INDUSTRY SPOTLIGHT: LEGAL

DARKTRACE

AT A GLANCE:

- Self-Learning AI technology which understands 'normal' for each user and device
- Autonomously detects and responds to novel and sophisticated cyber-threats
- Identifies critical vulnerabilities and misconfigurations
- Defends against bespoke compliance breaches

The last few years have marked a paradigm shift in the cyber-threat landscape for the legal sector, with law firms around the world affected by Maze ransomware and nation-state attacks as threat actors increase their cyber operations. Organizations urgently need to rethink their cyber security strategies and deploy an adaptive, autonomous, defensive technology.

THOMMESSEN HOLMAN WEBB LAWYERS Bressler AMERY & ROSS

IceMiller LEGAL COUNSEL withersworldwide Gleiss Lutz

SLAUGHTER AND MAY IBB Law Jackson McDonald Legal Depth | Breadth | Presence

/ Protecting Sensitive Data as Double Extortion Ransomware Rises

Handling large volumes of sensitive data, the legal sector is a perfect target for cyber-criminals. In today's digital world, even the most private legal documents are regularly revised online. From confidential information about M&As to disclosures made under attorney-client privilege, law firms handle data on a daily basis that would be disastrous if leaked, both for the results of individual cases and for these firms' long-term reputations.

Law firms lose on average 5% of their clients following a data breach, while a significant breach can be fatal for a company, as was the case for Mossack Fonseca in 2018 after the leaked Panama Papers. Three years on, ransomware variants like WastedLocker, Maze, and Egregor have raised the stakes higher than ever before.

Double extortion ransomware, where threat actors not only encrypt but also exfiltrate data, adds a further layer of risk to the legal sector, with the possibility that data could be made public on auction sites or online forums on the Dark Web. GDPR fines can cost firms up to 4% of their annual turnover if classified information becomes public knowledge.

Moreover, encrypted data can have a fatal effect on the outcome of legal disputes if essential documents cannot be accessed in time. And paying a ransom is no guarantee of restoring files – around 50% of companies never regain their documents after paying up.

With the pressure of non-compliance and the increasing scale and sophistication of cyber-attacks, now is the time for the legal sector to abandon legacy, signature-based tools in favor of a more advanced approach that uses Self-Learning AI to detect and respond to novel threats.

> Armed with Self-Learning AI, we feel strengthened in our fight for data security – we now know we are able to defend against the threats of tomorrow.
>
> / Ann Chung, General Manager, ONC Lawyers

/ Thwarting Fast-Moving Threats With Self-Learning AI in the Inbox

Darktrace's Immune System platform autonomously prevents, detects, investigates, and responds to threats in real time. It provides protection and visibility across the entire digital ecosystem, fighting threats on every front – from zero-day exploits on endpoint devices, to account compromise on cloud and SaaS platforms, to spear phishing emails in the inbox and beyond.

Many law firms across the world rely on Darktrace's AI-native technology. Self-Learning AI uses machine learning and advanced mathematics to learn the 'pattern of life' for every user and device in an organization, and all the connections between them. Unlike traditional security tools, which are only effective against known threats and low-hanging fruit, Self-Learning AI stops novel attacks on the first encounter through continually updating its understanding of 'normal' and spotting subtle deviations across the digital ecosystem.

Darktrace RESPOND, Darktrace's Autonomous Response capability, responds to emerging threats within seconds. Its machine-speed reaction is crucial in stopping fast-moving ransomware before it has had the chance to develop, as well as providing essential support for human security teams who cannot be expected to respond in time.

Darktrace Self-Learning AI allows law firms globally to demonstrate a serious cyber security strategy, one in line with client expectations, and to increase confidence in their defenses against all threats.

> Darktrace has enabled us to take our cyber security to a level we presumed unattainable. We can defend our network 24/7 and address unfolding threats before they cause harm.
>
> / Asfar Sadewa, Head of IT, Jackson McDonald

/ Stopping Crypto-Jacking and a Botnet Army at K&L Gates

K&L Gates, a global law firm with 45 offices worldwide and gross revenue in excess of $1.2 billion, implemented Self-Learning AI to protect its digital business. The initial installation took under an hour, and Darktrace's AI immediately started developing an understanding of every user and device in the organization.

Soon after installation, Darktrace DETECT discovered a number of genuine threats, including a covert crypto-jacking operation and the use of a non-compliant VPN that threatened to take corporate devices into the fold of a large botnet army. Darktrace's AI instantly identified these incidents, alerting the security team before this could become a crisis.

Armed with Darktrace, K&L Gates can confidently defend its critical data, as Self-Learning AI detects even the most sophisticated and stealthy threats that other tools miss.

Figure 1: Darktrace RESPOND autonomously neutralizes threats, surgically blocking malicious activity

About Darktrace

Darktrace (DARK.L), a global leader in cyber security AI, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. We protect more than 7,400 customers from the world's most complex threats, including ransomware, cloud, and SaaS attacks. Darktrace is delivering the first-ever Cyber AI Loop, fueling a continuous security capability that can autonomously spot and respond to novel in-progress threats within seconds. Darktrace was named one of TIME magazine's "Most Influential Companies" in 2021.

To learn more, visit darktrace.com

Scan to LEARN MORE