Case Study

BINARY DEFENSE

Private equity firms rely upon Managed Detection & Response to keep financial data secure

Industry

Financial/Private Equity

Challenges

Inability to filter the "noise" from regular alerting systems

Need for timely, comprehensive, actionable threat identification

How to make sense of a quickly-changing industry

Results

Visibility and insight through advanced cybersecurity

A security partner acting as an extension of internal team

Measured, quantifiable results

Industry thought leadership helps firm be more proactive

"Binary Defense provided greater visibility, a depth of information, timeliness of calls—even in the middle of the night, if needed—and an additional set of technical eyes that enhance our capabilities."
– IT/Cybersecurity Manager at Private Equity Firm

Private equity firms process tremendous amounts of sensitive data
In the fast-paced private equity (PE) market, data changes hands at a breakneck speed every day. Consider the types of data that could be passing through a PE firm: proprietary company information, financials, bank account numbers, the list goes on—exactly the type of information hackers want to obtain. Through phishing emails to employees, as well as other ever-evolving methods, hackers pose an unrelenting threat.

Statistics show that financial firms are attacked at an alarming rate of 30 times per second[1]. A breach can cost a company hundreds of millions of dollars. Just look to recent headlines about the Capital One breach, for example[2], with an estimated cost of $150 million to repair the damage done.

Trying to mitigate all of the threats, as well as staying on top of cybersecurity trends, can be too much for a small IT team to handle. Some PE firms may only have one person on staff dedicated to cybersecurity, or a resource that is also responsible for other areas within Information Technology.

Finding a vendor partner that can truly be an extension of a PE firm's internal IT team is paramount. A viable option is to outsource a Security Operations Center (SOC)—a service in which a team of dedicated security analysts can detect and analyze advanced attack patterns and alert clients of these malicious threats within minutes.

Visibility, priority and insight across endpoints
One Binary Defense customer is a PE firm that had invested in a Security Information & Event Management (SIEM) service from a different vendor to help distill the large volumes of data, but their IT Manager was doing manual work to analyze and respond to alerts generated by the SIEM. The firm needed additional help to secure the individual endpoints (laptops, desktops, servers) within the organization. "In PE, my users are constantly receiving tons of files—gigs upon gigs. I need to ensure our end users don't download malicious files and that nothing is buried to leave our system vulnerable. It's a balance between enabling employees to do business and providing safeguards," the IT Manager said.

Binary Defense MDR and SOC elevate protection
This customer selected the Binary Defense Managed Detection & Response solution, which is a cloud-based solution with a nano agent that installs on every endpoint at the PE firm without adding costly hardware, resource-

[1] https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/#3a127a766e90
[2] https://www.cnbc.com/video/2019/07/30/capital-one-believes-breach-will-cost-up-to-150-million.html

Binary Defense MDR, SOC

Advanced endpoint detection

24/7 around-the-clock event monitoring

Real-time analysis of threat behavior

Lightweight and easy deployment

Expert and trusted extension of your team

"I feel protected, 24/7."
-IT/Cybersecurity Manager at Private Equity Firm

intensive software, or external personnel. MDR adds another layer of protection to the safeguards already in place with the SIEM. The Binary Defense SOC team actively monitors the entire network, including the SIEM and all of the endpoints, to detect threats and respond as needed, effectively eliminating the manual work that the PE firm's IT team was doing to stay on top of alerts.

The software and service combination expand the company's protection to a level impossible without the dedicated team of SOC analysts who investigate suspicious activity and security incidents. "At first I was skeptical it would be just another SOC," said the IT manager. "But it provided greater visibility, a depth of information, timeliness of calls—even in the middle of the night, if needed—and an additional set of technical eyes that enhance our capabilities. I feel protected, 24/7."

Insights enable actionable intelligence
Binary Defense's expert analysts act as an extension of the PE firm's team by providing value-added insights and communications. Each Binary Defense SOC analyst emails the PE firm IT manager at the beginning of each shift with their contact information. "I don't have to pull up an 800 number and wait until the next business day to get a response," the IT Manager said.

Binary Defense sends its subscribers a daily e-newsletter to outline current priority threats and recommended actions. The newsletter is written by the counterintelligence team, comprised of experienced professionals from the military, government and private sector. These daily messages are much more digestible for busy IT professionals who don't have time to seek out this information themselves.

Quarterly reviews between Binary Defense and the PE firm help to ensure transparency and provide a deep dive on performance.

Partnership, innovation and alignment
Industry leadership is important to this PE firm's cybersecurity program, especially as the financial services industry is at a greater risk to cyberattacks than any other. Not only is there a significant impact to the organization's bottom line if a company is breached, but a longer-term impact on a company's reputation as customer trust is eroded. It's estimated that one in three customers will choose to no longer do business with a company that has been the victim of a security breach. Binary Defense seeks to partner with its financial industry customers to provide updates about the latest threats facing the industry, give access to the most innovative technologies, and share a forward-looking product roadmap.

600 Alpha Parkway, Stow, OH 44224
+1 800-246-2792
info@BinaryDefense.com

BINARY DEFENSE™

Copyright © 2019 Binary Defense

Learn more about us
www.BinaryDefense.com