

Cyber Defense for Financial Services

Cyber security is recognised as the biggest risk facing the financial system. Banks around the world have been victims to major breaches, and all were shaken by the \$81 million cyber theft from the Bangladesh central bank in 2016, via SWIFT.

While the financial services industry is highly aware of the risks, their policies and defenses are not always up to the task of defending against cyber-threats. These risks are multiplying as the threat landscape gets more sophisticated.

Most attackers are motivated by monetary rewards, either holding companies to ransom or stealing personally identifiable information (PII) of customers that can be sold and then used for identity fraud and related crimes.

But there is also a trend towards long-term attacks against the integrity of data and financial systems. An attacker that succeeds in causing doubts about the reliability of information and affecting investor confidence has the potential to make more money, and do serious, long-term damage.

Globally operating financial services firms must now comply with new regulations to avoid large fines, including the EU's General Data Protection Regulation (GDPR) and the New York Department of Financial Services' (DFS) 23 NYCRR 500. Singapore's Cyber Security Agency (CSA) has also proposed regulations that would require financial services organizations to report cyber incidents to the Commissioner for Cybersecurity, and notably the CSA would have the right to overturn privacy laws to access any computer system relevant to an investigation.

To comply with new rules and, critically, to win and maintain the trust of customers, financial institutions must be dedicated to enhancing customers' privacy and protecting against a range of potential attacks, including latent threats that come from within.


“ Investors are increasingly demanding best-of class technology to defend their managed assets, Darktrace gives us that. ”

Conor Claxton, Chief Operating Officer, MacroSynergy

Threats By Numbers

 Financial service firms targeted in **27%** of all recorded attacks.

In 2017 the financial industry was, for the second year in a row, targeted with the highest volume of security incidents and the third highest volume of cyber-attacks.

 European banks take an average of **59 days** to detect a security breach.

The amount of data being stolen from businesses is increasing, with European banks facing an average of 85 serious attempts to breach their cyber-security systems over 12 months. According to the Ponemon Institute, 36% of these attacks resulted in successfully stealing data.



AEA Investors



Background

Founded in 1968, AEA Investors is a leading private equity firm with over \$10 billion assets under management. The firm has roughly 110 employees and operates across five offices in the United States, Europe, and Asia.

Challenge

AEA Investors has been a pioneer in the industry for over 50 years, trusted for its global network, financial success, and proactive approach to cyber security. As a leading private equity firm, AEA is not only responsible for securing its own private data, but also the sensitive non-public information of its portfolio companies. While the firm has always prioritized its cyber defense strategy, AEA's security team was fully aware of the unpredictable and fast-evolving nature of today's threat landscape, and the challenge this posed to securing its critical data against advanced attacks.

“

Darktrace detects threats that other tools miss. With Darktrace, we know that our firm's financial data is secure.

**Ngoc Lu, Chief Technology Officer,
AEA Investors**

”

Solution

After a successful trial period that lasted four weeks, AEA Investors deployed Darktrace's Enterprise Immune System in its internal network. Darktrace managed the deployment as a dedicated service, installing sensors in the firm's environment to feed data back to a Darktrace cloud instance for analysis. By learning the organization's normal 'pattern of life', Darktrace's self-learning technology can detect subtle deviations indicative of a threat.

Through Darktrace's Threat Visualizer, AEA's security team has complete visibility of activity in its internal network, and can investigate prioritized alerts by analyzing the rich context around each event. On one occasion, Darktrace detected a malware event that evaded the firm's other tools, enabling the security team to remediate the threat before it had time to cause damage.

“Darktrace detects threats that other tools miss,” commented Ngoc Lu, Chief Technology Officer at AEA Investors. “With Darktrace, we know that our firm's financial data is secure.”