cbts

Case Study

Financial Institution

Client: Financial Institution

Doing business for over 30 years, client is a leading provider of data-driven marketing, loyalty and payment solutions for consumer-facing companies worldwide.

Challenge	CBTS solution	Results
• Lack of visibility into the network to ensure performance and availability.	• CBTS installed and configured Gigamon's GigaVUE to capture and aggregate large volumes of network data.	• Client now has visibility into intra and internet data, reducing complexity and time spent troubleshooting.
• IT networking team was spending too much time managing large amounts of data.	• CBTS Implemented ExtraHop Reveal(x) 360 for cyber analytics.	• Timely and accurate insight with real-time analytics and machine learning.
• Unable to automate and provision security policies across the network.	• CBTS installed and configured Tufin for security visibility, analytics and centralized provisioning.	• A toolset that enabled management of rules that are easy to administrate via a central dashboard.
• Industry regulatory compliance requirements and need to ensure they've hardened their network	• CBTS security consultants performed network, phishing, and web application penetration tests.	• CBTS provided findings reports that prioritized vulnerabilities and recommendations by severity, priority and difficulty.

Security challenge

As a financial institution, the client maintains a large, complex, mission critical network. Monitoring of the network for security, performance and capacity had expanded beyond the capabilities of the wide variety of existing toolsets.

Because of the complexity of the network and the amount of data received, IT operations were spending too much time monitoring and troubleshooting based off a lack of actionable information and comprehensive visibility.

Financial institutions are prime targets for hackers, making it necessary to be proactive in discovering IT security flaws. This, as well as meeting compliance regulations placed on the industry, make penetration testing a necessity.

CBTS security solution

Utilizing an integrated solution, CBTS designed, installed and configured Gigamon GigaVue to acquire network traffic from across on-premises and cloud environments. Working in conjunction with ExtraHop, CBTS installed and configured Reveal(x) 360 for real-time advanced analytics, and Tufin for centralized management.

To harden their network and meet industry compliance, CBTS security consultants performed several multi-phase penetration tests against the customer's network, applications, and end users, simulating real attacks using tools, methodologies, and targets that actual attackers would use.

Results

The client's networking team has gone from receiving incomplete raw network data, to real-time actionable insights with the necessary visibility and network traffic analytics to manage performance, security, and availability. Using the Tufin orchestration suite, a central repository of all the firewall rules and objects have simplified management across multi-vendor and multi-platform technologies and eliminated hours of repetitive cycles for the network operations staff, freeing time to focus on business objectives.

After completing all penetration testing, the findings from the assessment were compiled. CBTS consultants reviewed all vulnerabilities discovered and exploited, as well as all access and sensitive data that was obtained. Vulnerabilities were prioritized by severity, priority, and difficulty, and each was documented. Mitigation strategies and remediation recommendations were also developed for each vulnerability. All of this material was gathered and placed in a findings report, which also included an executive and technical summary. Client now has an actionable plan to remediate vulnerabilities for a more hardened network and to meet regulatory compliance requirements.

cbts

Security, covered.