DARKTRACE

CASE STUDY

Brooks Brothers

Overview

Industry

- Retail

Challenge

- Lack of visibility and control over complex hybrid infrastructure
- Inability to contain automated, machine-speed cyber-attacks
- Abundance of false positive alerts from conventional tools
- Vulnerabilities exposed by manufacturing supply chains

Results

- Deployed the Enterprise Immune System and Darktrace Antigena
- Achieved 100% visibility of hybrid cloud architecture
- Neutralized attacks in seconds using Autonomous Response AI
- Eliminated false positive alerts and dramatically reduced triage time

Business Background

Founded in 1818 with a single store in New York City, Brooks Brothers today boasts more than 250 locations in the United States, as well as over 250 locations internationally. The time-honored clothier is credited with introducing several staples of modern fashion to the US, including the ready-made suit and the button-down polo shirt.

> We needed a tool that understands how our unique business works, and that can scale as we grow and change over time. The Enterprise Immune System does both.
>
> **Brooks Brothers**

Challenge

Entrusted with safeguarding extensive manufacturing supply chains, a global workforce several thousand strong, and a rapidly complexifying hybrid infrastructure, Brooks Brothers' security team was overwhelmed. Its array of conventional point solutions proved insufficient to manage such complexity and scale. Instead, they inundated the team with thousands of disjointed, often false positive alerts, which served to drown out genuine security incidents.

Yet today's cyber-attacks are increasingly automated, with, for instance, some strains of ransomware now able to encrypt an entire network in minutes. There is no time for human professionals to triage alerts and take appropriate action — these manual processes will never be as fast as the machine-speed threats they seek to contain. More fundamentally, legacy security systems rely on predefining malicious behavior, which renders them blind to novel threats.

Solution

Brooks Brothers soon deployed the Enterprise Immune System and Darktrace Antigena to defend its global hybrid infrastructure. By leveraging world-leading Cyber AI, the Enterprise Immune System continuously self-learns the typical 'pattern of life' of every Brooks Brothers user, device, cloud container, and virtual machine.

This evolving knowledge of the company enables Darktrace AI to pick up on even the most subtle deviations from normalcy. Thus, unlike traditional, signature-based tools that detect only the attacks of the past, Darktrace's unique approach catches entirely novel attacks, which inevitably exhibit anomalous behavior.

With Darktrace defending its dynamic workloads in the cloud, Brooks Brothers' security team gained immediate oversight over cloud activities that had previously been blind spots. Its real-time analysis of cloud traffic allows the system to go beyond the limited insights that log-based tools provide — while avoiding the complexity of capture agents.

And at a time when cloud services often become unmanageably distributed and decentralized, the Enterprise Immune System's real-time understanding of Brooks Brothers' entire cloud infrastructure has returned control to its security team.

To contain fast-acting attacks in the cloud and on-premises, Brooks Brothers depends on Darktrace Antigena, the first Autonomous Response AI technology. Rooted in the Enterprise Immune System's knowledge of 'self' for the firm, Antigena confines compromised devices and cloud containers to their normal 'patterns of life' during incidents, intelligently intervening to contain the threat while allowing normal operations to continue.

Business interruption losses suffered in the aftermath of cyber-attack can cost millions of dollars and countless hours of productivity, rendering Antigena's surgical response invaluable.

> Darktrace Antigena is the only security tool we trust to take machine-speed action on our behalf.
>
> **Brooks Brothers**

Benefits

The Enterprise Immune System enables Brooks Brothers to stay a step ahead of today's sophisticated attacks, affording the firm confidence in the integrity of its data and in the resiliency of its infrastructure. Darktrace also provides total visibility over its extensive supply chains — environments replete with third parties that all represent vectors for compromise.

Critically, the Enterprise Immune System defends the company from the 'inside out'; it spots threats from third-party vendors that have already bypassed the perimeter, which Antigena then neutralizes autonomously.

Moreover, Darktrace has all but eliminated the problem of false positive alerts that plagued the company's previous security posture. Rather than rely on black-and-white rules that cast a wide net to spot malicious activity — while flagging benign activity in the process — Darktrace leverages probabilistic mathematics to correlate hundreds of weak indicators and cut through the noise.

"With Darktrace, our strained team can focus on the security incidents that matter most." — Brooks Brothers

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