

Prudential plc



Overview

Industry

- Financial services

Challenge

- Need for AI to scale with scope of international business
- Flood of false positive alerts generated by conventional tools
- Difficulty achieving visibility over dynamic cloud architecture
- Challenge of detecting never-before-seen cyber-threats

Results

- Deployed the Enterprise Immune System on-premises and in the cloud
- Leveraged AI to learn 'normal' on the job and defend millions of assets and entities
- Gained visibility over expansive digital infrastructure for the first time
- Automatic prioritization of alerts enabled team to focus on high-level tasks

Business Background

Founded in 1848, Prudential plc is today one of the world's largest life insurance companies, managing more than \$800 billion in assets. The company has over 20,000 employees, who work to provide tailored policies to 26 million customers across four continents.

“

Our team needs to understand billions of network events, and the Enterprise Immune System is the only tool capable of operating at that scale to cut through the noise.

”

Guillermo Guerra, VP and CISO, Prudential

Challenge

With a vast hybrid and multi-cloud infrastructure to defend, Prudential could no longer rely on its siloed security solutions. These tools afforded the security team only a segmented, incomplete view of internal user traffic, rather than the enterprise-wide understanding of the business necessary to detect sophisticated threats.

What is more, the tools Prudential leveraged to protect its thousands of laptops, mobile devices, and cloud services inundated the security team with too many alerts to parse in a timely manner. Although the majority of these alerts were not related to malicious activity, each nevertheless required investigation, preventing the team from focusing on higher-level work.

Solution

Prudential soon deployed Darktrace's Enterprise Immune System across its global hybrid infrastructure. The Enterprise Immune System immediately began learning the normal 'pattern of life' of every user, device, and cloud environment. And as the company's employees change and its infrastructure expands, Darktrace AI keeps pace by continuously refining its understanding of the digital business.

Critically, this evolving sense of 'self' enables the Enterprise Immune System to spot the anomalous behavior indicative of a threat, including never-before-seen strains of malware and subtle insider threats that traditional tools are not designed to detect.

"Darktrace gives us visibility over our entire network from a single screen," commented Guillermo Guerra, VP and CISO at Prudential. "We have total confidence in its ability to catch attacks before they escalate."

Darktrace AI has proven especially valuable in defending the company's IaaS and SaaS platforms, where the unintentional exposure of private workloads to the public internet is far from uncommon. The Enterprise Immune System is able to flag these subtle misconfigurations because, unlike conventional tools that apply uniform rules to defend disparate users and cloud environments, Darktrace AI develops a nuanced understanding of normal for each entity it safeguards.

“

Without artificial intelligence, our SOC analysts would not be able to maintain our most sensitive assets.

Guillermo Guerra, VP and CISO,
Prudential plc

”

Benefits

Darktrace's self-learning approach to security has all but evaporated the flood of false positive alerts that once overwhelmed the security team. The Enterprise Immune System correlates hundreds of weak indicators to sift through the noise, automatically prioritizing the most urgent incidents.

Moreover, Darktrace's technology did not require a 'rip and replace' of Prudential's already deployed legacy tools; rather, it complements these tools and can often serve as a 'truth platform' that helps validate the output of the rest of the security stack. In Darktrace's Threat Visualizer interface, Prudential's digital business is mapped out in real time. Further, the interface's playback feature gives the security team the ability to investigate historical incidents at any level of detail according to specific parameters.

"We're using the Threat Visualizer to corroborate alerts we see on our other security tools," commented Guerra. "It's been a huge value add from the start."

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