DARKTRACE

CASE STUDY

Aptean

Overview

Industry

- Technology

Challenge

- Gaining visibility into complex cloud infrastructure
- Securing global network and remote users
- Inability of legacy tools to detect novel cyber-threats
- Difficulty of parsing through hundreds of false positives

Results

- Deployed the Enterprise Immune System and Darktrace Cloud
- Achieved 100% network and cloud visibility for the first time
- Immediately detected exposed desktop and cryptojacking activity
- Dramatically reduced incidence of false positive alerts

Business Background

Aptean is an international software company that creates industry-specific solutions designed to support its customers' unique business models. These solutions include Enterprise Resource Planning (ERP), Supply Chain Management (SCM), Manufacturing Execution Systems (MES), and compliance tools. Headquartered in Alpharetta, Georgia, Aptean has offices in North America, Europe, and Asia-Pacific. To protect its expansive global network as well as its cloud environments from today's sophisticated cyber-attackers, the company sought an advanced security tool that could enable the oversight of its entire enterprise in a unified view.

> We have offices and users around the world, so visibility was a huge challenge. Darktrace has become an indispensable tool for us: it illuminates our network and cloud infrastructure in real time.
>
> **Jason Barr, CISO, Aptean**

Challenge

With sensitive data housed both on premises and in the cloud, Aptean recognized the imperative of analyzing all of its global network traffic and cloud instances for malicious activity. Such comprehensive visibility has become essential to thwart cloud-based attacks, which often gain entry by exploiting common security blind spots and critical misconfigurations on the customer end. Yet specialized cloud security tools like CASBs lack the crucial context of on-premise network activity, rendering them ineffective at differentiating between behaviors that are benign under one circumstance but harmful in another. To shine a light on its unique cloud attack vectors, the company needed a security tool capable of correlating security insights from across the digital infrastructure.

"Conventional cloud security tools simply can't keep up as attacks change," commented Jason Barr, CISO at Aptean. "Darktrace AI adapts while on the job, allowing us to defend the cloud with confidence."

Beyond cloud-based threats, Aptean's security stack was poorly equipped to counter the fast-acting and never-before-seen attacks that characterize the modern threat landscape. It relied heavily on a SIEM tool that required extensive care and feeding, a significant amount of operational overhead, and months to optimize. At the same time, the company's security team could not tune the SIEM to detect novel threats, since it had no way of knowing what these attacks would look like. Even among the alerts that the SIEM managed to generate, Barr noted that the overwhelming majority were false positives that not only inundated the team with unnecessary work, but also hindered their ability to investigate genuine threats.

Solution

Following the completion of a successful Proof of Value (POV), Aptean deployed Darktrace's Enterprise Immune System, including Darktrace Cloud. By leveraging artificial intelligence developed at the University of Cambridge, the Enterprise Immune System learns the normal 'pattern of life' of every Aptean user, device, and container. This continuously refined sense of 'self' — which evolves as the company's employees change and its infrastructure expands — enables Darktrace AI to detect even subtle deviations from normalcy. Thus, unlike SIEMs pre-programmed to spot known attacks, Darktrace's unique approach catches never-before-seen threats before they do damage.

"With our SIEM tool, I may see 500 alerts for every one that's something of value," commented Barr. "Darktrace automatically weeds out those false positives, which lets our team focus attention where it's needed."

After deploying Darktrace Cloud to defend its SaaS applications, Aptean's security team also gained immediate insight into its activity in Box and Office 365. By correlating a number of weak indicators of potential compromise — across both these services and the on-premise network — Darktrace AI understands emergent threats against Aptean's hybrid infrastructure more comprehensively than any other tool can.

> As a SaaS provider ourselves, we know the importance of securing our cloud services against advanced attacks. Darktrace's approach is the best on the market today at finding cloud-based threats before they escalate.
>
> **Jason Barr, CISO, Aptean**

Benefits

Right away during the POV process, Darktrace detected a number of serious threats on Aptean's network, including crypto-mining activity that was sapping resources from the company without its knowledge. The incidence of such 'crypto-jacking' has skyrocketed in the past several years, due to the soaring value of cryptocurrencies like bitcoin, the widespread availability of ready-to-deploy crypto-mining kits, and the expensive computing power required for the task. Indeed, the energy it takes to mine a single bitcoin can cost anywhere from $531 to $26,170 — a bill that is often foisted upon unsuspecting companies and governments. Darktrace's highly intuitive user interface, Threat Visualizer, shines a light on these subtle behaviors while facilitating future investigation at any level of detail.

Darktrace helps Aptean stay a step ahead of today's sophisticated attackers, affirming the firm confidence in the integrity of its data and the resilience of its infrastructure. And whereas there is no silver bullet when it comes to cyber security, the Enterprise Immune System gives Aptean's security team confidence that it can detect and fight back against tomorrow's attackers — whether they strike on-premise or in the cloud.

Contact Us

North America: +1 415 229 9100

Latin America: +55 11 97242 2011

Europe: +44 (0) 1223 394 100

Asia-Pacific: +65 6804 5010

info@darktrace.com

darktrace.com