corelight

Case Study

Major mortgage lender deploys Corelight to unlock hybrid and multi-cloud visibility

AT A GLANCE

- 300+ locations across 49 states
- Visibility gaps in hybrid, multi-cloud environment
- Integration requirements with legacy solutions
- Security team divided into ops + engineering

BACKGROUND

This case study centers around a leading American mortgage lender and advisor with thousands of employees serving hundreds of branch locations across the US and over $70 billion in loans serviced.

The lead security engineer, responsible for their SOC's security tooling and engineering, wanted to bolster their network defense capabilities by closing key visibility gaps in their environment, which is distributed across on-prem data centers and the cloud—AWS and Azure.

CUSTOMER CHALLENGE

As a national lender, the company's network traffic is complex and highly distributed, including east/west traffic in corporate data centers and cloud. The security team needs to monitor key internal server infrastructure and user behaviors such as file share access activity, and the native logging capability of these systems left significant visibility gaps.

"We had a legacy network security product deployed that was something of a 'set it and forget it' product. The vendor managed it on our behalf and would alert us on some things, but we didn't have the visibility and access to the underlying data to be able to reliably validate and action those signals" said their lead security engineer.

> **"It was eye opening and a real wake up moment where we said: wow, ok so this is what is actually happening on the network!"**
>
> - Lead security engineer

The team wasn't getting the visibility or telemetry they needed, including EC2, RDS, and S3 related traffic in AWS instances. They needed a solution that would provide comprehensive, actionable data across their complex environment but also complement the visibility and detection capabilities offered by their firewall, CASB, and SASE solutions while natively integrating with their SIEM.

SOLUTION

To address these challenges, the security team needed an NDR platform that could seamlessly integrate with their SIEM, deploy across a range of environments, and provide high fidelity telemetry. They considered open source alternatives but were deterred by the time required to maintain a DIY solution, given the team's bandwidth.

Their lead security engineer recognized Corelight's strength in this space, offering the power of open source technologies in its commercial Open NDR Platform. "Going into the PoC I'm not sure we appreciated the full value of what Corelight can offer," he said, "When we actually got to dig into the data and detections it was eye opening and a real wake up moment where we said: *wow, ok so this is what is actually happening on the network!*"

Corelight also satisfied the Information Security Team's NDR solution requirements for SIEM integration and cloud deployment and he noted the responsiveness and high quality of service provided by Corelight's technical account management and support staff.

"There is so much unrealized wealth in your cloud network data that many organizations don't leverage," said the lead security engineer. "I would strongly recommend that security teams consider deploying NDR in the cloud to expand visibility and cover gaps unaddressed by the native security services of the cloud service providers."

RESULTS

The security team successfully deployed Corelight across their hybrid, multi-cloud environment and integrated it with their SIEM, unlocking comprehensive network visibility and expanding threat detection coverage with Corelight's security analytics powered by machine learning, behavioral analysis, signatures, and threat intelligence.

> **"This is awesome, we've never had this level of visibility before."**
>
> - Lead security engineer

Corelight's Open NDR Platform helped the company close blind spots and supported the security team's use cases, including:

- Spotting file extension changes in Corelight's SMB.log that could signal ransomware activity
- Monitor port and protocol usage in AWS to ensure policy compliance is maintained
- Verifying that corporate encryption policies were being followed

"We also held a working session with our SOC analysts using Corelight's Threat Hunting Guide to explore the data generated by the platform," continued the lead security engineer. "The analyst's reaction was so cool to see: 'This is awesome, we've never had this level of visibility before.' You could see light bulbs going off as they were brainstorming new ways they could proactively look for adversarial movement with the visibility Corelight unlocked."

corelight

To learn more, request a demo at **https://corelight.com/contact**

info@corelight.com | 888-547-9497