Forescout Compliance Guide

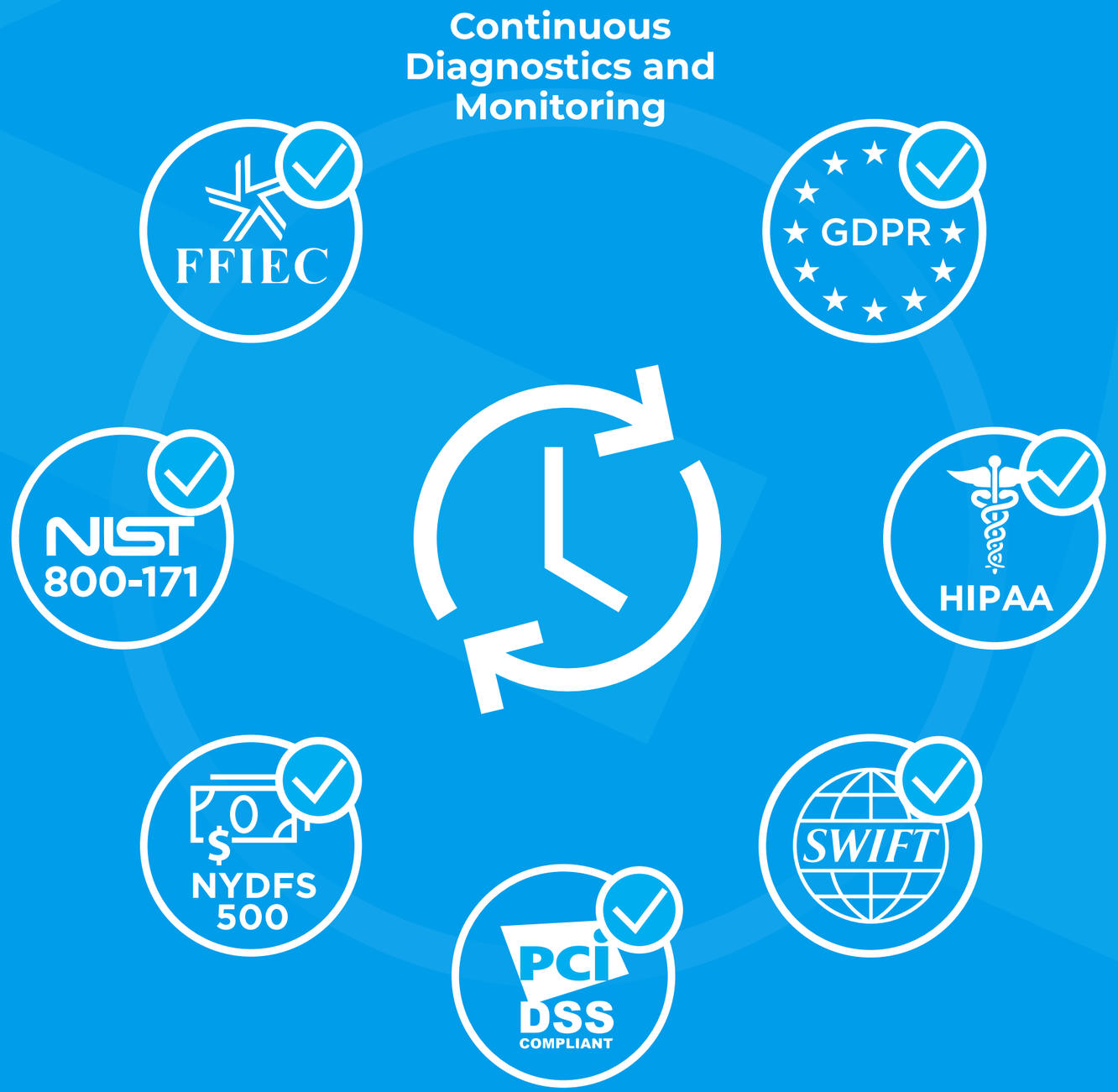


Table of Contents

Are you compliant? Are you truly secure?
New devices join your network every hour.

Compliance Preamble

Unknown devices join your network every hour—everything from unmanaged laptops, smartphones and tablets to servers, virtual instances, IoT devices and industrial systems of all kinds. These devices significantly expand your attack surface yet are invisible to many security products. Every unknown device represents significant risk to your endpoint compliance and, ultimately, your regulatory compliance strategy.

Effectively manage risk and address your regulatory compliance needs with the Forescout platform. This agentless solution provides the unique ability to see devices the instant they connect to the network, control them and orchestrate information sharing and threat response among disparate security tools. In fact, our platform is proven to dramatically minimize breaches and reduce reputational risk.

What Does Your Data Look Like?

Classified or Controlled Unclassified Information

Payment Card Information

Patient Health Information

Private Tax Information

Personally Identifiable Information

Data Security Concerns

6
Data Breaches

7
Data Privacy

8
Securing Financial Networks

9
National Security Concerns

10
Protecting PHI

11
Protecting Cardholder Data

USA Population: 327 million

Almost half of all Americans have had their health or other personal information breached!

Data Breaches

Up Close and Personal

PHI **Private Health Information**

54.25%

Between 2009 and 2017, over 176 million healthcare records in the U.S. were breached. That equates to more than 50% of the country's population (54.25%). Healthcare data breaches are now being reported at a rate of more than one per day. [1]

PII **Personally Identifiable Information**

43%

Equifax breach affected 43% of the U.S. population.[2]

PTI **Private Tax Information**

100k

The personal data of as many as 100,000 taxpayers was compromised, resulting in over $30 million in fraudulent tax returns.[3]

Data Privacy: *Dotting all the I's*

Whether you are securing financial communications or transactions, protecting patient medical records, students or employee and customer data or preventing loss of cardholder data, the first step to successful risk and compliance is absolute visibility.

See. Forescout's unparalleled ability to see IT, IoT and OT devices spans all sectors, territories and industries and provides support for dozens of frameworks, controls, mandates and regulations.

Control. Paired with this visibility is the ability to control and limit access by these devices to only areas and levels to which they are authorized, based on corporate security policy.

Orchestrate. Given that many of the current regulations, whether federal, state or global in nature, require breach disclosure within hours of a breach, it is critical that security platforms work together to remediate and respond quickly and effectively.

[1] https://www.hipaajournal.com/healthcare-data-breach-statistics/

[2] https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html AND https://www.census.gov/popclock/

[3] https://www.cnet.com/news/hackers-used-college-student-loans-tool-to-steal-30-million/

> "Voluntary compliance is the preferred route. But we will back this up by tough action where necessary; hefty fines can and will be levied on those organizations that persistently, deliberately or negligently flout the law." 1
>
> — UK Information Commissioner Elizabeth Denham, April 2018

Data Privacy

and Your Rights as a Data Controller

GDPR is here and it's a monster with large teeth. As the UK Information Commissioner said, the fines can be hefty. Due diligence on the part of the data controller is critical to avoiding and potentially lessening the impact of a fine.

10 ways to define the fine[2]:

1. Nature of the infringement
2. Intention
3. Mitigation
4. Preventive measures
5. History
6. Cooperation
7. Data type
8. Notification
9. Certification
10. Other factors

What do you need to do to assure your board that you're doing all you can to protect the company's data from well-publicized breaches and managing GDPR risk?

Do everything you can to identify the source of personal data

Know when a device connects to your network, who connected and the type of data they should be allowed to access.

Protect the personal data you own

Minimize the risk of lost or destroyed data by segmenting networks and controlling access to segments containing personal data such as HR or customer data.

Make sure your security vendors are teaming up to help you

Prevent and identify security breaches by orchestrating (sharing information) across your security solutions—the key to quick response and notification if necessary.

Learn More

GDPR: A Europe-Based Regulation with Global Impact White Paper

Addressing the EU General Data Protection Regulation (GDPR) Solution Brief

[1] Elizabeth Denham's keynote speech at the IAPP Europe Data Protection Intensive 2018, London, 18 April 2018: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/04/iapp-europe-data-protection-intensive-2018/

[2] https://www.gdpreu.org/compliance/fines-and-penalties/

Forescout delivers real-time discovery, classification, monitoring and policy-based management of devices as they connect to your campus or cloud network.

Securing Financial Networks

The changing IT landscape with cloud adoption, IoT and increasing IP-enabled devices makes it challenging to achieve and maintain regulatory compliance. Mitigating risk across the expanding attack surface requires coordination of both cybersecurity and IT management tools. IT audit and security teams are struggling to get a complete view of control gaps and effectiveness.

SWIFT HEADLINES

The financial services industry is increasingly targeted by cybercriminals, as recently confirmed by several reported SWIFT breaches at banks in Bangladesh, Ecuador and Taiwan.

MIFID II ADDS COMPLEXITY

MiFID II layers new complexities on a very complex regulatory landscape. Banks will need to monitor, record and secure all communications that may lead to a transaction while providing proof of compliance that they are doing so.

TAKING A BITE OUT OF THE BIG APPLE

Over 9 million New Yorkers had their personal records breached in 2017[1]—quadruple the number of New Yorkers affected in 2016, largely due to the Equifax breach. That represents 46% of the population of New York State.[2]

Forescout Supports MiFID II Compliance

MiFID II requires you to store large amounts of information for future audits. This requirement is being met today by expansion into cloud computing.

But as your workloads move to the cloud, how do you assess, classify and control devices and virtual machines that you can't see? How do you protect cloud-based workloads that are running on infrastructure not owned and operated by your enterprise? What about securing unmanaged and IoT devices?

Forescout delivers real-time discovery, classification, monitoring and policy-based management of devices as they connect to your campus or cloud network. Moreover, unlike traditional security management solutions, Forescout does not require onboard software agents or previous knowledge of endpoints. As a result, Forescout can offer a single-pane-of-glass perspective across campus and cloud environments so that you obtain visibility and control of physical devices, virtual machines and cloud instances, irrespective of where they reside.

1 https://ag.ny.gov/press-release/ag-schneiderman-announces-record-number-data-breach-notices-2017
2 https://www.census.gov/quickfacts/NY

> "When it's late at night, or when my staff is sleeping, Forescout is working with our other security solutions to take immediate action on threats. You can't put a price tag on that type of automation"
>
> — Michael Roling, Chief Information Security Officer, State of Missouri

National Security Concerns

Do you currently do business with the federal government and are focused on becoming DFARS/NIST 800-171 compliant?

Maybe you belong to a federal government agency and are subject to being compliant with NIST 800-53 controls.

Or, you're managing information security for one of the thousands of law enforcement agencies around the country and need to adhere to CJIS.

Forescout supports the protection of classified and unclassified information, regardless of the framework you use to comply with regulations or federal standards.

How we help:

1. IMPROVED ASSET INTELLIGENCE

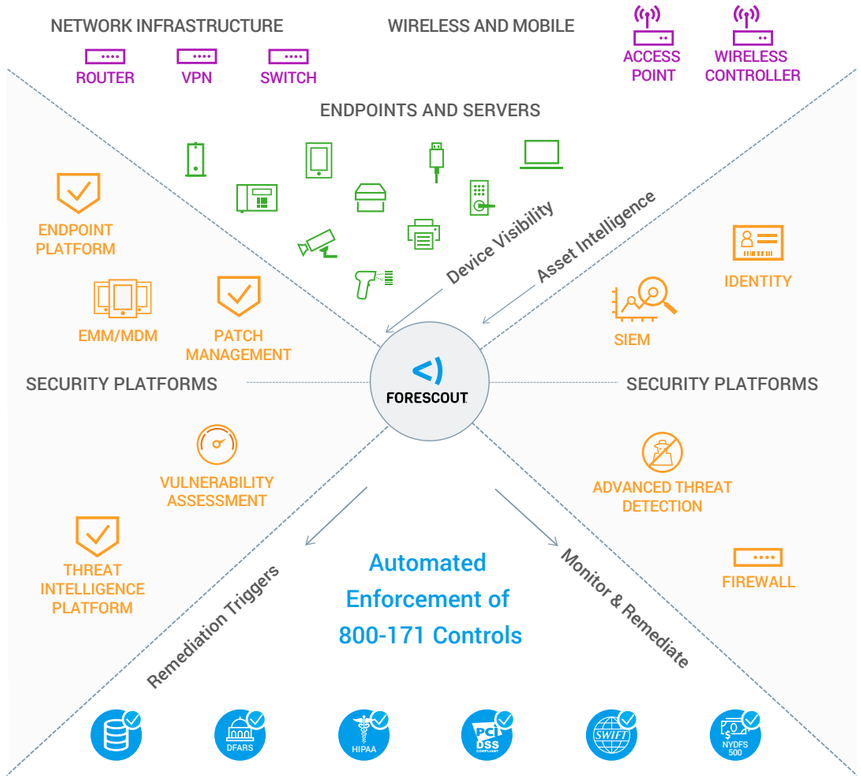
According to IDC, Forescout can help an organization see approximately 25% more devices than previously known.[1]

2. BUSINESS AND SECURITY PROCESS AUTOMATION

The Forescout platform helps government agencies at the federal, state and municipal levels meet their numerous access control and continuous device compliance requirements with an agentless, easy-to-deploy and scalable solution. It provides these groups with automated and continuous visibility and compliance.

3. ORCHESTRATION OF REMEDIATION TASKS ACROSS DOZENS OF SECURITY PRODUCTS

Forescout Extended Modules orchestrate information sharing and automate workflows among many of the security compliance tools in the federal government. Forescout plays a key role in enabling security personnel to share information between these tools and rapidly automate responses to incidents.



1 IDC Business Value of Forescout: https://www.forescout.com/idc-business-value/

> "Forescout was the only company that could meet all of the hospital's requirements. In any regulated environment like ours, that requires control over threats, Forescout provides tremendous value."
>
> — Alex Naveira, Network Engineer, Nicklaus Children's Hospital

Protecting PHI:

How HITRUST Helps Cover the Compliance Bases

The average global cost of data breach per lost or stolen record was $141. However, healthcare organizations had an average cost of $380, and in financial services, the average cost was $245.1

Challenges to protecting PHI

EXPLOSION OF BYOD

While many organizations are relaxing their BYOD policies to allow tablets and smartphones to be incorporated in the clinicians' and non-clinicians' daily work routine, many are just personal devices that employees choose to use for work-related tasks.

UNDETECTED MOBILE DEVICES

In line with the BYOD explosion challenge comes the problem of gaining visibility into hundreds, possibly thousands, of devices that enter or leave the healthcare network every day.

MEDICAL EQUIPMENT THAT STORE DATA

Many medical IoT devices are especially vulnerable since they cannot host third-party security agents, run outdated or unsupported operating systems, cannot be patched and often lack even the most basic security features.

The HITRUST Common Security Framework (CSF) is a superset of security controls and requirements derived from multiple standards and regulations, including HIPAA, PCI-DSS, NIST Risk Management Framework, FFIEC, GDPR and NYDFS 23 NYCRR500.

HITRUST was developed to provide a common framework that any healthcare or related organization can use to create, access, store or exchange protected health information.

The Forescout platform provides administrators with the critical ability to see and monitor myriad devices on the network in real time, from endpoints, such as PCs, laptops and printers, to IoT devices (including network-connected medical systems) and personally owned smartphones and tablets.

By helping to enforce the HITRUST CSF, Forescout helps healthcare organizations comply with these regulatory standards.

1 https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&

Nearly half (44.6%) of companies fall out of PCI DSS compliance within nine months of validation.

Protecting Cardholder Data

PAYMENT CARD BREACHES INCREASED BY 6% YEAR OVER YEAR…

The appeal of credit and debit card numbers continues to increase year over year.

"Nearly 20% of breaches in 2017 included credit and debit card information, a nearly 6% increase from last year."

— *Identity Theft Resource Center 2017 Year-End Review*

…AND YET, ONLY HALF OF RETAIL ORGANIZATIONS CAN CLAIM TO BE FULLY PCI DSS COMPLIANT.

"In 2016, for the first time, more than half (55.4%) of organizations were fully PCI DSS compliant at interim validation.

Nearly half (44.6%) of companies fall out of PCI DSS compliance within nine months of validation."

—*Verizon 2017 Payment Security Report*

The proliferation of point-of-sale (POS) systems, automated teller machines (ATMs), hand-held payment devices, kiosks and other endpoints increases the attack surface for hackers interested in financial gain by selling payment card information on the black market. Regulations such as the PCI DSS govern the way entities store, process and transmit cardholder data. Yet, only half of the organizations surveyed were found compliant with this standard. To effectively protect payment card data, entities must:

1. Realize that PCI compliance is not all there is to life. Strong security must be a superset of a risk and compliance strategy. Companies must be able to continuously validate that their cybersecurity strategy is fully capable of mitigating potential threats on their PCI networks.

2. Increase asset intelligence. How do you currently deal with shadow IT? The unknown point-of-sale system, the mobile payment devices? Are your known devices compliant with your corporate security policies? Are the agents updated and running?

3. Utilize network segmentation. Can you visualize all the traffic coming from IP-enabled devices on your PCI or Society for Worldwide Interbank Financial Telecommunication (SWIFT) network? Is the traffic safe or suspicious? When "safe" devices begin to act suspiciously, are they quarantined?

4. Reduce operational complexity by automating. Retail companies rely on having efficient systems with minimum downtime. Automation reduces the downtime involved in removing suspicious systems and returning them to full access.

1 https://www.idtheftcenter.org/2017-data-breaches

Regulations from A to Z

13

Continuous Diagnostics and Monitoring

14

Meeting FFIEC Requirements

16

Addressing GDPR Compliance

18

Supporting HIPAA Requirements

20

Automating NIST 800-171 Compliance

22

Becoming NYDFS 500 Compliant

24

Supporting PCI-DSS Controls

27

Simplifying SWIFT Compliance

Continuous Diagnostics and Monitoring

Forescout is Foundational for CDM Ongoing Assessment

Forescout ensures devices are allowed to remain connected.

The Continuous Diagnostics and Mitigation (CDM) program selected Forescout in Phase 1 as the de facto standard for Hardware Asset Management (HWAM) and visibility. Phase 1 and 2 of the program identify "what" and "who" are on federal networks. Phase 3 involves understanding what is happening on the network and Boundary Protection (BOUND).

Forescout satisfies the BOUND Network Access Control requirements to ensure:

- Devices are authenticated to remain connected
- Only authorized and compliant devices are allowed to connect
- Automatic remediation of noncompliant devices
- Devices are located in the appropriate logic segment of the network based on authentication and policy compliance

Learn More

Forescout: Foundational for CDM Ongoing Assessment Solution Brief

The Next Phase of Continuous Diagnostics and Mitigation (CDM) Solution Brief

Forescout provides the foundation for Continuous Diagnostics and Monitoring, as described below.

Establish and populate FISMA Containers	Populate devices within the enterprise into the appropriate FISMA containers for all the assets in HWAM seen and reported to the dashboard.
Security Controls Automation/ Implementation	Automate implementation of security controls in real time as devices connect to the network or change behavior and/or configuration.
OA OPERATIONAL REQUIREMENTS	
OR-1 Provide ongoing assessment data consolidation and assessment frequencies.	Forescout's ability to provide a continuous collection of data on endpoints connecting and disconnecting is critical to the organizational assessment (OA) process. Its policy-based decisions are scalable and can be mapped directly back to the controls required to both assess and then automate to reduce human interaction for the quick positive cyber hygiene that is required to "stay green" in the OA process.
OR-2 Complete the ongoing assessment activities so that mitigation responses and operational recovery can be completed.	Forescout's real-time visibility and real-world actions combined can mitigate threats and reduce or even prevent the exposure of others to newly assessed threats found in the information systems. Orchestration drives both the detection and the remediation/ control process while keeping pace and quickly scaling to over 2 million devices in a single Enterprise Manager deployment.
ONGOING ASSESSMENT MONITORING FUNCTIONAL REQUIREMENTS	
FR-1 Monitor for changes to the data elements/attributes for all CDM capabilities and report changes to CDM Operate, Monitor and Improve (OMI).	The Forescout platform evaluates the endpoint to detect changes to the data elements/attributes in real time. In accord with the OA process, it provides timely notification of changes and gives the ability to automate responses based on the security policy as it relates to the FISMA container controls.

Meeting **FFIEC** Requirements

Moving swiftly to address business technology needs while maintaining security and adhering to regulatory requirements can be an intense juggling act. Scaling effectively while reducing risk requires: 1) comprehensive asset intelligence, 2) automated policy compliance directed at devices as they access the network, and 3) technology tools that can be orchestrated to provide results leading to effective decision-making and rapid incident response.

Forescout reduces the risk of data breaches.

The Forescout platform supports and promotes a robust and effective information security program by providing a single-pane-of-glass view of endpoint and network control posture across campus, data center, cloud and OT networks. This capability addresses the need for access control, configuration control and protective control compliance. Forescout reduces the risk of data breaches and malware attacks by helping to ensure these controls are implemented completely and effectively at all times.

Forescout helps financial institutions meet FFIEC requirements as described below.

Control #	Definition	Forescout Value
II.A.2	Vulnerabilities	• Real-time inventory of every IP-addressable device on the network and, through orchestration using Forescout Extended Modules, can compare what has been scanned by vulnerability tools and initiate a scan for any missed devices or those that joined the network between scans. • Visibility into endpoints on the network, including applications and services running on these endpoints as well as servers which can be synced in real time with the CMDB or asset record database. • Visibility into network, infrastructure and endpoint configuration controls to help ensure complete compliance.
II.C.4 & II.C.5.	Control Implementation, Inventory & Classification of Assets	• Real-time visibility of endpoint agent-based controls, patching and configuration with orchestration capabilities to remediate automatically or initiate a remediation process. • Complements agent-based security with its agentless approach. The Forescout platform is infrastructure-agnostic and provides real-time visibility into configuration status and gaps for all network infrastructure independent of vendor. • Can validate that other security-tool-related processes are complete and compliant with policy, such as vulnerability management, logging and more. • Real-time visibility into endpoint- and network-based controls aligns with NIST and other frameworks. The Forescout Extended Module for Advanced Compliance enables organizations to leverage the SCAP standard to automate configuration and vulnerability assessment and provide security policy compliance metrics and many NIST and CIS benchmarks.

Meeting **FFIEC** Requirements (con't)

Forescout helps secure access to financial networks.

The Forescout platform helps you establish trusted and untrusted zones to protect financial data through network segmentation and network access control. It can automate security segment assignments and create access enforcement using policy-based assignment and enforcement of ACLs and VLANs. The platform enables real-time visibility into devices the minute they connect to the network, to automate and enforce policy-based network access control, endpoint compliance and mobile device security.

Forescout helps financial institutions meet FFIEC requirements as described below.

Control #	Definition	Forescout Value
II.C.9 & II.C.9(a)	Network Controls and Wireless Network Considerations	• Leveraging real-time visibility, Forescout automates asset inventory reconciliation to help ensure an up-to-date and accurate inventory. • Enables automated segmentation of network access by user, device classification and/or posture, regardless of how that device is connecting to the network—wired, wireless or VPN. Network segregation strategies can be deployed centrally through the Forescout platform
II.C.21	Business Continuity Considerations	• Forescout supports service resilience, high availability and disaster recovery across its hardware and software components through failover clustering and other options.

Learn More

Meeting FFIEC Requirements Solution Brief

Forescout Financial Services Solution Brief

Addressing **GDPR** Compliance

Forescout helps implement best practices for data privacy

The Forescout platform is a key component in GDPR readiness.

The GDPR is short on details, but it does provide solid guidelines for organizations to demonstrate accountability when it comes to data security. The GDPR requires organizations to assess the level at which private data is at risk and determine which practices and technologies will effectively reduce those risks. From there, next steps are largely left to each organization.

The Forescout platform is a key component of many organizations' GDPR readiness strategies because it is such an effective tool for strengthening data privacy and protection, reducing overall risk and demonstrating compliance.

Forescout helps organizations implement best practices for data privacy as described below.

GDPR Requirement	Forescout Value
Article 25 "Data Protection by Design and by Default"—Implement technical and operational measures to ensure that only personal data which are necessary for each specific purpose of the processing are processed.	The Forescout platform offers the unique ability to see devices the instant they connect to your network, without requiring software agents or previous device knowledge. It profiles and classifies devices, users, applications and operating systems while continuously monitoring managed devices, personally owned devices and other endpoints, as well as ports and connections. Centrally administered, it can dynamically manage up to 2 million devices in a single Enterprise Manager deployment.
Article 32 "Security of processing"—implement the appropriate technical and organization measures to ensure a level of security appropriate to the risk, including: a. The pseudonymization and encryption of personal data b. Ability to ensure confidentiality, integrity, availability and resilience of processing systems and services.	Forescout Extended Modules for SIEM enable bi-directional integration with leading SIEM systems. Extended Modules for SIEM combine Forescout's device visibility, access control and automated response capabilities with the powerful correlation, analysis and search features of SIEM solutions. The result is enhanced threat insight, analytics-driven decisions and greater operational efficiency. With Forescout and popular SIEM solutions, security teams can: • Store Forescout device visibility data in SIEM solutions for long-term trend analysis, visualization and incident investigation. • Correlate high-value endpoint context from the Forescout platform with other data sources to identify and prioritize incidents. • Initiate Forescout control via network and host actions from a SIEM to automate incident response, remediation and threat mitigation. • Demonstrate what personal data is accessed, by whom, how it is used and when it is deleted. • Forescout and Splunk customers can leverage the joint solution and Adaptive Response framework within Splunk ES for closed-loop remediation and threat mitigation.

Addressing **GDPR** Compliance (con't)

The Forescout platform can help you demonstrate compliance and avoid fines.

Forescout Extended Modules for Next-Generation Firewalls (NGFWs) enable IT teams to orchestrate dynamic network segmentation and create context-aware security policies within next-generation firewalls based on continuous device monitoring and extensive endpoint insight from the Forescout platform.

Forescout Extended Modules for Next-Generation Firewalls can also send GDPR compliance data collected by the Forescout platform on connecting devices back to the firewalls. So, for example, if a device's encryption is sub-standard, that information can be sent to the firewall and dynamically added to a rule that restricts access to certain services until the device is remediated.

Forescout helps organizations implement best practices for data privacy as described below.

GDPR Requirement	Forescout Value
Article 33 "Notification of a Personal Data Breach to the Supervisory Authority"—In case of a personal data breach the organization shall inform the security authority without undue delay and, where feasible, not later than 72 hours after they have become aware of it.	In the event of a data breach, a combined Forescout-SIEM solution can help you document your actions, demonstrate compliance to the GDPR supervisory authority and avoid fines.

Learn More

GDPR: A Europe-Based Regulation with Global Impact White Paper

Addressing the EU General Data Protection Regulation (GDPR) Solution Brief

Supporting **HIPAA** Requirements

Forescout helps healthcare organizations build and maintain a secure network, drive a vulnerability management program, implement strong access control measures, monitor and test networks and maintain an information security policy.

Forescout can help secure and protect electronic health records.

IoT adoption is increasing network attack surfaces by opening up more entry points for stealing protected electronic health records. Forescout supports the HIPAA Administrative, Technical and Physical safeguards and can help you identify devices that enter or leave your network, providing you with the ability to control the access these devices should have to network resources and data.

The bottom line is that Forescout sees IP-addressable endpoints, manages those endpoints through policies and rule sets, and integrates with current security tools to help meet requirements for continuous monitoring, enable security procedures, and implement automated responses to secure and protect electronic health records.

Forescout supports the HIPAA Administrative, Technical and Physical Safeguards as described below.

	Safeguards	Forescout Value
Administrative	Security Management Process	The Forescout platform can continuously acquire, assess and take action on new information in order to identify vulnerabilities, remediate noncompliant or compromised devices and minimize the window of opportunity for attackers.
	Security Incident Procedures	Forescout can integrate with third-party advanced threat detection (ATD) and SIEM systems to provide actionable threat information that the policy manager can use to isolate or initiate remediation actions.
Technical	Access Control	The Forescout platform provides critical capabilities for enforcing access control: • Enables limitation of access to healthcare information systems to authorized users, processes administered on behalf of authorized users or specified devices/information systems. • Can integrate with a variety of third-party authentication systems to validate unique identity and users prior to providing role-based network access. • For managed devices, Forescout can identify the users currently logged in and their account types. It compares these with policies for the device and user. If discrepancies are found, Forescout can restrict or deny access. • When a remote device requests a network connection, Forescout's initial scan can identify the type of connection and restrict or deny access if the endpoint posture is compromised. At the same time, it can evaluate the device configuration, installed software and patch levels for compliance with security policy.
	Audit Controls	When a device requests network access, the Forescout platform's initial inspection can determine whether logging is enabled and how it is configured, including the chosen location for log storage.
	Person or Entity Authentication	Just as the Forescout platform scans connecting endpoints to assess their configuration and inventories installed services, it can also conduct similar evaluations of network devices and network-based security infrastructure.

Supporting **HIPAA** Requirements (con't)

Forescout can help secure and protect electronic health records.

The Forescout platform helps overcome limitations with its agentless approach and its support for heterogeneous systems.

In addition to playing a critical role in securing devices and networks, the Forescout platform can also orchestrate and enable a variety of security tools to share information and work together. This orchestration allows enterprises to integrate and automate their security responses while also helping them to support compliance and standardization goals as well as preserving their investments in existing security tools.

Learn More

Addressing the HIPAA Security Rule with Forescout Solution Brief

Forescout supports the HIPAA Administrative, Technical and Physical Safeguards as described below.

Safeguards		Forescout Value
Physical	Device & Media Controls	The Forescout platform can help ensure that relevant third-party protection software is installed, correctly configured and operational. Connecting devices can be evaluated as part of Forescout's access inspection, and non-conforming hosts can be quarantined or removed from the network until repaired. It can identify open ports, active protocols and services currently running, and compare that inventory with configuration policies for that host. It can also restrict or deny access for noncompliant devices and issue a user notification or remediation alert.

Automating **NIST 800-171** Compliance

The Department of Defense requires all its contractors (providers of goods and services) to comply with NIST 800-171. Prime contractors also need to ensure the mandate flows down to their subcontractors. All entities must report breaches within 72 hours of discovery.

Forescout eliminates blind spots and improves process workflow automation.

Noncompliance can lead to loss of contract, disbarment and reputational risk and a negative impact on the company's brand, leading to loss of revenue.

800-171 compliance requires full visibility into any source of data that might contain Controlled Unclassified Information (CUI) which, quite frankly, is a very broad category.

Forescout addresses 12 of the 14 NIST 800-171 families. With visibility into devices connected to the network, Forescout provides direct or supplemental support for over 80 percent of the technical controls. The Forescout platform does not require agents to detect devices as they connect to the network. It automates simple and repeatable tasks and infuses those elements into existing IT security and management services: eliminating blind spots and improving process workflow automation.

Forescout provides automated NIST 800-171 compliance as described below.

Control Family	Forescout Value
Access Control	The Forescout platform identifies users attempting to access controlled unclassified information they are not authorized access to by their Active Directory group. It provides device- and role-based network authentication and authorization, allowing individuals and their devices to get their identified network access determined by VLANs or ACLs.
Audit & Accountability	When a device requests network access, the Forescout platform's initial inspection can determine whether logging is enabled and how it is configured, including the chosen location for log storage.
Configuration Management	The Forescout platform can protect against vulnerabilities by ensuring systems are configured based on defined corporate security policies: • Detect hosts without an installed antivirus application, one with no running antivirus or threat signatures that are not current. • Deny or quarantine endpoints without installed or functional antivirus and require that the endpoint be remediated before granting network access.
Identification & Authentication	The Forescout platform can deliver real-time enforcement of policies for non-privileged accounts.
Incident Response	Forescout Extended Modules for Security Information and Event Management (SIEM) facilitate information sharing and policy management improve situational awareness and mitigate risks using advanced analytics. The Forescout platform now includes the Device Intelligence Dashboard—a customizable web dashboard that providesa consolidated view of your device landscape and compliance across the extended enterprise. Security operations centers (SOCs) can use the device intelligence dashboard for incident response. During a threat outbreak or security incident, SOC operators can quickly get the device context they need, including device classification, connection, compliance and risk status at their fingertips. This eliminates tedious manual processes to identify devices, where and how they are connected to the network, and their current security posture.

Automating **NIST 800-171** Compliance (con't)

Forescout is used by government agencies to help protect critical network infrastructure.

Forescout helps government agencies at the federal, state and municipal levels meet their numerous access control and continuous device compliance requirements with an agentless, easy-to-deploy and scalable solution. The product provides these groups with continuous visibility and compliance. Government agencies use the Forescout platform today to protect their critical network infrastructure and sensitive data, improve their risk posture, measure compliance with security policies and improve operational efficiency.

The Forescout platform provides an extensive range of automated controls that preserve the user experience and keep business operations running to the maximum extent possible.

Learn More

- **Continuous Compliance with 800-171 White Paper**
- **Accelerate and Maintain NIST Compliance Solution Brief**
- **Campus Compliance Solution Brief**

Forescout provides automated NIST 800-171 compliance as described below.

Control Family	Forescout Value
Risk Assessment	Forescout's ability to see and control managed and unmanaged devices, including IoT devices on a network, reduces the risk of potential attacks and remediates malicious code or high-risk devices.
System & Comms Protection	The Forescout platform can help restrict communications between shared information sources to ensure that only approved devices and users are accessing the data residing on the shared source (such as a SharePoint server). This is a first step in ensuring that information control is in place, by controlling who and what has access to it.
System & Information Integrity	The Forescout platform can inventory network-connected systems to identify missing patches/security fixes, outdated antivirus signatures installed at the client host-based protection solution or holes in security assessments due to hidden or missing endpoints from the scan inventory. The benefit to the customer is knowing all systems are accounted for and reporting into their respective host-based security solution, ensuring they are secured by the latest protections.

Becoming **NYDFS 500** Compliant

The New York State Department of Financial Services (NYDFS) covers entities operating (domestic or foreign) in New York State subject to banking law, insurance law or financial services law.

Put broadly, compliance with NYDFS 500 requires entities to: 1) continuously conduct full technology risk assessments, 2) create and maintain an official cybersecurity program and 3) ensure cybersecurity policy and procedures are documented, communicated, educated and accessible. Additionally, financial entities are required to notify the superintendent of cybersecurity within 72 hours if a reportable cybersecurity event has occurred.

The cornerstone of continuous compliance is continuous visibility. The Continuous Diagnostics and Mitigation (CDM) program established by Congress is a dynamic approach to fortifying the cybersecurity of government networks and systems. CDM provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

Forescout provides ongoing assessment and remediation for endpoint's connection lifecycle.

Forescout helps you become NYDFS 500 compliant with the mandates as described below.

NYDFS Section/Sub-section	Forescout Value
500.02.b.1 – 5 **Cybersecurity Program**	The Forescout platform can continuously acquire, assess and take action on new information in order to identify vulnerabilities, remediate noncompliant or compromised devices and minimize the window of opportunity for attackers. The platform automatically initiates one or more of your policy-based enforcement and remediation actions, ranging from an email notification of noncompliance to mandatory remediation to outright quarantine or access prevention.
500.03.a; 500.03.c – h 500.03.m – **Cybersecurity Policy**	
500.05.a – b **Penetration Testing and Vulnerability Assessments**	Comprehensive integration with vulnerability assessment (VA) systems provide the means to initiate scanning of devices and automate policy-based enforcement actions as needed.
500.06.a.2 **Audit Trail**	When a device requests network access, the Forescout platform's initial inspection can determine whether logging is enabled and how it is configured, including the chosen location for log storage.
500.07 **Access Privileges**	The Forescout platform identifies users attempting to access financial information they are not authorized access to by their Active Directory group. It provides device- and role-based network authentication and authorization, allowing individuals and their devices to get their identified network access determined by VLANs or ACLs.
500.09 **Risk Assessment**	Forescout's ability to see and control managed and unmanaged devices, including IoT devices on a network reduces the risk of potential attacks and remediates malicious code or high-risk devices.
500.14.a **Training and Monitoring**	Forescout Extended Modules provide true security orchestration between Forescout and various protection systems. The combined solution can automatically detect indicators of compromise (IOCs) on your financial network(s) and quarantine infected devices, thereby limiting malware propagation and breaking the cyber kill chain.

Becoming **NYDFS 500** Compliant (con't)

Forescout can minimize the window of opportunity for attackers.

Forescout agentlessly detects devices as they connect to the network, automates simple and repeatable tasks and infuses those elements into existing IT security and management services. As a result, it can illuminate blind spots and improve process workflow automation. Forescout elevates your security strategy above traditional point-in-time security models (visibility through snapshots) to a Continuous Compliance Management program, providing ongoing assessment and remediation for the endpoint's connection lifecycle.

Learn More

Forescout Financial Services Solution Brief

Forescout helps you become NYDFS 500 compliant with the mandates as described below.

NYDFS Section/ Sub-section	Forescout Value
500.15 **Encryption of Nonpublic Information**	The Forescout platform gathers insights regarding the endpoint, its location, who owns it and what's on it. It can help to ensure that encryption and data loss prevention agents are working across the financial network's infrastructure. Forescout can grant or deny access based on device compliance and user authorization.
500.16 **Incident Response Plan**	With Forescout and popular SIEM solutions, security teams can: • Store Forescout device visibility data in SIEM solutions for long-term trend analysis, visualization and incident investigation. • Correlate high-value endpoint context from the Forescout platform with other data sources to identify and prioritize incidents. • Initiate Forescout control via network and host actions from a SIEM to automate incident response, remediation and threat mitigation. • Forescout and Splunk customers can leverage the joint solution and Adaptive Response framework within Splunk ES for closed-loop remediation and threat mitigation.
500.17.a.1 - 2 **Notices to Superintendent**	The Forescout platform helps satisfy the requirement for notifying the superintendent of cybersecurity within 72 hours by helping with incident response through visibility and control of devices on the network and integration with various solutions from Splunk® and ServiceNow®.

Supporting **PCI-DSS** Controls

The Payment Card Industry Data Security Standard (PCI DSS) is a global standard that governs the way entities store, process and transmit cardholder data. If you are an organization that accepts payment cards for any service or product, you are obligated to comply with PCI DSS.

Forescout can help prevent exploitation of system vulnerabilities.

Whether it's helping organizations build and maintain a secure network, drive a vulnerability management program, implement strong access control measures, monitor and test networks, or maintain an information security policy, Forescout plays a vital role in helping to keep cardholder data secure.

Forescout is uniquely positioned to help address a set of requirements in eight of the 12 key categories of PCI DSS 3.2 mandates. For example, you can:

- Detect hosts without an antivirus program
- Restrict access to cardholder data on a need-to-know basis
- Monitor and detect wireless access points connected to the PCI network

Forescout supports implementing PCI-DSS controls as described below.

PCI Requirement	Forescout Value
1. Install and maintain a firewall configuration to protect cardholder data.	The Forescout platform helps to protect systems from unauthorized access from untrusted networks: • Provides a list of open ports on PCI servers. • Identifies traffic attempts from the card holder data zone outside of the DMZ. • Restricts user and device access using device- and role-based access control. • Denies access and/or quarantines endpoints attempting to access the network without personal firewall software installed and functional.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.	The Forescout platform allows you to assess and identify IoT devices with factory default or weak credentials and automate policy actions to mitigate risk: Forescout uses agentless assessment to identify IoT devices accessible via SSH, Telnet and SNMPv2 protocols. You can then use the Forescout-provided IoT credentials library or your own custom credential library to identify devices using factory-default or commonly used credentials and SNMP strings in IoT devices. For high-risk devices with weak credentials, you can use Forescout policies to automate risk mitigation actions such as isolating or segmenting the devices until they are remediated.
5. Protect systems against malware and regularly update antivirus programs.	The Forescout platform can help to prevent the exploitation of system vulnerabilities by: • Detecting hosts without an installed antivirus application, one with no running antivirus or threat signatures that are not current. • Denying or quarantining endpoints without installed or functional antivirus and requiring the endpoint be remediated before granting network access.

Supporting **PCI-DSS** Controls (con't)

Forescout dynamically manages hundreds of thousands of endpoints from one console.

Most organizations find without compliance, there's chaos. The Forescout platform offers a set of unique technologies that works with your devices—managed and unmanaged, known and unknown, PC and mobile, IoT, embedded and virtual. The platform helps ensure that endpoints on your network are compliant with your anti-virus policy, properly patched and have the proper policy-sanctioned software.

The Forescout platform automatically identifies policy violations, remediates endpoint security deficiencies and measures adherence to regulatory mandates. In the retail industry, it is important to have reliable and efficient systems. The platform physically installs out of band, avoiding latency or issues related to the potential for network failure, and works in heterogenous environents. It can be centrally administered to dynamically manage tens or hundreds of thousands of endpoints from one console. Forescout CounterACT provides organizations an efficient way to drive compliance toward a set of PCI DSS 3.2 requirements.

Forescout supports implementing PCI-DSS controls as described below.

PCI Requirement	Forescout Value
6. Develop and maintain secure systems and applications.	To help ensure that system components have the necessary patches, The Forescout platform can: • Identify endpoints without the latest known security patches and quarantine them until patched. • Identify traffic attempts between PCI Development, Test and Production Zones. • Segregate these environments by enforcing roles-based access. • Identify unauthorized user access to servers based on their Active Directory group.
7. Restrict access to cardholder data by business need to know.	The Forescout platform identifies users attempting to access cardholder information they are not authorized access to by their Active Directory group. It provides device- and role-based network authentication and authorization, allowing individuals and their devices to get their identified network access determined by VLANs or ACLs.
8. Identify and authenticate access to systems components.	The Forescout platform integrates with a variety of third-party authentication systems to validate unique identity and users prior to getting role-based network access. Forescout can also present the use policies to the users that attempt to access the card holder data zone.

Supporting **PCI-DSS** Controls (con't)

Forescout you define and deploy controls at your own pace.

The Forescout platform lets you allow, deny or limit network access based on device posture and security policies. It handles a full spectrum of control actions, making it simple to grant the identified level of network access to people and devices as you define and deploy controls at your own pace.

These capabilities help organizations processing credit card payments address components of PCI DSS 3.2 and more effectively secure their network, sidestepping the considerable costs, disruptions and brand damage that can result from data breaches and compliance failures.

Learn More

Addressing PCI DSS 3.2 Solution Brief

Forescout supports implementing PCI-DSS controls as described below.

PCI Requirement	Forescout Value
11. Regularly test security systems and processes.	The Forescout platform can help with continuous compliance by: • Monitoring and detecting authorized and unauthorized wireless access points connected to the PCI network. • Creating policies to automatically isolate rogue access points, as well as notifying personnel of discoveries. • Helping to ensure real-time vulnerability scan compliance with various third-party vulnerability scanners. • Performing vulnerability scans for endpoints and networks determined by policy. • Detecting malicious activity and integrating with third-party advanced threat detection and SIEM systems.
12. Maintain a policy that addresses information security for all personnel.	The Forescout platform presents the company's information security policy to employees and requires employees to acknowledge reading and understanding it.

Simplifying **SWIFT** Compliance

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) through its Customer Security Programme (CSP) provides a security framework to monitor and protect the SWIFT infrastructure.

Forescout agent-lessly detects devices as they connect to the network.

The SWIFT Customer Security Programme (CSP) is designed to drive security improvement and transparency for the world's financial community, and also to help customers prevent cyberfraud. As of January 1, 2018, any bank that uses the SWIFT network must comply with SWIFT's CSP.

SWIFT hacks happen when cybercriminals get in between the customer's network and the SWIFT network. There, they can change or reroute messages and even currency, making a successful SWIFT hack highly lucrative for cybercriminals. These cyberattacks can be prevented with a strong security posture and absolute visibility.

Forescout helps organizations implement controls to protect the SWIFT infrastructure as described below.

Control #	Forescout Value
1.1 Swift Environmental Protection	See and control devices on your SWIFT network, regardless of whether or not they have security agents installed. The platform automatically initiates one or more of your policy-based enforcement and remediation actions, ranging from an email notification of noncompliance to mandatory remediation to outright quarantine or access prevention.
1.2 Operating System Privileged Account Control	Integration with privileged account management (PAM) systems provides real-time agentless visibility into undiscovered local privileged accounts in the SWIFT infrastructure and automated response to threats based on holistic visibility into user activity, device security posture, incident severity and overall threat exposure.
2.2 Security Updates	The Forescout platform lets you identify missing patches on your endpoints and servers using a combination of native support and module configuration. You can then orchestrate resolution through a number of tools.
2.3 System Hardening	The Forescout platform provides the means to harden the SWIFT environment, covering operating systems and networks for Windows, Linux, VMware® and networks.
2.7A Vulnerability Scanning	Comprehensive integration with VA systems provides the means to initiate scanning of devices and automate policy-based enforcement actions as needed.

Simplifying **SWIFT** Compliance (con't)

Forescout helps build and secure networks.

Forescout plays a crucial role in helping ensure your SWIFT CSP compliance in all four SWIFT deployment architectures A1, A2, A3 and B. For example, Forescout helps SWIFT customers build and maintain secure networks, drive their vulnerability management programmes, implement strong access control measures, monitor and test networks and maintain information security policies.

Forescout helps organizations implement controls to protect the SWIFT infrastructure as described below.

Control #	Forescout Value
4.1 Password Policy	The Forescout platform integrates with existing directory systems to assist with password policy enforcement and management: • Enforce network-based remediation for devices with users violating password policies. • Pop up a browser message or send an email when password is close to expiration to aid usability.
5.1 Logical Access Control	The Forescout platform gathers rich contextual insights regarding the endpoint, its location, who owns it and what's on it. It can help to ensure: • Unauthorized devices and unsanctioned applications are not on your SWIFT network. • Authorized devices are configured with the latest operating systems, up-to-date antivirus software is installed and running, and vulnerabilities are properly patched. • Encryption and data loss prevention agents are working across the SWIFT infrastructure. • Users are prevented from running unauthorized applications or peripheral devices on thenetwork. • Access is granted or denied based on device compliance and user authorization.
6.1 Malware Protection	Forescout Extended Modules provide true security orchestration between Forescout and various protection systems. The combined solution can automatically detect indicators of compromise (IOCs) on your SWIFT network(s) and quarantine infected devices, thereby limiting malware propagation and breaking the cyber kill chain.

Simplifying **SWIFT** Compliance (con't)

Forescout extends the reach of existing IDS and IPS systems.

Forescout integrates with more than 70 network, security, mobility and IT management products via Forescout Base and Extended Modules*.

Forescout physically installs out of band, avoiding latency or issues related to the potential for network failure, and works across heterogeneous environments. It can be centrally administered to dynamically manage more than one million endpoints from a single console. Forescout provides organizations an efficient way to drive compliance toward the SWIFT CSP.

Learn More

SWIFT CSP Solution Brief

Forescout Financial Services Solution Brief

* As of December, 2017

Forescout helps organizations implement controls to protect the SWIFT infrastructure as described below.

Control #	Forescout Value
6.4 Logging and Monitoring	Forescout Extended Modules for Security Information and Event Management (SIEM) facilitate information sharing and policy management via Forescout and leading SIEM systems to improve situational awareness and mitigate risks using advanced analytics.
6.5A Intrusion Detection	Forescout extends the reach of existing IDS and IPS systems through Forescout Extended Modules. • The IDS/IPS system detects an intrusion and notifies Forescout. • Forescout takes network or endpoint remediation actions, such as quarantining or performing an endpoint antivirus scan.
7.1 Cyber Incident Response Planning	The Forescout platform plays a key role in incident response: • Visibility and control of devices on the network and integration with various solutions from Splunk® and ServiceNow®. • The Forescout Device Intelligence Dashboard, a customizable web dashboard, provides a consolidated view of your device landscape and compliance across the extended enterprise. During a threat outbreak or security incident, SOC operators can quickly get the device context they need, which eliminates tedious manual processes.

Demo

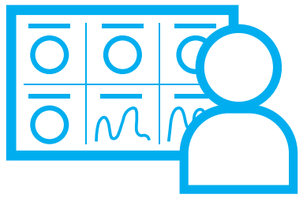
31

Take a
Test Drive

Take a Test Drive

During your three-hour test drive, the Forescout crew will spin up virtual sessions and take you through real-world cybersecurity scenarios. Everything you learn can be quickly applied to your environment using the Forescout platform.

TAKE A SPIN



Personal Demo

Want a hands-on demo right in your office? Set up a meeting with a Forescout representative.

REQUEST A DEMO

Acronym Glossary

CIS: Center for Internet Security
CJIS: Criminal Justice Information Services
CMDB: configuration management database
DFARS: Defense Federal Acquisition Regulation Supplement
FFIEC: Federal Financial Institutions Examination Council
FISMA: Federal Information Security Management Act
GDPR: General Data Protection Regulation
HIPAA: Health Insurance Portability and Accountability Act
HITRUST: Health Information Trust Alliance
HWAM: Hardware asset management
IDS: intrusion detection systems
IPS: and intrusion prevention systems
MiFID II: Markets in Financial Instruments Directive II
NIST: National Institute of Standards and Technology
NYDF: NY Department of Financial Services Cybersecurity Regulation
PCI DSS: Payment Card Industry Data Security Standard
SCAP: Security Content Automation Protocol
SIEM: security information and event management

Forescout **Network Access Control** protects CUI data

Forescout **Continuous Firewall and Device Monitoring** detects advanced persistent threats (APTs) and indicators of compromise (IOCs)

Forescout **eliminates blind spots** and **improves process workflow automation**.

FORESCOUT®
Active Defense for the Enterprise of Things™

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

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners. **Version 1_19**