FORESCOUT

Securing Your SWIFT Environment Begins with Absolute Visibility

> **It is absolutely critical to gain 100% visibility into all SWIFT components. 99.999999% isn't good enough. ForeScout believes absolute visibility should be non-negotiable and the way to achieve this is with an agentless solution."**
>
> — Steve Redman, Chief Marketing Officer, ForeScout Technologies

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 cyber fraud. As of January 1, 2018, any bank that uses the SWIFT network, must comply with SWIFT's CSP.

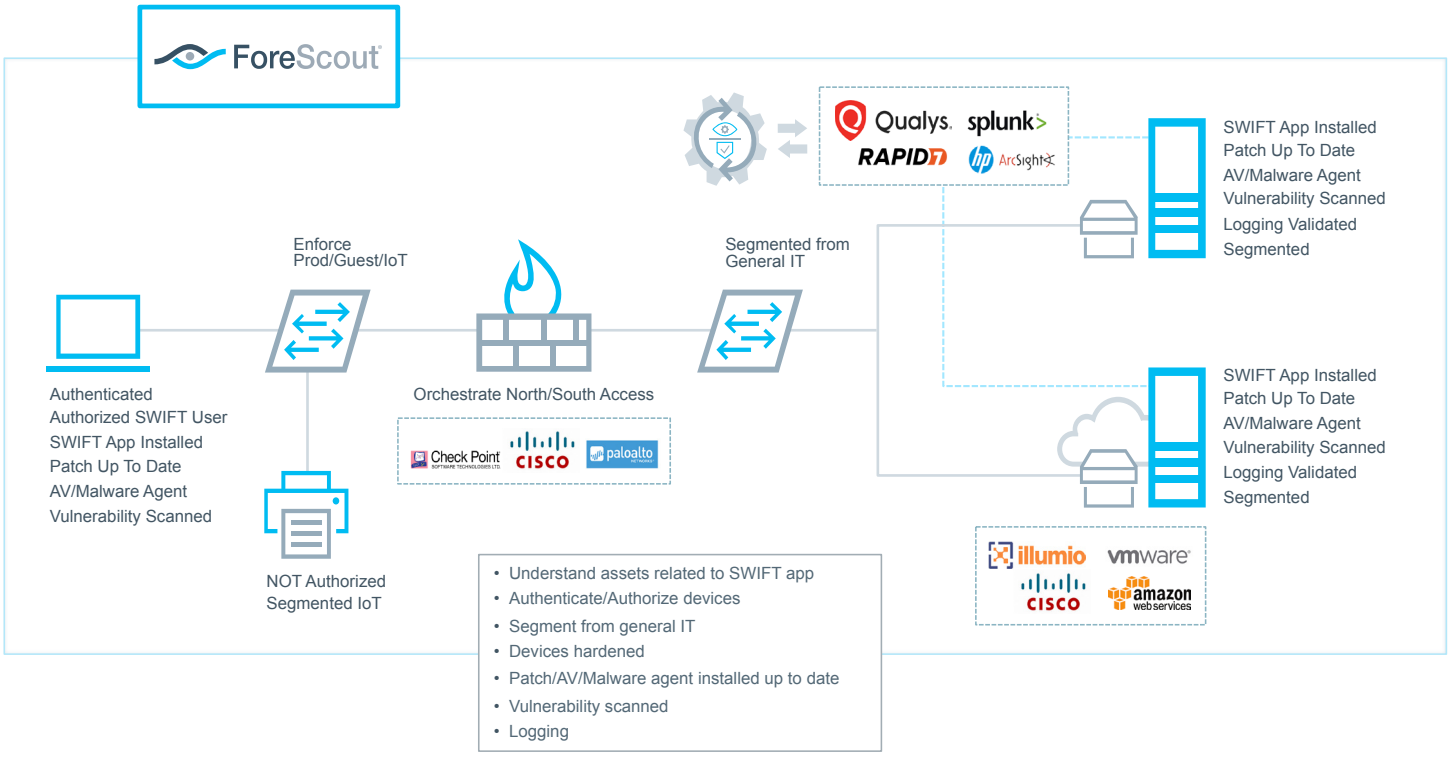
SWIFT hacks happen when cybercriminals get in between the customer's network and the SWIFT network. There, they can change or reroute messages and even currency, making a successful SWIFT hack highly lucrative for cybercriminals. These cyberattacks can be prevented with a strong security posture and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

Steve Redman, Chief Marketing Officer of ForeScout Technologies explains: "The number and severity of cyberattacks targeting SWIFT networks is growing. These attacks happen entirely through the customer enterprise, as opposed to the infrastructure that SWIFT owns and operates, putting the onus for security squarely on banks and businesses."

Transforming Security Through Visibility™

Security starts with knowing what is on your network: clients, servers, gateways, network fabric and vast numbers of Internet of Things (IoT) devices—many of which can't run agents. This is alarming given that anything left unseen is a potential attack vector. According to Redman, "It is absolutely critical to gain 100% visibility into all SWIFT components. 99.999999% isn't good enough. ForeScout believes absolute visibility should be non-negotiable and the way to achieve this is with an agentless solution."

ForeScout visibility, control and orchestration capabilities within a SWIFT environment.



Improve Cybersecurity at Business Speed with these Seven Tips:

1. **Gain continuous, in-depth device visibility.** Accurate device visibility and context are paramount to understanding and improving security posture. Ever-changing financial networks complicate this process as compute, network, storage and mobility assets join and leave the network.

   Solution: Use a device visibility platform that gathers asset intelligence continuously upon connection—without disrupting business operations—and shares real-time data with your configuration management database (CMDB).

2. **Consolidate governance and controls to manage risk.** Adding elastic compute, network, storage and mobility technology often requires highly specific, point-security solutions—fragmenting control and adding risk to your firm.

   Solution: Use the same people, processes and asset intelligence to build context and reinforce actions, and implement governance and policies leveraging segmentation and access controls.

3. **Implement granular network segmentation.** A well-formulated network segmentation strategy enables you to separate highly sensitive financial data and mission-critical applications.

   Solution: Leverage real-time asset intelligence to create security policies and determine the optimal network segmentation zones in the cloud or in virtual environments. You may choose to segregate device types across the campus, data center servers and the cloud.

4. **Secure and manage privileged accounts and credentials.** Exploitation of privileged account credentials is a common way for attackers to access sensitive financial data and applications.

   Solution: Use an agentless solution to gain visibility of accounts on all types of managed and unmanaged devices, including IoT devices. Next, automate policy-based access control and enforcement of these devices based on their security posture and behavior.

5. **Automate detection and response to strengthen defense.** Avoiding breaches is a top priority for the financial firms, yet security teams often don't know where to focus their attention due to too much data from disparate, disjointed security tools.

   Solution: Orchestrate security information sharing and workflows across your current SIEM, ATD and other security and IT management tools to get the most from your investments and accelerate incident response.

6. **Maintain consistent security and streamline compliance.** Financial institutions are impacted by up to 24 federal and state regulatory, oversight and examination agencies that require broad and deep technology controls.

   Solution: Extend continuous monitoring and security controls across your entire environment—from campus to data center to cloud—to ease compliance. Use an advanced network visibility solution to discover non-compliant devices and trigger/enforce updates.

7. **Scale security without disrupting critical operations.** Large-scale, global financial services firms often have hundreds of thousands of endpoints to secure. Flexibility and centralized management are key.

   Solution: Use a heterogeneous security solution that works across campus, data center and cloud environments—allowing you to manage a large number of endpoints with a single console for greater control and efficiency.

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