cyglass

LEGAL INDUSTRY
CASE STUDY

CYGLASS HELPS A TOP 100 LAW FIRM UNCOVER AND STOP AN ONGOING BREACH

THE CYGLASS IMPACT

There were no indicators. Everything appeared normal to the network security team. However, behind the scenes and undetected to the existing security tooling, critical data was being exfiltrated.

Enter CyGlass. Within days, CyGlass began to pick up a sequence of emerging behaviors uncovering a major breach. The first sign was the detection of a vulnerability being exploited in the firewall, which permitted a privileged user to unblock a port without being detected. Second, short-lived SSL connections in tandem with unsigned and self-signed certificates began communicating with the Microsoft Exchange server.

Through the combination of these two indicators, large packets of data exiting the network through the firewall vulnerability were detected. Unauthorized lateral movements were uncovered in combination with repeated anonymous login attempts outside the normal user profile, all suggesting either an insider threat or that administrator credentials were compromised. In this case it was the latter.

Within hours of uncovering these corresponding anomalous behaviors illustrating the breach, the customer was able to take corrective action to take control of their network once again.

BACKGROUND

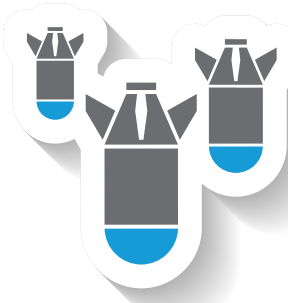
Law firms are increasingly being seen as a lucrative and soft target for cyber threat actors. Since 2011, 80% of the top 100 law firms have experienced a breach.

Law firms work with the widest spectrum of clientele's sensitive and critical data. It can range anywhere from tax returns, to merger and acquisition contracts, all the way through and beyond legislative data, privacy and health care information.

At the same time, most law firms do not have resources for extensive tooling and security operations. Finally, lawyers in general want to practice law and not be distracted by technology issues.

THREATS DETECTED

- Firewall vulnerability
- Masquerader
- Credential Compromise
- Rogue behaviors
- Insider Threats
- Lateral Movement
- Data exfiltration



THE CUSTOMER REQUIREMENTS

CyGlass was put in place, after the customer determined that the´current security controls at the law firm could be enhanced with a tool that provided visibility and detection of unknown dark threats. The customer had 3 primary requirements:

1. The solution must be capable of uncovering anomalous behaviors in network traffic and overlay that information with authentication data.
2. Previously unknown vulneratbilities to critical assets should be uncovered during the process.
3. The solution must be easy to deploy, use and maintain with minimal upfront investment.

THE SOLUTION

The CyGlass SaaS offering was an immediate win for the customer. Two lightweight collectors were deployed on premise at the customer and connected to the AWS CyGlass Analytics with minimal effort. Within hours, the customer was collecting valuable insight into the network behaviors and organization's critical assets.

CyGlass began its learning process by ingesting the historical log data the customer provided as well as capturing the ongoing network traffic (pcap, http, netflows). In addition to this, CyGlass overlaid the authentication logs to gain understanding of the normal behaviors of users in the environment. Critical assets were then classfied to provide deeper context into the overall network behavior and assist in prioritizing threats as they began to emerge.

As the initial firewall vulnerabiliites were detected, the customer could easily follow the correlation of anomalous behaviors which were pinpointed and prioritized for them. From there, the visual mapping connected these behaviors and uncovered the associated credenital compromises, lateral movements in the network and data being exfiltrated.

THE OUTCOME

Upon detecting the interconnected behaviors in the network, which clearly outlined the ongoing breach, the customer was able to immediately begin taking remediative action.

Once the firewall vulnerabilities were rectified, and other configurations within the environment were checked for weaknesses, the customer was able to eliminate accounts and credentials that had been compromised as well as determine whether additonal credentials had been taken.

With a breach, one can never be sure if all backdoors have been eliminated. CyGlass not only uncovered the ongoing breach, however also continues to provide an ongoing monitoring effect for the environment, continuing to look for those anomalous behaviors that would suggest a malicious actor may still have access.

Although CyGlass was deployed as a breach was already underway, the customer was able to limit the damage done and quickly mitigate the risks. What would have otherwise took months of investigative work, was now resolved within days.

For more information, please contact sales@cyglass.com