Case Study

BINARY DEFENSE™

Binary Defense Helps Law Firm Improve Cybersecurity by Installing and Tuning SIEM

Business

Large provider of legal voluntary benefits to numerous Fortune 500 companies

Challenges

Minimal security staff to manage a vast amount of security data

No around-the-clock monitoring to ensure continuous security coverage

No communication process to escalate alarms to internal stakeholders

Results

Binary Defense implemented AT&T Cybersecurity USM for the law firm

The experts at Binary Defense are an extension of the law firm's security team, providing around-the-clock protection

Through monitoring, Binary Defense detected an employee had fallen victim to phishing scam and was able to remediate the issue

The legal industry faces complicated cybersecurity challenges
The legal industry continues to be a target for cyber security criminals looking to gain access to business capital, trade secrets and intellectual capital.

The four biggest cybersecurity risks law firms currently face are:
- Phishing
- Ransomware
- Leaks of sensitive data
- The risk of malpractice allegations due to poor cybersecurity

Cybercrime continues to evolve at an alarming pace. If these threats are not contained and stopped, firms can lose assets, highly-sensitive, confidential information, and incur millions of dollars in damages. Add to that the public relations nightmare of the backlash from clients whose information was compromised. After a breach, customer trust is eroded, leading them to seek legal counsel elsewhere. The entire business suffers.

The American Bar Association has issued a formal opinion on attorneys' ethical obligations to avoid cybersecurity breaches. Lawyers are expected to make reasonable efforts when communicating confidential information using the Internet. In addition, depending on the industry of law firms' clients, they may be subject to comply with regulations such as HIPAA (healthcare). However, some firms might not have a security staff that can tackle security issues around the clock.

A Security Information & Event Monitoring System (SIEM) is a useful tool for monitoring data across a law firm's network
A SIEM helps keep an organization safe by centralizing data from various network devices, including servers, firewalls, etc., and correlating that data to provide a holistic overview of an organization's security environment. Alerts are generated if abnormal activity is detected. These alerts need to be reviewed by a person to determine if a threat is present, and then acted on if necessary. To fully respond to SIEM alarms, an organization needs to be staffed for 24-hour support or outsource this work to a Security Operations Center (SOC).

Staying on top of evolving threats required advanced cybersecurity solutions
A Binary Defense customer is a large provider of legal voluntary benefits for numerous Fortune 500 companies. Compliance regulations had driven the organization's security efforts through the years, but this strategy didn't take evolving cyber threats into account. This law firm has always embraced the importance of cybersecurity and knew they needed to increase their security to stay ahead of the threats.

Partner Spotlight: AT&T Cybersecurity United Security Management (USM)

AT&T Cybersecurity offers an all-in-one platform that responds, detects, assesses, responds to and reports necessary threats.

Key features include:

- Network asset discovery
- SIEM event correlation, auto-prioritized
- Dark web monitoring for stolen credentials
- 24/7 monitoring

Binary Defense SIEM

Binary Defense SIEM services protect your company's most valuable assets with network monitoring that is human-driven and technology-assisted. Our platform uses advanced detection technology and a team of dedicated security analysts that integrate seamlessly into your team to provide protection around the clock.

However, the firm had a small IT security staff who, despite their best efforts, could not keep up with the vast amounts of security data generated daily. The staff worked during regular business hours with no overnight shift to continue to monitor the data. This is an issue facing IT departments in all industries. Many organizations simply don't have the budget to hire for 24-hour coverage, and workers skilled in cybersecurity are in short supply. Many cybercriminals operate overseas, working in completely opposite time zones from the US, so the end of our work day has no bearing on their criminal activity.

And finally, the firm had no clear process for escalating security alarms to their internal stakeholders. They decided they needed help, and they turned to the experts at Binary Defense.

Firm sought a vendor partner to act as an extension of their team

The firm wanted to implement a new SIEM that could be managed by security experts acting as an extension of their team. In selecting a cybersecurity partner, they were looking for a vendor that could:

- Provide one-on-one security training to members of the entire information technology staff
- Protect data by leveraging top notch technologies and cybersecurity risk solutions
- Identify and manage vulnerabilities proactively to detect and alert the highest risk areas for rapid remediation

The firm selected AT&T Cybersecurity Unified Security Management (USM) as their SIEM. As an AT&T Cybersecurity Global Partner of the Year in 2019, 2018 and 2016, Binary Defense is known for their expertise in installation and management of USM, and the firm knew they were the right team to partner with. The Binary Defense team provided a thorough onboarding plan, which included staff training, a process for escalations, and a deep understanding of the law firm's unique challenges. With this information, Binary Defense is able to act as an extension of the law firm's team.

Once Binary Defense installed and tuned the new SIEM, their SOC team began monitoring 24/7/365. The Binary Defense analysts, in one case, found evidence of suspicious activity on the firm's network after an employee had clicked on a phishing email and entered personal and business credentials on a malicious site. The activity triggered alarms through the AT&T SIEM and Binary Defense immediately notified the firm. Because of this quick action, the firm was able to investigate and remediate the threat within days. It's been reported that it usually takes about 197 days for an organization to detect a breach, on average. By then, it's a foregone conclusion that hackers have stolen files, financial information, confidential client data, and more. Being notified of the threat saved the company potentially millions of dollars. (The global average cost of a data breach is $3.2 million.)

For more information, visit BinaryDefense.com/SIEM.