2021 Industry Spotlight: Education

Last year, the education sector underwent a seismic shift in working practices. With universities, schools, and colleges having to rapidly switch to online methods of learning, new vulnerabilities emerged – and attackers were quick to exploit them.

At a Glance

- ✔ Detects novel attacks and insider threats in their earliest stages
- ✔ Continuously updates and adapts to changing patterns to support remote and hybrid learning
- ✔ Responds autonomously to stop emerging threats at machine speed
- ✔ Protects cloud, SaaS, email, OT, endpoints, and the traditional network

Protecting Personal Data and IP Alongside Remote Learning

The education sector holds an enormous amount of personal data over vast open systems, as well as valuable research and intellectual property. Despite this, most schools, universities, and other educational institutions still rely on outdated legacy tools for cyber defense. Dependent on historical attack data and developed in siloes, they lack the visibility and context needed to determine malicious from benign. As a result, educational organizations often lack critical protection across their digital ecosystem, leaving them vulnerable to attacks of all kinds - from insider threats to infected USBs and phishing attacks.

National bodies such as the USA's FBI and the UK's National Cyber Security Centre (NCSC) have warned about the threat cyber-attacks pose to schools and colleges, able to seriously disrupt learning and even hold institutions to ransom. In March 2021, the NCSC updated their guidelines, urging educational establishments in the UK to mitigate cyber-risk in response to a new wave of targeted ransomware attacks.

Additionally, with many universities conducting crucial analysis into the COVID-19 pandemic, labs, research centers, and university databases have become particularly tempting targets for criminals. With learning and research increasingly becoming digital, and with the stakes higher than ever, the need for advanced cyber security in educational institutions is of critical importance.

> "No other security tool on the market comes close. The sheer volume of data that Darktrace actively defends would take a team of 50 to 60 security professionals to do."
>
> Richard Jenkins, Head of Information Risk Management, Cyber Security and Governance, International Baccalaureate (IB)

Autonomous Defense for the Education Sector

Today, Darktrace protects some of the world's leading universities, museums, and educational foundations, allowing them to stop zero-day attacks and ransomware in a matter of minutes.

Inspired by the principles of the human immune system, Darktrace's self-learning AI understands 'normal' for every user and device, and all the connections between them. This unique understanding of 'self' enables the AI to provide real-time threat detection, investigation, and Autonomous Response to spot and stop the full range of threats – including state-sponsored attacks, ransomware, and insiders.

Darktrace's AI-native technology identifies and autonomously disrupts threats wherever they occur in an organization, including SaaS applications, email, and endpoint devices, protecting students, staff, and data in real time. A fundamentally dynamic and self-learning technology, Darktrace continuously revises its understanding of 'normal' in order to evolve alongside organizations - even through times of unprecedented change - and accurately protect data and digital systems wherever they are located.

In today's threat landscape, AI technology is no longer a nice to have but a necessity in protecting against advanced attacks.

Detecting Compromised Remote Devices at Salve Regina University

In April 2020, as Salve Regina University was transitioning to online learning, Darktrace detected that some machines were compromised and were accessing the secure network through VPNs. Cyber AI was able to autonomously and quickly pinpoint this anomalous behavior, indicative of an emerging cyber-threat, and isolate the incident for closer inspection.

As the university continued to shift to the new mode of working, with people operating remotely, Darktrace adapted to this change in real time, very quickly giving Salve Regina's IT security team the ability to have the same functionality that they had had when working on campus. Self-learning AI that adapts alongside changing digital infrastructure enables students to continue learning – with as little disruption as possible.

"Darktrace proved to be valuable from the offset, finding several security breaches, which would have otherwise gone undetected."

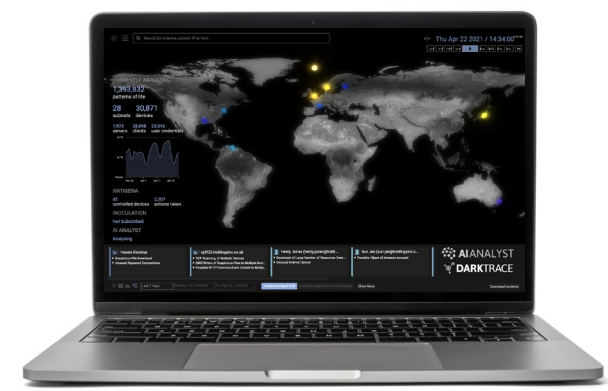
Chales Choy, IT Security Officer,
Hong Kong University of Science

Threats by Numbers

of malware incidents came from the education sector in June 2020, the most of any industry.

of secondary schools and higher education institutions have suffered from phishing and watering hole attacks.

Over half of further and higher education institutions are attacked or breached at least once a week.



Darktrace autonomously protects students and staff wherever they are