CUSTOMER STORY

Government Agency Reconstructs Attack LifeCycle Using the FireEye Network Forensics Platform

SECURITY REIMAGINED

CUSTOMER PROFILE

United States Government Agency

ORGANIZATIONAL CHALLENGE

This U.S. government agency has several office locations, serviced by high-speed network links that faced a constant barrage of intrusion attempts by nation-state actors and highly structured organizations. Without a single source of aggregated traffic history across its distributed network, the entity's security team was spending an enormous amount of time researching the legitimacy of network alerts. There was no ability to quickly view network packets in real-time or an efficient way to conduct long-term flow analysis, limiting both detection and incident response performance.

An additional challenge was that prior to a new security measure being implemented there was no way to test its effectiveness using real network data. The team knew that having this capability would improve confidence in the prevention tactics that were being deployed.

SOLUTION

After an extensive survey of network forensic products, the agency chose the FireEye Network Forensics Platform, in part because it was capable of scaling to 10 GB/sec full duplex rates and could aggregate the organization's multiple links into a single appliance. The FireEye solution gives the agency the ability to capture traffic from all key network entry/exit points, data centers, and remote office locations.

By leveraging an intuitive set of APIs provided by the FireEye platform, integration with the existing SIEM dashboard was seamless, enabling immediate alert contextualization pivoting directly to packet data from network security and log events. The automated Pivot2Pcap capabilities facilitate real-time access to packets and NetFlow indexing is available for long-term analysis and integration with third-party tools. These features enabled the security team to save hours (and sometimes days) of time.

The FireEye Network Forensics Platform fulfills key requirements:

- Records and aggregates data and full packet capture on all network traffic across multiple high speed links, indexed for rapid analysis
- Validates the effectiveness of new security strategies against real network data

In addition to providing quick access to packet data from network events, the Network Forensics Platform gives the agency high-speed access to historical network traffic stored in standard packet capture (PCAP) formats, including NetFlow v5, v9, and IPFIX records. Indexed by time and flow information, the team can efficiently conduct long-term flow analysis and provide timely context during investigation and mitigation tasks.

Within weeks of deploying the FireEye Network Forensics Platform, the agency discovered a brute force login attempt. The incident response team was able to go back in time, view the attacker's actions, and reconstruct the kill chain to identify at-risk data on the compromised system.

BUSINESS BENEFITS

Some of the other benefits the agency has realized with the FireEye Network Forensics Platform:

- **More efficient use of resources:** Having a single source of aggregated network traffic data from the agency's multiple locations and the ability to pivot directly to packet data from the legacy SIEM solution permits faster analysis of network events and saves the security team hours of investigation time.
- **Enhanced incident response capabilities:** With its new ability to analyze long-term flow data, the team can rapidly reconstruct the kill chain to learn about attacker tactics, quantify the impact, and prepare better defenses for the future.
- **Cost effective distributed network traffic recording:** The aggregation of multiple links into a single capture appliance allow for extensive monitoring and visibility to be achieved at a centralized location.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**

FireEye