Case Study

BANK FINDS A BETTER WAY TO FIGHT ADVANCED ATTACK CAMPAIGNS

The Challenge

The security operations team was frustrated by the lack of easy, fast network visibility on connections end-to-end. Getting a clear, fast end-to-end view was not practical through their existing, traditional toolset: endpoint security, ASA firewall, an intrusion prevention system, proxy servers — even their SIEM system. The SIEM was not user-friendly; detection and query took too long to get the information they needed. And they found they were still missing a lot of banking specific trojans and malicious activity across their network.

—

"There wasn't anything that we could log into that gave us a holistic view, a historical view, from the beginning to the end of a connection."

They needed to be able to conduct faster investigations on anomalous log activity, irregular network traffic and the lateral movement of malware. Specifically they wanted to detect tagged documents and the flow of traffic through their ASA firewalls. They also needed to be able to record investigations and PCAP details for potential forensics.

Considering the Alternatives

The security team knew that for the bank to meet their strategic growth objectives they needed a better solution. The team wanted a single advanced threat visibility and investigation platform, to meet their current requirements but also to grow with the bank. They asked five vendors to do a proof of concept on the following use cases:

- Provide end-to-end connection visibility
- Detect and investigate irregular or malicious activity
- Support a high-performance traffic archive
- Accelerate user-to-conversation workflows
- Provide context-driven investigation

—

About the Organization

Multi-National Banking Group

The bank currently offers a range of wholesale and retail banking, insurance, asset management and wealth management services through several different business units and regional partnerships. Delivering their innovative, client value propositions requires greater collaboration between business units and fast, secure data integration of different information systems.

Distributed endpoints rely upon up-to-date and secure information system integration to enable staff to make fast, well-informed decisions on the ground and deliver a superior customer experience. The bank is looking to digitally transformed services to further increase operational efficiencies and market share. Superior customer service backed by IT system stability is seen as a competitive differentiator.

ARBOR® NETWORKS

The Security Division of NETSCOUT

The Arbor Networks Spectrum won hands down:

—

"Compared to the other products the Spectrum system's ability to flag specific threats, to detect vulnerabilities from the end user perspective – from the beginning of the connection to the end – is light years ahead."

Take Control with Complete Network Visibility and Fast, Easy Network Threat Analytics

The Arbor Network's Spectrum platform provides easy, real-time flow and packet analysis for connections end-to-end. Designed with the user in mind, Spectrum's interactive UI allows users to easily zoom/pivot on visual representations of new indicators and, in many cases, automatically correlated network activity. Indicators can be mapped into groups, e.g. users, business function, and location.

Built-in investigation workflows and Arbor's Active Threat Level Analysis System (ATLAS) informed analytics provides complete, focused visibility into both past and present network activity. The Spectrum investigations module automatically aggregates related indicators, host profiles and network connections into a single view of an advanced threat. The Host Dossier helps track lateral movement within the network, providing a detailed view of network traffic between hosts and connection points of interest — end-to-end.

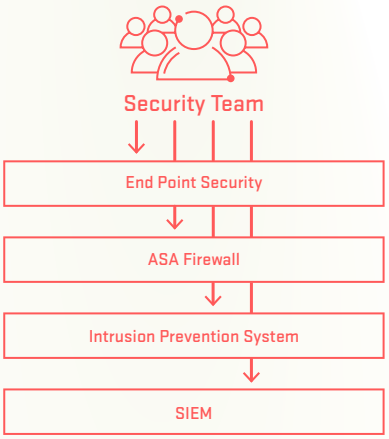
The security team is empowered to detect and connect global attack indicators to seemingly discrete events in their own network. ATLAS threat intelligence derives from the world's largest globally scoped real time threat analysis network. The hourly ATLAS Intelligence Feed (AIF) is fully integrated into Spectrum workflows and analysis; it provides internet scale visibility into the threats that matter most. Global threat indicators are connected to the organization's internal traffic patterns, much of it automatically through Spectrum profiles and workflows, to detect their most relevant and dangerous threats.

Spectrum enables the security team to rapidly search and pivot on months of past network traffic and user activity, turning days and hours of investigative work into seconds. Surface detailed threat activity with fast, scalable packet and flow analysis over current and past network traffic. The Spectrum platform enables disruptive, automated forensics with automatic packet capture of any threat indicator.

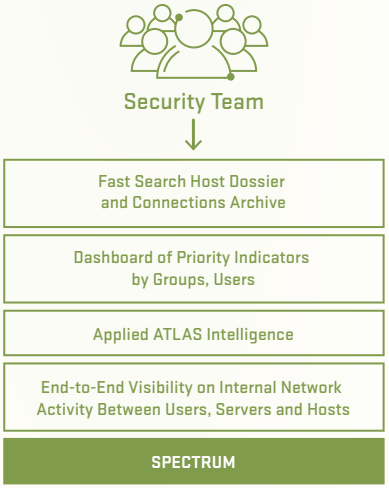
—

"Proxy guys, endpoint guys use it. Threat investigation teams use it for specific alerts. Perimeter guys use it. A lot of different teams actually use it."

BEFORE SPECTRUM



AFTER SPECTRUM



Benefits

The bank security operations team quickly achieved their goal of fast network visibility on connections end-to-end. They estimated they sped up their threat investigations 10x.

—

"Spectrum has given us true end to end visibility we never had before, and other solutions do not give. We are very happy with the solution, and service from Arbor. It has helped us reduce our mean time to detection considerably."

They are confident they can support secure systems growth and integration with The Spectrum platform. By leveraging host dossier capabilities and global threat intelligence during investigations they have been able to detect and mitigate more bank specific advanced malware that their other systems were missing, helping them diminish system vulnerabilities with a much greater degree of confidence. In fact, they are now looking at how Spectrum can secure their users, traffic and applications as they move into more Software Defined Networking (SDN).

What problems can the Arbor Spectrum Solution help you solve?

Visit www.arbornetworks.com/advanced-threat-arbor-spectrum for more.

—

About Arbor Networks

Arbor Networks, the cyber security division of NETSCOUT, helps secure the world's largest enterprise and service provider networks from DDoS attacks and advanced threats. Arbor is the world's leading provider of DDoS protection in the enterprise, carrier and mobile market segments, according to Infonetics Research. Arbor's advanced threat solutions deliver complete network visibility through a combination of packet capture and NetFlow technology, enabling the rapid detection and mitigation of malware and malicious insiders. Arbor also delivers market-leading analytics for dynamic incident response, historical analysis, visualization and forensics. Arbor strives to be a "force multiplier," making network and security teams the experts. Our goal is to provide a richer picture into networks and more security context so customers can solve problems faster and reduce the risks to their business.

To learn more about Arbor products and services, please visit our website at arbornetworks.com.

ARBOR NETWORKS

The Security Division of NETSCOUT

Corporate Headquarters
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA +1 866 212 7267
T +1 781 362 4300

North America Sales
Toll Free +1 855 773 9200

Europe
T +44 207 127 8147

Asia Pacific
T +65 6664 3140

Latin & Central America
T +52 55 4624 4842

www.arbornetworks.com

—

CS/BANKBETTERFIGHT/EN/0617-LETTER