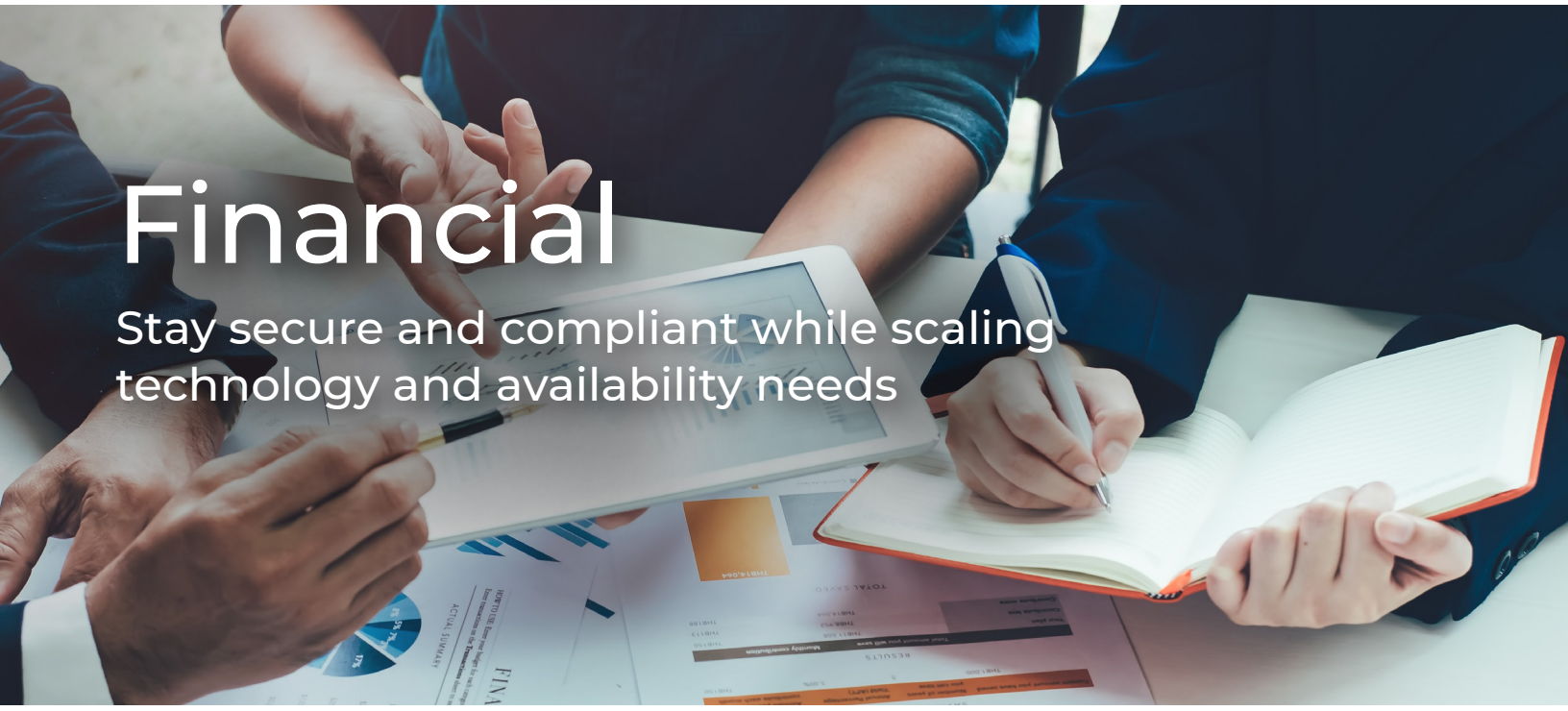

Financial

Stay secure and compliant while scaling technology and availability needs

> The Forescout platform told us so much more about each device, plus it gave us the automated, granular control capability that we were missing.
> **— Dale Marroquin, Information Security Officer, Credit Human Credit Union**

The security requirements of networks in financial institutions are extremely complex. Security and availability must match the speed of business.Regulatory compliance must be demonstrable. Business risk must be minimized and confidential customer data must be protected at all costs.Forescout achieves this by providing agentless device visibility and contextual intelligence, continuous monitoring as well as automated control that scales across the campus, data center, cloud and mobile workforce.

The Challenge

Financial services firms must innovate to succeed and develop cutting-edge services to meet client needs. To deliver these services, this requires on-demand scalability and available technology to a growing number of services and users. Complicating this requirement is how to dynamically extend security and compliance across evolving virtual and cloud-based business architectures.

Don't Forfeit the Need for Business Speed to be Secure and Compliant

The ever-changing landscape of compute, network, storage and mobility assets in financial services introduces security blind spots and non-compliant devices into the environment. Of course, non-compliant devices are potential entry points for hackers. And as critical applications increasingly interconnect and access each other's information, they add "east-west" traffic that circumvents many security controls, increasing the possibility that malware spreads and threats go unchecked.

Business Challenges

- Serve the business needs securely as technology demands evolve
- Minimize security risk and protect the business reputation
- Demonstrate regulatory and security policy compliance
- Preserve customer trust by protecting data privacy
- Increase staff productivity and service levels
- Improve security posture while reducing total cost of ownership

Technical Challenges

- Address risks to critical applications and processes across the entire network
- Continuously identify, classify and understand the status of all network-connected devices without disrupting the business
- Ensure dynamic but controlled network access and segmentation without hindering daily activities of employees, customers, partners and guests
- Guard against targeted malware threats

> "Forescout provides JPMorgan Chase with enhanced visibility and control across the hundreds of thousands of devices connected to our corporate network."
> **— Rohan Amin, Global CISO, JPMorgan Chase & Co.**

Minimize security risk exposure as you embrace operational agility

One of the key priorities of a financial services firm is to protect its assets, data, and applications while establishing the right balance of controls. Understanding your control status while meeting the dynamic business demands is difficult. Adding devices, servers, virtual machines and access to clouds hinders visibility, fragments control and adds business risk—all of which make it harder to stay in compliance.

Security solutions for financial services need to help consolidate control with a central view of the overall security posture. To effectively manage risk, security professionals need to identify the most critical processes, applications and technologies and match them with prioritized protections. Proper governance requires thoughtful intelligence to carefully build strict controls, including network segmentation to protect the "east-west" traffic and device access controls to restrict the threat access potential.

To overcome these hurdles, a security solution needs to provide comprehensive visibility across all technology resources using the same people and processes. This visibility must continuously offer insight in device and application security status to eliminate blind spots, build the foundation for proper controls, facilitate asset inventory and tracking. And lastly, the solution should protect without slowing access to critical business services.

The Forescout Solution

Forescout offers a security solution that provides visibility and posture status into extended network environments, while consolidating control to reduce risk and maintain compliance.

Exceptional Device Visibility

Forescout provides unparalleled insight into your entire device landscape without disrupting critical business processes. It starts by discovering every IP-connected device and virtual machine across your extended enterprise networks.

- See devices the instant they connect to the network. Continuously monitor the status as devices and virtual machines come and go
- Instantly detect issues that go unnoticed by point-in-time vulnerability scanning
- Auto-classify traditional IT, Internet of Things and OT devices (such as building automation) using a multi-dimensional classification taxonomy to identify device function and type, operating system and version, and vendor and model

Real-Time Asset Intelligence and Management

Build an asset inventory of all IP-connected network, data center, Internet of Things, and Cloud devices without impacting performance or reliability.

- Gain asset intelligence from connected devices for richer policies, segmentation and control
- Share contextual data with IT asset management (ITAM) tools or computerized maintenance management systems (CMMS) to build a more accurate asset inventory and maintenance solution

Automated, On-Connect Compliance

Ease compliance with on-connect status and simplify reporting with real-time compliance reports.

- Align with stringent security regulations such as MiFID II, GDPR, SWIFT CSP, FFIEC, SOX, and NYDFS[1]
- Increase auditing and compliance team efficiencies by 26 percent on average[2]

Policy-Based Access Control

Use the Asset Intelligence from Forescout to confidently enforce corporate policy-driven network access, using factors such as device type, ownership, security hygiene and vulnerabilities.

- Isolate legacy and noncompliant devices on your network to reduce cybersecurity risk
- Automatically notify users to remediate or eliminate staff workloads with auto remediation
- Ease guest or BYOD access. Visitors can receive internet access through a guest VLAN, and lobby kiosks can be placed on secure segments that cannot touch operational financial systems or sensitive customer privacy information.

Adaptive Segmentation

Standardize network segmentation policies and management across the firms' headquarters, data center, and cloud environments.

- Assign devices into network segmentation zones that contain similar policy and compliance requirements
- Leverage out-of-the-box integrations with next-generation firewalls for device-based policies
- Protect critical assets and minimize potential issues from “east-west” traffic that other security measures might miss

Orchestrate Information Sharing Among Leading Security Tools

Forescout extends agentless visibility and control capabilities to leading network, security, mobility and IT management products via Forescout eyeExtend Modules.

- Make your existing security investments work better and automate security responses
- Share context and control intelligence among systems to enforce unified network security policy
- Reduce vulnerability windows by automating system-wide threat response
- Provide a higher return on investment from existing security tools and save time due to enhanced workflow automation

Centralized Management and Control

Forescout eyeManage provides you with a single pane of glass to centrally manage and control multiple eyeSight and eyeControl instances in large network environments. This gives overall visibility and control of devices and Virtual Machines (VMs) across your campus, data center and clouds—streamlining your operations across your enterprise.

Scale

Forescout is proven in customer networks exceeding one million endpoints. This scalability is especially attractive in banking environments, where distributed branches are the norm, and where mergers and acquisitions are commonplace.

***Notes**

1. General Data Protection Regulation (GDPR), SWIFT Customer Security Programme (CSP), Federal Financial Institutions Examination Council (FFIEC), New York Department of Financial Services (NYDFS), Sarbanes-Oxley (SOX), Markets in Financial Instruments Directive (MiFID II)
2. IDC study: https://www.forescout.com/idc-business-value/ Learn more at www.Forescout.com
3. General Data Protection Regulation (GDPR), SWIFT Customer Security Programme (CSP), Federal Financial Institutions Examination Council (FFIEC), New York Department of Financial Services (NYDFS), Sarbanes-Oxley (SOX), Markets in Financial Instruments Directive (MiFID II)

FORESCOUT

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