

2021 Industry Spotlight: Financial Services

Cyber-attacks are growing in speed, sophistication, and scale. With offensive AI on the horizon, the financial services sector will continue to be challenged to protect sensitive data and systems. Signature-based tools have proven insufficient at catching the latest attacker innovations, and as increasingly targeted and tailored threats emerge, it is clear that a new approach to cyber security is needed.

At a Glance

- ✓ Protects over 700 financial services organizations globally
- ✓ Detects and responds to the full range of cyber-threats
- ✓ Neutralizes threats as they occur with no business disruption
- ✓ Autonomously investigates, triages, and reports on threats
- ✓ Provides complete visibility across the entire dynamic workforce

Balancing Digitalization with Cyber Security

Financial services organizations face unprecedented cyber challenges. As one of the most targeted sectors by cyber-criminals, the threats they are facing are sophisticated and happening at machine speed. Instances of ransomware, phishing, and man-in-the-middle attacks have all risen substantially over the past few months, and the reality is that these threats have the potential to jeopardize national economic security.

In May 2020, the scale and severity of ransomware on the financial services sector became evident. One of Costa Rica's most prominent banks was hit with Maze. The attackers first exfiltrated sensitive information - including 11 million credit card credentials - before encrypting the data and demanding payment. In a two-pronged approach, the cyber-criminal gang then leaked some of the data. The extent of this breach can be attributed to the fact that the group had infiltrated the bank's systems three months prior to their discovery.

Personal and financial data such as that affected in this Maze attack is the lifeblood of cyber-crime – making organizations operating within the financial services sector a key target for threat actors. Balancing the protection of sensitive data and systems with the transformation projects brought about by remote working remains a difficult challenge, with greater digitalization offering both increased personalization for customers and new points of entry for cyber-criminals.

Over the past year, the financial services sector has seen:

- A surge in mobile and online banking which has drastically widened the attack surface. Cyber-criminals have capitalized on this through banking trojans and supply chain attacks.
- Customers readily trusting a wide range of online sites with their banking details, increasing the risk of credential theft and fraud.
- State-sponsored cyber-attacks continuing to rise in the face of growing geopolitical tensions, with the financial services sector being disproportionately affected.
- Security teams struggling to monitor remote workers, increasing the risk of malicious insiders or employees inadvertently exposing data.
- Pressure to upgrade digital banking infrastructure and comply with the ever-changing influx of regulations, such as the NYDFS 500, APRA CPS 234, GDPR, and the CCPA.

With these risks and regulations, the need for a comprehensive cyber security technology covering the entire digital business is critical.



How Self-Learning AI Protects Financial Services Organizations

Relied on by some of the world's largest financial services organizations, Darktrace is uniquely positioned to defend against the full range of cyber-threats. The Self-Learning AI technology detects and responds to all emerging malicious activity, reacting in seconds to protect organizations from zero-day exploits, insider threats, and machine-speed ransomware.

Rather than relying on historical attack data, Darktrace learns 'on the job'. By understanding what 'normal' looks like for each unique organization, the AI is able to spot the subtlest signals indicative of malicious activity. The AI then autonomously responds in real time, taking targeted and proportionate action to neutralize the threat. This capability is crucial in fighting off sophisticated strains of ransomware, which can encrypt an entire database in under 30 seconds.

With an intuitive user interface, Darktrace provides organizations with complete visibility of their dynamic workforce, as well as the unparalleled ability to detect and contain fast-acting threats. Operative across the cloud, SaaS, IoT, endpoint devices, email, and the traditional network, Darktrace protects organizations' data and digital systems wherever they are located.

Darktrace also supports financial services organizations' compliance with regulations such as the CPPA, GDPR, NYDFS 500, and more.

Autonomously Neutralizing Ransomware

At a leading investment company in Asia, Darktrace autonomously detected and responded to a ransomware attack – preventing a crisis.

The attack began when an associate inadvertently downloaded a malicious file designed to look like an authentic email, infecting their computer. This infected device then connected to the GandCrab ransomware infrastructure and started to encrypt almost 5,000 internal documents, adding a file extension containing a ransom note demanding payment in order to unlock them.

At the same time as the device downloaded this executable, Darktrace identified the ongoing threat as a widespread and sophisticated ransomware attack. The AI stopped all outgoing communications from the infected device, neutralizing the infection, and preventing subsequent data loss.

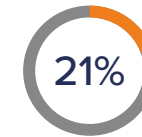
“Whatever the issue, wherever it is on our infrastructure, Darktrace will stop it spreading, buying back precious time for us to mitigate the threat entirely.”

Derik Scheepers, Head of IT Operations,
PPS Insurance

Threats by Numbers



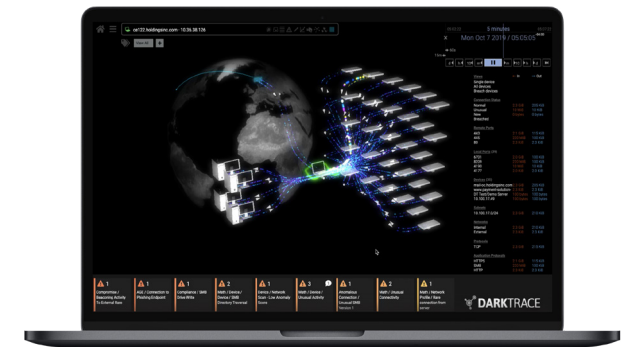
\$5.9 million is the average cost of a data breach in the financial services sector.



21% of sensitive files have been left exposed in the financial services sector.

“Darktrace gives us an edge against fast-moving attackers and malicious or accidental insider threat.”

Adnan Uz-Zaman, Network and Infrastructure Lead, Waverton



Self-Learning AI identifies a ransomware attack