ANONYMOUS CASE STUDY

Wall Street Financial Services Firm Addresses Analyst Burnout & Encryption Blindness with LiveAction ThreatEye NV

Customer

Global Financial Services Firm

Challenges

- Alert Overload
- IDS No Longer Effective
- Encryption Blind Spots
- Limited Visibility of IoT Device Network Traffic
- Mapping Network Topology

Solution Evaluation

- Advanced threat detection, regardless of encryption
- Correlation with CrowdStrike threat intel
- Packet Capture for Forensic Analysis

Results

- Increased visibility to all network traffic
- High fidelity alerts to inform investigation
- Compliance: increased assurance
- Detection: Advanced threats, Including Ransomware & Insider Threat

New York, NY

The client is a top global financial services firm specializing in institutional trading, investment banking, research, and related brokerage services. It is based in New York and operates in 20 locations across the U.S., Europe, Asia, and Australia.

Wall Street Firm Faces Cybersecurity Challenge

Imagine a firm that provides visibility into investments around the world, losing visibility into its own network due to the increase in encrypted traffic. This global financial services firm found itself in that very situation, and their leadership decided to quickly rectify the problem.

As they began their migration from on-prem to a hybrid cloud infrastructure, company's IT and Cybersecurity teams were increasingly operating in the dark. Clients expect and the company delivers on its intent to keep confidential financial transactions private. It utilizes extremely high levels of encrypted network traffic to maintain both privacy and compliance. However, high levels of encryption created an enormous encryption blind spot.

The organization's Chief Information Security Officer says, "Traditional security tools, like our Intrusion Detection System (IDS), were no longer delivering value. Encryption blocked their ability to analyze most of our traffic."

IDS and other passive security tools depend on plain-text inspection to determine if traffic is legitimate or malicious. Now, with most network traffic encrypted, IDS and similar tools are obsolete.

This creates significant cyberrisk for organizations. Research revealed that in Q2 2021, 91.5% of malware arrived via encryption. Ransomware actors hide within encryption for lateral movement. And so do rogue employees. "Insider threat is a big concern in the financial services space," says the company's compliance officer, "and this concern has visibility at an executive level."

In addition to outdated tools, another significant challenge the organization faced was alert fatigue, which was leading to network defender burnout. The organization could not afford to lose valuable IT or security professionals in a job market where hundreds of thousands of positions remain unfilled.

Alerts without context or risk scoring wasted time, offered little direction for response and in most cases, were not worthy of investigation.

The Journey: Evaluating Network Detection and Response

While evaluating possible solutions, the global financial services firm wanted the following capabilities and benefits:

- Increase visibility into network traffic and topology, regardless of encryption
- Reduce and enrich alerts to decrease burnout & guide response
- Packet capture and recording (PCAP) for forensics & compliance
- Threat intelligence integration with its EDR (CrowdStrike)
- A platform that could benefit both SecOps and NetOps

It decided to evaluate Network Detection and Response (NDR) platforms to satisfy the list.

NDR is a key part of the SOC visibility triad. And NDR platforms continuously monitor, learning normal behavior on your network so they can detect rogue and malicious activity.

Why did the firm choose LiveAction ThreatEye NV?

With a primary concern around threat detection and encryption blind spots, the firm chose LiveAction's NDR approach, ThreatEye NV, because of the way it solves these problems.

Detecting Threats, Even Within Encryption

One thing the financial services team was impressed with is that LiveAction's Network Detection and Response platform analyzes more than 150 packet traits & behaviors. And it works across multi-vendor, multi-domain, and multi-cloud networked environments, scaled to process millions of events every second. It is a sensor deployed SaaS offering.

The platform uses a uniquely powerful approach to detect advanced threats unfolding on the network and enable rapid investigation. This is called Encrypted Traffic Analysis (ETA). Instead of relying on plain-text or data decryption attempts, it looks at the **behavior of traffic on the network regardless of encryption status.**

The fundamentals of this approach combine data collection, advanced behavioral analysis, and machine learning (ML). The ThreatEye platform analyzes traffic in real-time, strictly with flow data, and then aggregates and correlates multiple events to provide the context security teams need. This **complex event processing is powerful and feeds into** SOAR and SIEM.

PCAP for Forensics and Investigation

The global finance firm also wanted packet inspection (PCAP) and recording for forensics and investigation. It greatly valued the power of ThreatEye NV to drill down to a location, a single hop, a packet, or even a phone number. And it's long-term behavior analysis window makes this even more powerful.

Threat Intelligence Integration

Also, just as the company hoped, the LiveAction NDR platform correlates with the CrowdStrike threat intelligence service it uses. And many more, because of its vendor agnostic approach.

> With a primary concern around threat detection and encryption blind spots, the firm chose LiveAction's NDR approach, ThreatEye NV, because of the way it solves these problems.

Reducing Alert Fatigue & Analyst Burnout

The organization says its decision to deploy ThreatEye is paying off by greatly reducing the number of alerts network defenders must investigate. ThreatEye NV created alerts are high-fidelity, enriched, threat scored, and MITRE ATT&CK labeled. This reduces risk, saves time, and decreases the chance of a successful attack.

The importance of solving this problem cannot be overstated when you consider that more 6 out of 10 cybersecurity analysts intend to quit their jobs in the next year.

Alignment of security and privacy

ThreatEye NV does not require breaking and inspecting encrypted traffic, which is something the National Security Agency warned against. Instead, it uses Encrypted Traffic Analysis (ETA) and Deep Packet Dynamics (DPD) to understand all network behaviors while maintaining privacy, compliance, and cybersecurity.

What was the end result?

The firm reports increased network visibility, enriched alerts that lighten the burden on the SOC team, and senior leadership can report that advanced threat detection is now strong: from phishing to ransomware, to insider threat.

For more information:
https://www.liveaction.com/network-detection-and-response/

LiveAction provides unmatched visibility for network security and performance from a single source of truth.

LiveAction®