DARKTRACE

INDUSTRY SPOTLIGHT

Cyber Defense for Legal

Law firms and legal services organizations have faced some of the costliest data breaches in recent years due to financial penalties and the high rate of customer defection following compromise.

Because of the valuable, confidential, and highly sensitive nature of the data stored within their networks, the legal industry is often seen by hackers as the 'soft underbelly' of the professional services sector. Poorly protected firms can serve as a threat vector, offering attackers a wealth of valuable information and an easy jumping-on point to client networks.

Meanwhile, digitization means that paper files have been replaced by servers, laptops, cell phones, and the cloud. The use of digital services has made storage cheaper, working habits more flexible, and access to information far easier, but these advantages have also widened organizations' attack surface. Further, the gap in understanding between senior management and their IT teams has contributed to slow responses by the legal industry when it comes to security.

Defending the integrity of this information seems an impossible task. The increasing digitization of sensitive data requires legal organizations to implement new and strict security measures while maintaining the technological flexibility that modern workplaces require.

Firms that suffer from a lack of visibility into their evolving network environments are struggling to pinpoint and mitigate threats effectively. As attacks increase in sophistication and the regulatory environment moves towards tighter disclosure mandates and steeper fines, the legal industry must take a more proactive approach when it comes to cyber defense.

CDH Cliffe Dekker Hofmeyr

Jackson McDonald Legal Depth | Breadth | Presence

Clifford Chance

Sackers

DAC Beachcroft

Shook Lin & Bok

Nutter

Wolf Greenfield Specialists in Intellectual Property Law

IM irwinmitchell solicitors

> Darktrace allows us to show that we are on top of cyber security: we are monitoring, we are alerting, we are investigating, and not just small areas of our network but all of our network
>
> **Mark Vivian, Head of IT Security, Irwin Mitchell**

Threats By Numbers

Hacked legal organizations lose **5%** of their clients following a data breach.

Clients must be able to trust that their counsel will protect the integrity of their information during high-stakes litigation. As a result, they are holding firms to higher security standards than ever before and demanding that cyber risk is intelligently and continually addressed.

41% of incidents are caused by employees.

Humans are often a firm's weakest link. Because they often have privileged access, malicious insiders can cause immense damage. Non-malicious employees can also pose a risk, as even the best workers may contravene security policies for the sake of efficiency or fall prey to attackers that seek access by manipulating trust. No matter how well trained personnel are, human error is always a risk.

DARKTRACE

CASE STUDY

K&L Gates

K&L GATES

Background

Established in 1883, K&L Gates is a global law firm that represents leading corporations in every major industry across five continents. Headquartered in the United States, K&L Gates has 45 offices worldwide, nearly 2,000 attorneys, and gross revenue in excess of $1.2 billion. The firm takes a distinctively integrated approach to client services, working across international offices to manage clients in areas ranging from energy and finance, through to intellectual property, real estate, and litigation.

Challenge

The legal sector is a prime target for cyber-crime, including fast-moving ransomware, insider threat, and 'low and slow' attacks. As one of the largest law firms in the world, K&L Gates was particularly concerned about client confidentiality, the increasing risk of third-party 'relationship hijacking', and defending its mission-critical intellectual property, such as case work and litigation strategies. To protect its critical data and maintain client trust, K&L Gates recognized the need to augment its security stack with cyber AI technology that can autonomously detect and fight back against advanced threats.

> Darktrace's early threat detection capabilities have made us more confident than ever in our firm's ability to spot advanced threats, before they have time to do damage.
>
> **Dave Coughanour, Director of Security, K&L Gates**

Solution

With these concerns in mind, K&L Gates decided to deploy Darktrace's Enterprise Immune System into the core of its network. The initial installation took under an hour, and Darktrace's AI immediately started learning the normal 'pattern of life' for every user and device on the network.

Soon after installation, the Enterprise Immune System detected a number of genuine threats, including a covert crypto-mining operation and 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, as they represented a deviation from the firm's normal 'pattern of life'.

While the organization's existing tools disturbed the use of these technologies, Darktrace allowed the firm to fully remediate the issues with much less effort than their previous approach. Armed with the Enterprise Immune System, K&L Gates can confidently defend its critical data, as Darktrace's cyber AI technology detects even the most sophisticated and stealthy threats that other tools miss.

"Maintaining our clients' trust is core to who we are as a law firm," said Dave Coughanour, Director of Security at K&L Gates. "Darktrace's early threat detection capabilities have made us more confident than ever in our firm's ability to spot advanced threats, before they have time to do damage."