identify risk
- Prioritize risk based on potential impact
- Mitigate most severe risks

The binding operational directive (BOD) requires agencies to patch known vulnerabilities within a set time frame—from 2 weeks to 6 months, depending on severity.*

* https://www.cisa.gov/known-exploited-vulnerabilities-catalog and https://cyber.dhs.gov/bod/22-01/

CDM Zero Trust approach

Encompasses capabilities and tools for federal agencies in a phased approach

Phase 1: What is on the network? Continuous discovery and monitoring

Phase 2: Who is on the network? Identifying credentialed users

Phase 3: What is happening on the network? Continuous tracking

Phase 4: How is data protected? Securing data

See how your agency stacks up

CDM provider checklist

- Open platform that integrates with other security management tools so agencies can quickly find and remediate known vulnerabilities per BOD 22-01
- Comprehensive network visibility of all connected devices, control, and automation
- Continuously analyzes profile data and context from both the network and the device
- Automated, dynamic network segmentation based on device profile, context, and risk assessment
- Policy-based identification of known vulnerabilities to accelerate compliance with BOD 22-01
- CISA's CDM program partner and an experienced government solution provider*

*Forescout provides real-time asset management for nearly all federal agencies as the preferred solution for CDM hardware asset management (HWAM).

Forescout can help you meet Zero Trust and CDM requirements

Device visibility, analysis & control
- Agentless, continuous device discovery
- Real-time asset intelligence
- Continuous visibility & policy-based device control

Dynamic network segmentation capabilities minimize attack surface & breach impact
- Application, device, role & boundary-centric
- Dynamic network segmentation
- A Zero Trust access broker

Orchestrates & automates for speedier mitigation & response
- Sharing real-time contextual insight
- Automate workflows
- Automate response actions

Benefits
- Increase IoT security and overall device compliance
- Increase utility/value of existing IT security tools
- Fast deployment & cost savings from automation

FORESCOUT