Industry Spotlight: Financial Services

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
- Autonomous investigates, triages, and reports on threats
- Provides complete visibility across the entire dynamic workforce

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 fundamentally different approach to cyber security is needed.

Industry Challenges
Financial services regularly tops lists of sectors most targeted by cyber-criminals, with this industry subject to attacks from a broad range of actors, from organized and well-funded cyber-criminal groups with financial goals, to hacktivist groups seeking to cause disruption and wreak havoc in the markets.

Security professionals in this industry are tasked with fending off a number of threat vectors, including targeted and convincing phishing emails, cloud-based attacks, and ransomware, which has rebounded with new severity in recent years. Sophisticated strains such as Maze and Ryuk are constantly being tweaked, and attackers are increasingly adopting ‘double extortion’ tactics to gain maximum leverage. The devastating repercussions of these attacks have been felt by some of the largest financial organizations around the globe, with threat actors exfiltrating and releasing millions of customers’ data in a single attack.

Rapid digital transformation and supply chains present additional risks. 2020 marked a watershed moment for many as threat actors used a vulnerability in SolarWinds’ software to compromise thousands of organizations, including banks and other financial institutions. The attack had gone unnoticed for several months, and to many this served as a wake up call that an approach based on manual rules and lists of signatures is no longer enough to combat the modern threat landscape.

Most financial services organizations now rely on cloud services to carry out daily operations, but the security implications of this transformation are significant, expanding the attack surface for threat actors, who can pivot through different areas of the digital estate to evade detection.

Customers readily trust financial services with highly sensitive information. As threat actors continue to innovate, organizations must seek to protect data with technology that can keep up with constant attacker innovation, and cover all corners of digital infrastructure – from email and cloud to the corporate network and remote endpoints. Taking the right approach to cyber security is crucial not only in preventing data loss and steep ransom demands, but in avoiding broader cyber disruption that can grind operations to a halt.

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

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

Adnan Uz-Zaman, Network and Infrastructure Lead, Waverton