Customer Case Study

Prominent Bank is SWIFT Compliant with Simple Segmentation

Financial services company uses zero trust connectivity and micro-segmentation to meet SWIFT's Customer Security Program control requirements

Customer Requirements

- Isolate SWIFT systems and restrict Internet access
- Real-time mapping of all SWIFT network assets and communications
- Prevent credentials from being compromised
- Protect against horizontal L2-L4 network attacks
- Non-disruptive solution with no changes to the underlay network

Solution

- Micro-segmentation and native end-to-end encryption across the LAN, WAN, and cloud
- Isolated and encrypted overlay networks that restrict Internet access
- Maps all systems and associated communications across SWIFT environment
- Real-time attack mitigation and resource failover across the LAN and WAN
- Confidentiality, integrity, and authenticity of data flows

Benefits

- Simplifies CSP compliance reporting
- Reduces attack surface and vulnerabilities
- Demonstrates conformance with the SWIFT security controls
- Prevents credentials from being compromised
- Ensures local SWIFT infrastructure is protected against malware

Overview

A leading universal bank serves corporate and retail clients through a network of over 8,000 branches and nearly 3,000 ATMs. In preparation for new regulations from the Society for Worldwide Interbank Financial Telecommunications (SWIFT), the bank required new security controls to segment and safeguard regulated applications across their IT environment.

SWIFT has produced a compliance framework, the Customer Security Program (CSP). CSP includes mandatory segmentation to safeguard local SWIFT environments from the broader enterprise and external environment.

Challenges

On top of providing the necessary micro-segmentation controls to adhere to SWIFT's CSP, the bank needed a solution that worked seamlessly with its existing infrastructure—no rip and replace—and was quick to deploy.

The Solution

Upon evaluation of various network segmentation alternatives, the bank realized that the cost and complexity of meeting CSP requirements by deploying, maintaining, and auditing traditional IT solutions was impractical. Complex audits of individual firewall rules, ACLs, and VLANS would be unsustainable and multi-factor authentication is way too complex for users. Furthermore, because of the complexity and expertise required to restrict routes, deploy nested firewall rules, and restrict port forwarding across hundreds of subnets within a multi-NAT environment, deployment time for one site was estimated to take 50 days using traditional IT technologies.

Instead, the bank chose Tempered Networks' Identity Defined Networking (IDN) solution that made it simple to create zero trust overlay networks to securely connect, protect, and micro-segment any device, workload, or endpoint regardless of network or location. IDN gave the bank a simple path to comply with CSP controls, connecting critical SWIFT systems--even unrouteable ones--easily.

IT staff at the bank are now able to securely connect and isolate their SWIFT systems from the general IT network, easily. Unlike traditional IT solutions, with Tempered Networks their SWIFT environment is isolated across its own encrypted and segmented overlay network that can't be violated. With IDN, the bank deployed in less than a day because the creation of an encrypted overlay network can be performed in minutes.

Point-and-Click Segmentation of SWIFT Environment

The bank can transparently connect and control communications to, out of, and within its SWIFT environment to just the necessary systems that SWIFT requires to function. Boundary and host-level segmentation are both essential to the SWIFT security program's first and most foundational control: SWIFT environment segregation.

Real-Time Mapping of All SWIFT Network Assets

The bank now has real-time maps of all systems that are part of its SWIFT overlay environment. The real-time mapping gives them insight into the always-on security as well as verification of real-time mitigation activities, which are critical steps to securing SWIFT.

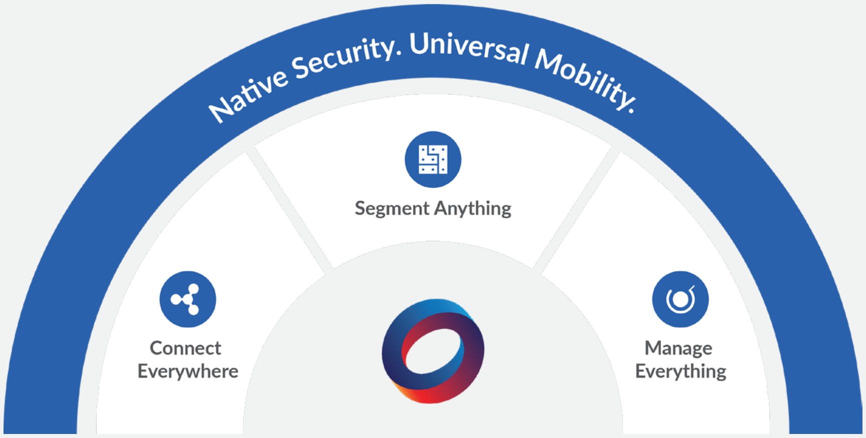
Fast Deployment With Low TCO

Since IDN removes the dependencies on the network for segmentation and protection, the bank has reduced ongoing IT operational complexity and implemented the solution in a few weeks, rather than months. The cost was about one-fourth of any other alternative available and was implemented and maintained by existing IT staff.

> **"Tempered Networks gave us a way to easily create segmented networks and real-time visibility of all systems in our SWIFT environment. Now our organization can quickly and easily generate reports about what is functioning inside our SWIFT environment and how it is being protected."**

Summary

Using Tempered Networks' unique identity-first approach for micro-segmentation, the bank has gained host-level security control and has successfully isolated and restricted Internet access to SWIFT systems. The IDN solution enabled the bank to easily achieve the necessary controls and compliance for SWIFT CSP, without disruption to existing infrastructure.



Experience the same simplicity, security, and cost-savings that our customers achieved.

To learn more or schedule a no obligation demo, email info@temperednetworks.com or visit www.temperednetworks.com