Reach

Case Study | Global MFG Co

A Threat-Informed Approach to Adopt SSL Decryption on Palo Alto Networks Firewalls

A global leader in the manufacturing industry knew the benefits of utilizing SSL decryption on their Palo Alto Networks firewalls, but were cautious to implement the capability. It's been a top priority for their IT Security Manager, an expert in PAN-OS, since joining the company. Since 80-90% of their network traffic was encrypted, extending visibility would allow his team to get a more complete picture of threats entering and exiting the network.

> “You're missing out on a huge chunk of your internet traffic if you're not implementing SSL decryption. The increase in visibility cascades to increased actions on the traffic, like file blocking and DLP, once you start getting this visibility.”

Concerns from the business around privacy and operational impact kept the project on hold for the better part of 6 years. Deploying this capability for all SSL traffic and to every employee in the workforce was not feasible. If he wanted buy in, the IT Security Manager knew he needed a data-driven, threat informed approach the rolling it out in phases, and to do so he needed to:

1 Identify who was being attacked the most in the organization.

2 Identify where attackers were hiding their activities in encrypted web-traffic.

Identifying Attacks Using Encrypted Communication

The IT Security Manager's first step was to look beyond what the network could currently see. He knew historical attack data unique to their environment was available in their security products, like email security and endpoint, and could be used to inform their adoption of decryption. However, his team did not have the time or resources to pull forensics and analyze attack types from disparate sources. Threat modeling using this data would allow him to effectively quantify and communicate which users needed decryption the most.

> “I could write scripts to parse email forensics related to URLs used in attacks, or iterate through alerts tied to our workforce's endpoints - but that is a manual, lengthy, and a resource-intensive process.”

Within minutes, Reach connected to their security stack and:

1

Analyzed email forensics to quantify the number of threats and threat types utilizing encryption in their delivery.

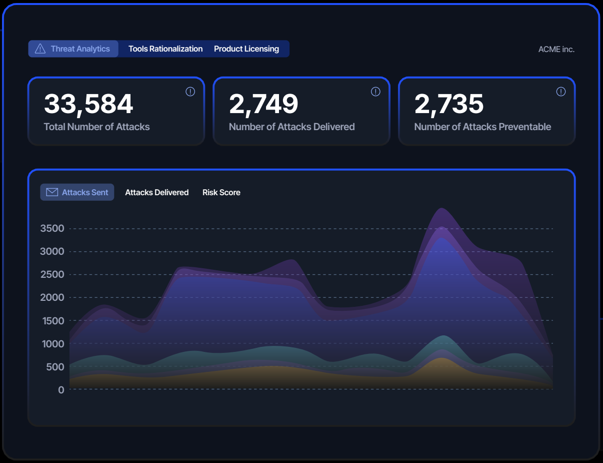
2

Correlated these threats with workforce data to determine which users received these attacks, which were riskier than average, and which had a higher risk contribution relative to the rest of the workforce.

Identifying Attacks Using Encrypted Communication

The result? A prioritized list of risky users derived from threat data and a realization that 4% of the population accounted for 70% of the company's overall risk.

Leadership now had data to understand that a majority of risk lived with a minority of users and gave the green light to start SSL decryption on a test group of those that were most attacked.



33,584 Total Number of Attacks

2,749 Number of Attacks Delivered

2,735 Number of Attacks Preventable

> With Reach, I'm using terms like 'these users provide more risk to the company overall', and I'm actually able to give concrete numbers and something valuable to leadership.

Having found the 4% of users posing the highest risk to the business, the next hurdle was identifying the URL categories that would extend visibility into the highest concentration of threats. Decrypting all SSL traffic out of the gate was not an option as doing so would:

1

Significantly impact the firewall's throughput and memory consumption.

2

Require expensive hardware upgrades across the network outside of their refresh lifecycle.

3

Require for a large amount of the employee time to monitor and manage.

> The security professional in me wants to do it all, but it's not reasonable for me to go from no SSL decryption to full SSL decryption on all traffic.

sales@reach.security | reach.security

A Threat-Informed Approach to Adopt SSL Decryption on Palo Alto Networks Firewalls

The IT Security Manager knew he could follow a similar threat modeling approach in analyzing logs and forensics from their endpoint and email security products to figure out which URL categories were tied to the highest concentration of threats targeting their users. He could then utilize this data to justify decrypting traffic on the same categories on his firewalls. But once again, manually conducting this exercise across the entire company would tap into resources that he didn't have.

With Reach connected to their products, the IT Security Leader was able to get immediate visibility into:

1

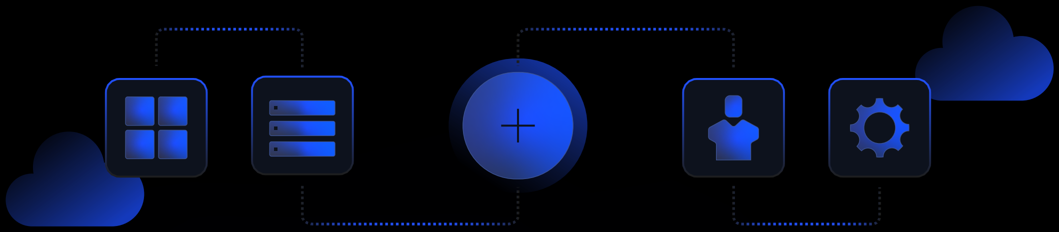
The 85% of attacks that leveraged encrypted traffic as part of their attack life cycle.

2

Network activity from attacks translated into content filtering categories.

3

Granular risk eduction metrics as a result of enabling decryption and extending visibility into traffic stemming from these categories.



> With Reach, I'm now able to say 'I'm not decrypting all URL traffic, I'm decrypting these categories based on attacks that we've seen and reviewed. I'm decrypting these categories for our highest risk users. It's much more manageable.

Realized Benefits

With a phased plan to roll out SSL decryption already in motion, the IT Security Leader has his eyes set on how he'll use the data to enhance protections across the board. What started as a staged approach to SSL decryption is now enabling the business to maximize the return on their firewall investment while simultaneously enabling the security teams to provide the best security possible for the organization.

> Once SSL decryption is in place for the entire company, I'll move on to deploying Reach's file blocking profile recommendations given that files were previously masked in our traffic. It's difficult to do this effectively when a majority of your network traffic is encrypted.

sales@reach.security | reach.security

On top of maximizing firewall capabilities, he has also seen a huge impact on the data quality in their SIEM as a result of having richer data sets of network traffic.

> Our SIEM has also become better with decryption. We have better logs to review and our incident data for analysts to take action on has improved significantly.

What's Next?

At the end of the day, data wins. Aggregating and normalizing data from disparate security tools, vendor agnostic, gave the manufacturing company a clear path to a decision to extend visibility across their network. The feedback from across the board from both end users and leadership has been overwhelmingly positive, and the IT Security Manager is looking forward to amplifying the roll out throughout the rest of the year. He expects to have SSL decryption enabled for the rest of the company's workforce within the year given the early success across the board.

> With the way things are going right now, the next year is 100% in scope for us to roll out decryption further across the rest of the company.

Get Started with Reach

To join the community of customers enjoying the benefits of Reach and learn more about how it can transform your security posture, visit:

reach.security/try-reach

Reach was founded to help organizations proactively find and fix hidden security blind spots. Traditional approaches surface issues, but stop short of fixing them. This leaves teams exposed, overwhelmed, and under-resourced. We built Reach to close that gap, delivering a platform powered by cybersecurity domain-specific AI models that reveal misconfigurations and underutilized capabilities across your existing security toolset; proactively remediate them; continuously validate that security controls are working as intended; and ensure your defenses stay aligned with your evolving environment and threat landscape.