Cisco Stealthwatch for Financial Services

Achieve rapid threat detection and response

Cybersecurity threats in the financial services industry are extensive and growing. Phishing, ransomware, email compromise, and DDoS attacks are recurring challenges. Still, new vulnerabilities develop each time banking technologies and consumer behaviors advance. Furthermore, with each public attack, regulatory bodies work to combat bad actors and prevent setbacks to the industry's prosperity and reputation, adding new requirements for financial services providers to follow.

At the same time, leading financial services companies endeavor to compete with financial technology upstarts that combine cloud solutions with data analysis and artificial intelligence. To maintain their advantage, firms must integrate existing systems with new payment methods and evaluate digital currency networks. Meanwhile, consumers are rapidly expanding their use of mobile and social technologies to pay for daily needs. Because of these rapid developments, financial services executives must step up their cybersecurity resources and capabilities.

While advancing their security defenses, each company must also contend with a growing body of regulations with sometimes conflicting guidelines. European banks that fall short of General Data Protection Regulation (GDPR) privacy rules can face fines of up to €20 million or 4 percent of the company's global annual turnover.[1] When agencies request proof of compliance or a cooperative approach to new threats, a quick response is required. And in dealing with third-party services, scrutiny of their security and compliance is mandatory.

The confluence of these challenges presents an unprecedented need for a sophisticated and global approach to cybersecurity—to protect customers' assets and Personally Identifiable Information (PII), as well as corporate financial solvency. In fact, a recent report states that for each cybersecurity incident, a financial institution loses nearly a million dollars.[2]

[1] "The State of Cybersecurity Laws in the Financial Services Industry," Cisco, May 18, 2017

[2] "Financial Firms Hit with Million Dollar Losses per Cybersecurity Incident," Kaspersky Lab, March 27, 2017

Cisco Stealthwatch helps financial services companies:

- Increase awareness of currency and data theft threats
- Reduce the response time for fraud and cyberattacks
- Preserve records of historic user behavior
- Increase security posture and banking compliance
- Maintain customer trust and industry reputation

Elavon expands threat visibility and rapid response

Elavon, the world's fourth-largest payment processor, needed to understand its global network traffic patterns and quickly identify anomalous behavior to better secure valuable data. Identifying and mitigating attacks before damage was done required real-time network monitoring.

After deploying Cisco Stealthwatch and ISE, Elavon is now able to "monitor the network and detect threat activity when security personnel can't." Early detection yields faster response, and broad visibility provides event attribution to a specific user and device for improved incident investigation.

Network visibility and insight

Fortunately, financial services security and IT teams can address their technology challenges with the network visibility and analytics provided by Cisco Stealthwatch™ technology and complementary security solutions. Together, these solutions enable a "security everywhere" strategy that leverages the network as a critical sensor and enforcer, and protects against theft of money and data.

Cisco Stealthwatch provides financial services companies with the visibility to gain real-time situational awareness of network activity across banking and insurance divisions, legacy and Internet banking systems, and employee and transactional devices. Visibility is cost-effectively achieved by collecting NetFlow and other telemetry data from existing network devices such as routers, switches, and firewalls.

The Cisco Stealthwatch solution records and stores NetFlow data, which includes sender and receiver IP addresses, along with the time, date, and size of every network transaction. This insight is critical for obtaining a comprehensive view of network traffic, as well as additional context such as application-level awareness. And data can be used to prepare compliance and risk assessments for internal units and regulatory bodies.

With metadata collected directly from a company's existing infrastructure, Cisco Stealthwatch transforms the network into a powerful security sensor. Visibility scales across corporate and remote employee devices, brick-and-mortar locations, points of presence, and data centers without relying on expensive probes. And the solution monitors traffic from specialized devices in banks, insurance agent offices, and third-party locations that may not be compatible with endpoint-monitoring software.

Additionally, the Stealthwatch Cloud License allows financial services companies to extend visibility and threat detection to public, private, and hybrid cloud environments by deploying lightweight agents that collect telemetry from distributed locations.

“Stealthwatch ... provides so much insight into what is really happening within your network, and gives the best blend of advance notice [and] historic reporting.”

Experian

“Stealthwatch has dramatically improved my organization’s security posture.”

Erie Insurance

Security analytics and incident response

Cisco Stealthwatch transforms the volumes of collected telemetry from network infrastructure devices into actionable intelligence. Through the solution’s powerful analytics, security teams can rapidly identify and counter network attacks and help ensure the uptime of ATMs, POS units, online banking, and other critical customer services.

With Cisco Stealthwatch, even the most evasive and sophisticated security incidents faced by the banking and insurance industries are quickly identified. And unlike traditional security solutions that may overlook persistent and targeted attacks, the solution does not rely on signatures to detect threats.

Instead, it builds a baseline of expected behavior from each network host and triggers alarms when anomalous activity is observed. If attackers or unauthorized users gain entry and perform unexpected or prohibited activities such as fraudulent digital banking, back office system breaches, email phishing, or DDoS attacks, the solution identifies the threat and alerts responders.

Financial services industry compliance

Cisco Stealthwatch provides continuous monitoring throughout banking and insurance company networks to help ensure that every corporate and third-party activity is logged. Furthermore, it delivers the comprehensive visibility and analytics necessary to maintain and demonstrate PCI compliance, and compliance with a vast number of industry regulators including the Basel Committee, Commodity Futures Trading Commission, Consumer Financial Protection Bureau, Federal Reserve Bank, and National Association of Insurance Commissioners.

For compliance reports and forensic investigations, the Cisco Stealthwatch solution uses NetFlow to build a historic audit trail, which inspectors can use to quickly uncover the underlying cause of an incident. If a security threat is detected, the operator can identify the point of infection and track its propagation within minutes.

“Stealthwatch has helped us increase the visibility of our network’s edge points by 75% and ... detect traffic anomalies in a few minutes. It has saved us lots of money, but more importantly, it helps us to maintain our priceless reputation as a very secure financial services company!”

Elavon

Advanced endpoint awareness with Cisco ISE

The Cisco® Identity Services Engine (ISE), a complementary security solution, helps address the challenges associated with widely distributed financial services networks through its highly secure network access and endpoint awareness.

When Cisco Stealthwatch is integrated with Cisco ISE, additional endpoint information, such as user, device, credentials, and security policy compliance, is woven into the network audit trail. Investigators can quickly identify the person and device type responsible for suspicious traffic.

Additionally, ISE simplifies customer, contractor, and regulator guest access with automatic registration and access limitations. When needed, ISE can quarantine users and devices from the network after Cisco Stealthwatch identifies a compromised endpoint, leveraging the network as a security enforcer. This capability helps prevent the spread of infection through the isolation of POS, Internet banking, or retail location threats, for example, until the issue has been investigated and remediated.

When integrating Cisco ISE and Cisco TrustSec® software-defined segmentation with Cisco Stealthwatch, the combined solution dramatically reduces the network attack surface. Cisco TrustSec assigns a Security Group Tag (SGT) to each user and endpoint based on their role. Administrators can then develop and enforce dynamic and adjustable SGT-based policies to restrict users from accessing unauthorized resources without disrupting network availability.

Learn more

Together, Cisco Stealthwatch, ISE, and TrustSec can provide financial services companies with highly secure and responsive networks that better protect against data and currency theft. For further details on Cisco Stealthwatch, visit https://www.cisco.com/go/stealthwatch. To learn more about how to enable your financial services network with Cisco, go to https://www.cisco.com/go/financialservices.

C22-739378-00 08/17