DARKTRACE

INDUSTRY SPOTLIGHT

Cyber Defense for Technology

The modern technology sector is uniquely defined by transformative ideas. As a consequence, today's tech companies invest enormous resources in both material and human capital to foster such ideas, with the recognition that its success ultimately hinges on its intellectual property.

Yet such lucrative IP has attracted increasingly sophisticated online threat actors, from financially motivated cyber-criminals to geopolitically motivated governments. According to the Intellectual Property Commission, IP theft costs US companies $600 billion each year — a figure that will only climb as stealthy cyber-threats like personalized spear phishing emails and 'low and slow' attacks continue to proliferate. Subtler still are insider threats, executed by credentialed users who possess an intimate understanding of both the systems they manipulate and the IP they steal. These innovative and stealthy attacks easily bypass traditional security tools, which are programmed to insulate networks from known, external threats.

From social media websites to ride-sharing services, the big ideas at the heart of the modern tech industry also depend inextricably on sensitive personal data, whose exfiltration has proven to be as costly as IP theft and even more reputationally damaging. The high-profile series of personal data breaches suffered by major tech firms in recent years has demonstrated that no organization — no matter how technically advanced — is immune to these cyber security concerns, while the enactment of stringent online privacy legislation means that such incidents also entail hefty fines and legal fees. The EU's General Data Protection Regulation, for instance, imposes fines on breached organizations up to €20 million or 4% of their annual global turnover, whichever is higher. Similar laws are rapidly taking effect around the world.

To reap the benefits of their transformative ideas, tech companies must recognize that robust cyber defenses are as critical to their long-term prosperity as these ideas themselves. Both innovative cyber-criminals and malicious insiders are greatly incentivized to steal such intellectual property, and yet traditional security tools are blind to these critical threat actors. Indeed, the recent wave of data breaches affecting tech companies paints a clear picture of an industry in need of a fundamentally different approach to cyber security. Cyber AI-based defenses deliver that novel approach, continually learning on the job to keep pace with today's ever-evolving cyber-attacks — before they inevitably strike.

> Darktrace is unique in its ability to detect any emerging cyber-threats, including 'unknown unknowns' that routinely bypass legacy security tools.
>
> **Eben Upton, CEO, Raspberry Pi**

Threats By Numbers

Annual US data breaches have increased **tenfold** since 2005

According to Statistica, there were 157 US breaches in 2005 compared to 1,579 in 2017. This upward trend particularly affects tech companies, given that lucrative IP and sensitive customer data are the lifeblood of the industry.

Most users don't trust tech companies with data.

According to a 2018 Reuters survey, just 13% of users have "a lot" of trust that Facebook will obey laws that protect their personal information, while 15% trust Yahoo! to do the same. The survey also found that privacy concerns represented the second largest reason why users avoid a given technology, behind only finding that technology unhelpful or uninteresting.

DARKTRACE

CASE STUDY

Micron Technology

Background

Founded in 1978, Micron Technology is a global semiconductor company. With over 34,000 employees, Micron produces advanced memory and storage semiconductor technologies in factories and design centers around the world, including in the United States, Europe, and Asia. Micron's product innovations have made the company a leader in the industry with over $20 billion in annual revenue.

Challenge

Micron's security program is largely centered around the risk of data theft, whether from an advanced external actor or an insider with privileged access. Faced with a rapidly evolving threat landscape, Micron sought a technology that could autonomously spot and stop cyber-threats and provide real-time visibility across the company's global network.

> Darktrace's AI has been immensely valuable in defending our intellectual property against advanced attacks.
>
> **J.R. Tietsort, CISO,**
> **Micron Technology**

Solution

To meet these needs, Micron deployed Darktrace's Enterprise Immune System technology. After a seamless installation, Darktrace's AI immediately began learning the normal 'pattern of life' for Micron's organization. This evolving understanding of 'normal' allows the AI to autonomously detect and respond to emerging threats before they become a crisis.

"Darktrace's AI has been immensely valuable in defending our intellectual property against advanced attacks," commented J.R. Tietsort, CISO at Micron Technology. "In a vast and highly complex network like ours, Darktrace often finds threats that other tools don't."

Micron's security team also gained access to Darktrace's Threat Visualizer, which provides a graphical and interactive overview of the network and displays prioritized anomalies and threats for investigation. Soon after installation, Darktrace's AI discovered a number of anomalies on the network that helped to prioritize tasking for Micron's security team. Mr. Tietsort summarized with "Darktrace helps me confirm that my human staff is focused on the highest value work."