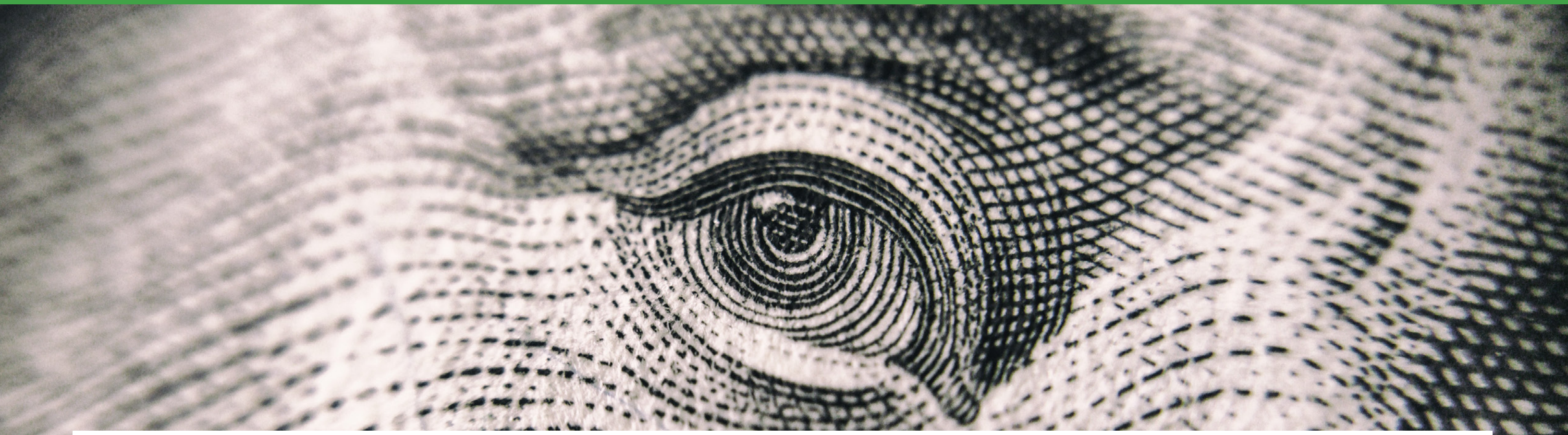
CASE STUDY

GARLAND TECHNOLOGY
See every bit, byte, and packet.



Security: Financial Services

Simplify security stack, while providing threat prevention optimization and analysis

The financial services industry experiences 35% of all data breaches,[1] and are 300 times as likely as other companies to be targeted by a cyberattack.[2] With the average cost of cybercrime per company in financial services around $18.5 million,[3] financial institutions spend an average of .3% of revenue and 10% of their IT budget on cybersecurity.[4]

Financial services IT SecOps teams are battling this high breach volume trying to protect not only financial loss but sensitive consumer data and the company reputation. And in this battle, the SecOps teams are better at detection than prevention, as the financial services industry is more "effective in detecting (56%) and containing (53%) cyberattacks than in preventing attacks (31%)."[5]

Challenge: So this is why, one of the world's largest investment companies, who specialize in mutual funds, exchange-traded funds (ETFs), financial planning and asset management came to Garland Technology looking to optimize their threat prevention strategy.

With the proper security tools in place, this company wanted added assurance that the inline web application firewall (WAF) tools they had in place were properly preventing possible threats.

This solution focused on their WAF, which filters, monitors, and blocks HTTP traffic. WAFs are considered different from a traditional firewall, in that a WAF is focused on filtering specific web application content, while regular firewalls serve as a safety gate between servers. WAFs inspect HTTP traffic to prevent attacks stemming from web application security flaws, such as SQL injection, cross-site scripting (XSS), file inclusion, and security misconfigurations.

Goal: Gain visibility into their security deployment, including the performance of the tool, ensuring all inline tools are optimized properly, and having the capability to trouble-shoot each device, while addressing if the tools are missing packets and threats or are straining network performance creating unneeded latency. Ultimately to ensure the WAFs are properly filtering specific web applications, anomalies, and threats.

Solution: Garland's engineering team worked with the IT team to design a connectivity architecture that solved all of their challenges and provided value they weren't expecting, leading them to expand this use case throughout their enterprise.

The EdgeLens® Inline Security Packet Broker transformed their network security capabilities with the "Historical Look Back" solution, which captures traffic before it goes into the web application firewall and after, sending both copies of data to performance monitoring tools, providing ultimate visibility coverage. This solution also simplified their security stack by providing the added capability to manage multiple inline and out-of-band tools from one device, while ensuring bypass resilience.

Historical Look Back

Before and After Optimization & Validation - Allowed them to analyze the WAF performance to see if it is configured properly or if it may be missing the threat, by analyzing packet data before and after the inline device to ensure optimal tool performance to validate any updates or troubleshoot why threats weren't blocked.

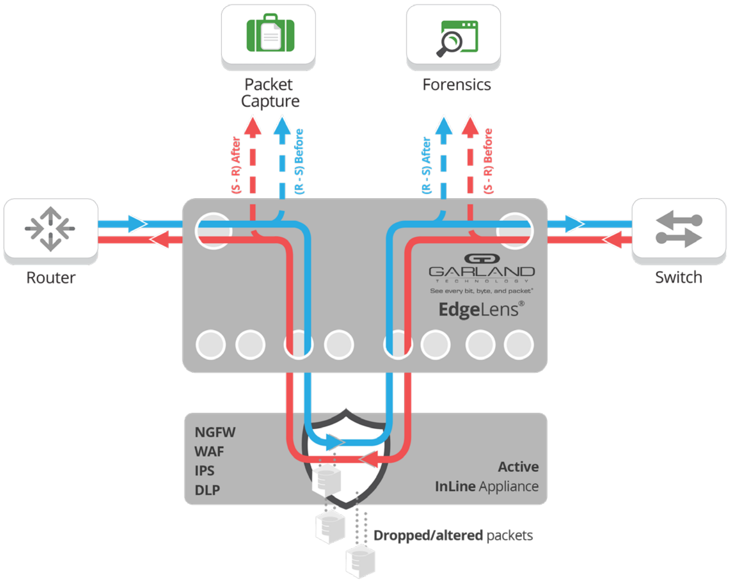


Diagram 1: Sends copies of traffic taken before and after the inline appliance to packet capture, forensics or network analyzers

This solution captures traffic before it goes into the inline tool and after -- sending both copies of data to out-of-band packet capture, storage and analysis tools. This allows teams to look deeper into traffic anomalies, as well as tool and network performance to properly validate updated or optimize configurations to ensure the device is properly blocking and filtering.

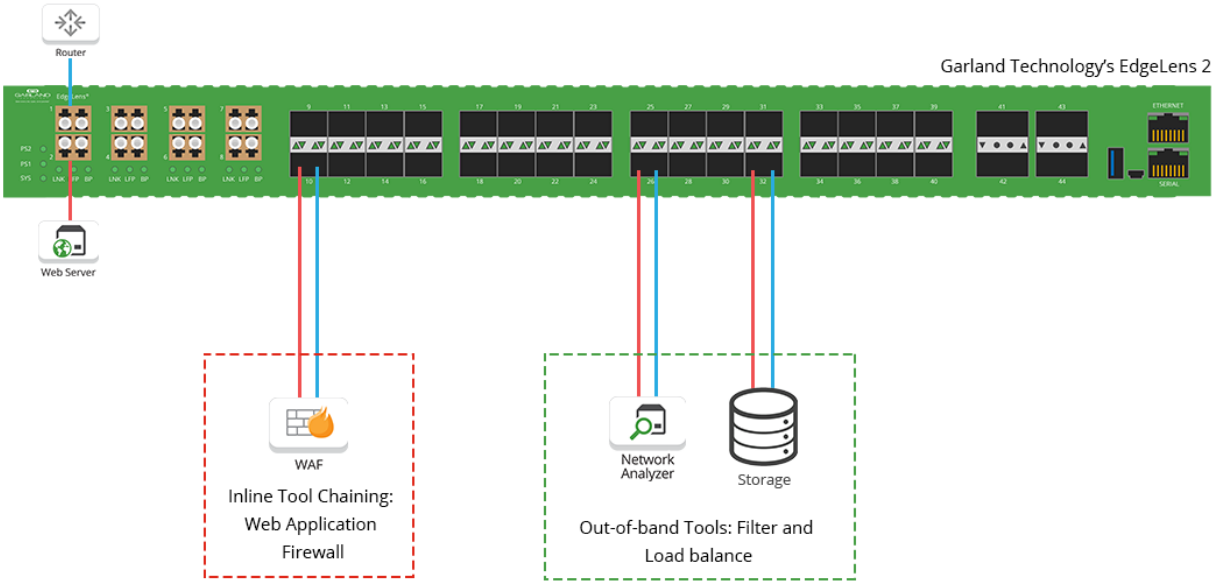

Router
Garland Technology's EdgeLens 2
Web Server
WAF
Inline Tool Chaining: Web Application Firewall
Network Analyzer
Storage
Out-of-band Tools: Filter and Load balance

Diagram 2: EdgeLens easily configures the historical look back solution

Look Back Forensics - If active blocking failed to stop a threat, they now have the ability to analyze breach forensics from the collected traffic. By sending traffic to out-of-band packet capture, storage and analysis tools the traffic from your inline IPS, Firewalls and WAFs tools, you are able to look back for post breach analysis.

Historical Look Back allows you to:

- Capture network traffic, without loss, at full line rate
- Easily correlate events generated by PCAP data
- Validate changes or updates that your tool is configured properly
- Increase efficiency of inline and out-of-band tools
- Facilitate the time-critical workflow for security incident response
- Enables forensic timelines of days/weeks/months
- Enable root cause analysis
- Extracted PCAP data may be presented as evidence in court as “chain of custody”
- Enable real-time security proof-of-concept evaluations without impacting the network

Simplified Security Stack

This solution provided an easy, hardware base chaining solution, that allows you to manage multiple inline and out-of-band tools individually, between multiple network segments from the same device, while also providing bypass resilience. If one of the tools in the chain can’t keep up, load balance to the other tools 1:1 or 1:N (one to many) tools.

The inline bypass function checked the health of their WAF devices, providing “inline lifecycle management” which allows you to easily take tools out-of-band for updates, installing patches, aintenance or troubleshooting to optimize and validate before pushing back inline. If the device is not active, they have the options to either implement a high availability (HA) solution, switch over to the secondary WAF, or skip over it and just allow the network to continue to run, without having to bring down the link.

Benefits:

- Distribute traffic before and after an inline tool (WAF, NGFW, or IPS) to out-of-band tools
- Simplify security stack and reduced network complexity by managing multiple inline tools
- Provide filtering, aggregation, and load balancing to inline links
- Reduced risk of unplanned downtime
- Network resilience - flexibility to bypass the tool and keep the network up, or to failover to a High Availability [HA] solution

Looking to add visibility and reduce network complexity, but not sure where to start? Join us for a brief network Design-IT consultation or demo. No obligation - it's what we love to do.

1-2016 Data Breach Investigations Report by Verizon Enterprise

2-https://www.bcg.com/d/press/20june2019-global-wealth-report-222692

3-Cost of Cybercrime Study in Financial Services: 2019 Report by Accenture

4-https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html

5-https://www.prnewswire.com/news-releases/synopsys-and-ponemon-release-new-study-highlighting-software-security-practices-and-challenges-in-the-financial-services-industry-300894781.html