2021 Industry Spotlight: Technology

The technology sector fundamentally unpins and intersects with every aspect of life today, driving innovation in the worlds of work and leisure. But while users enjoy the flexibility, efficiency, and personalized experience technology engenders, cyber-criminals look to exploit sensitive IP, customer data, and zero-day vulnerabilities.

At a Glance

- ✔ Protects over 500 technology companies globally
- ✔ Detects the full range of cyber-threats, including ransomware and data exfiltration
- ✔ Autonomously stops attacks in seconds, before the damage is done
- ✔ Reduces time to triage by up to 92%

The Security Challenges of Driving Innovation

Pushing the boundaries of innovation and personalization, the technology sector is particularly susceptible to zero-day attacks. The industry leads the charge in utilizing the latest, cutting-edge software and devices. But, there is a continual trade-off between innovation and security – with the latter often an afterthought given the speed required to get products to market. The result is multiple, latent zero-day vulnerabilities and software weaknesses.

The SolarWinds hack was a watershed moment for cyber security in the technology sector, not only highlighting attacker ingenuity but organizational vulnerability. Despite its scale, this threat went undetected for over eight months – exposing the fundamental limitations of signature-based tools in the face of novel and unpredictable threats.

Cyber-criminals are increasingly targeting the very software and hardware that underpins thousands of organizations in order to carry out widescale campaigns. Furthermore, the ubiquitous nature of technology enables threat actors to hit otherwise difficult to access industries, including government and healthcare organizations.

Technology companies hold highly valuable IP alongside vast volumes of customer data. For cyber-criminals, this signals jackpot, with files exchanged on the Dark Web, leveraged for ransom payment, or sold to competitors. Sophisticated attacks are often the work of nation-state attackers, looking to steal sensitive information and cause chaos.

Remote Working Risks

Mass scale digital transformation projects as a result of remote working have dramatically reshaped the threat landscape and widened the attack surface, making technology companies more vulnerable at both an organizational and customer level. Compounding the challenge is the growing trend towards integrations and interdependence between technology offerings.

To fight back, the technology industry must look towards Self-Learning AI technology, able to detect and autonomously respond to both known and unknown threats. Darktrace protects sensitive data, critical systems, and dynamic employees from cyber-threats, whether they emerge in cloud applications, endpoint devices, email environments, or the network.

A Self-Learning Approach

Trusted by over 5,000 organizations globally, Darktrace is the only technology able to autonomously detect, investigate, and respond to the full range of threats – no matter how novel or sophisticated. Defending the likes of Vodafone and Hedgeserv, Darktrace's Self-Learning AI protects against attacks across the entire digital ecosystem – from cloud and collaboration tools, to email and workers off the VPN, to IoT, OT, and the traditional network.

Darktrace works by learning what 'normal' looks like for every user and device in an organization, and all the connections between them. This contextual understanding enables the AI to identify the subtlest signals of attack in real time, no matter where they arise. Darktrace Antigena then surgically neutralizes the threat, autonomously stopping malicious activity at machine speed while allowing normal business operations to continue unimpeded.

Proven to stop zero-day exploits, ransomware, spear phishing, and nation-state attacks, among others, Darktrace defends organizations' workforces, data, and infrastructure. Darktrace Cyber AI Analyst automatically triages, interprets, and reports on the full scope of every incident, mimicking human analyst intuition to produce a natural language summary that highlights the activity seen, its attack phases, and Self-Learning AI's actions. This dramatically reduces time to meaning and puts teams in a position to take action.

Attack Case Study: Data Exfiltration via RDP

At a technology company in the APAC region, Darktrace detected a server-side attack targeting a Remote Desktop Protocol (RDP) server hosting 500 devices. Due to Darktrace's early identification, this threat was stopped before it could escalate into a Denial-of-Service or ransomware attack.

The threat started when attackers brute-forced an internet-facing RDP server and gained remote access to the desktop. Darktrace's AI then detected unusual administrative RDP connections from rare external locations to this server.

The attacker proceeded to download multiple files from rare domains and made over 4.4 million internal and external connection attempts on port 445 using the vulnerable SMBv1 protocol, attempting to build a botnet army. The server engaged in successful SMB sessions with over 270 internal and external IP addresses.

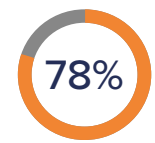
Darktrace's AI not only pinpointed the specific RDP server that the infection originated on but it also detected and investigated on every step of the attack in real time. Its granular insights into this threat enabled the security team to remediate the attack before it could cause a crisis.

> "The intelligence Darktrace gives us is clear and actionable - even my newest starters can use and learn from it on day one."
>
> CISO, Calligo

Threats by Numbers

of breaches involve intellectual property.

$5.04 million is the average cost of a data breach in the technology sector.



of organizations lack full visibility of remote workers when the VPN is disabled.

Darktrace autonomously protects users and data across the entire digital ecosystem - including remote employees off the VPN