VECTRA
SECURITY THAT THINKS.®

CASE STUDY

Greenhill stops cyberattacks from enterprise to Office 365 SaaS

At the investment bank of Greenhill and Co., helping clients manage risk is core to its business.

Headquartered in New York City, the renowned investment bank provides financial advice on significant mergers, acquisitions, and restructurings to institutions and governments worldwide.

Greenhill's clients include Alcoa, Experian, Gannett, GlaxoSmithKline, and the governments of the United States, Canada, the United Kingdom and Australia.

Reducing cyber risk

Greenhill makes it a regular practice to reduce both business and cyber risk.

"We needed more visibility in our network to identify cyberattack behaviors," recalls Greenhill CIO, John Shaffer.

> "Attackers today evade firewalls, IDS and other legacy security systems and spread inside the network looking for assets to steal."
>
> **John Shaffer**
> *CIO*
> *Greenhill*

Greenhill used its SIEM tools but "we had a tough time figuring out which firewall logs – lots of them – were serious and which ones were not," says Shaffer.

Shaffer was also concerned about the rise in credential abuse and account takeovers in SaaS platforms like Microsoft Office 365, which affects more than 30% of organizations each month. Attackers use social engineering to exploit human behavior, elevate account privileges and steal critical business-data.

Greenhill

Organization

Greenhill

Industry

Financial Services

Challenge

Needed more visibility into the network and an easier way to identify which threats were critical and which threats were not

Selection criteria

An AI-based network detection and response (NDR) solution that quickly identifies critical threats worth investigating and provides network visibility

Results

- Ability to focus on investigations and proactive threat hunting instead of chasing-down logs
- Confidence in identifying and stopping privilege escalation and account takeovers in Office 365
- AI-based algorithms that save time and effort for their security staff
- Can now pinpoint attacker behaviors on the network and immediately shut down attacks on the endpoint

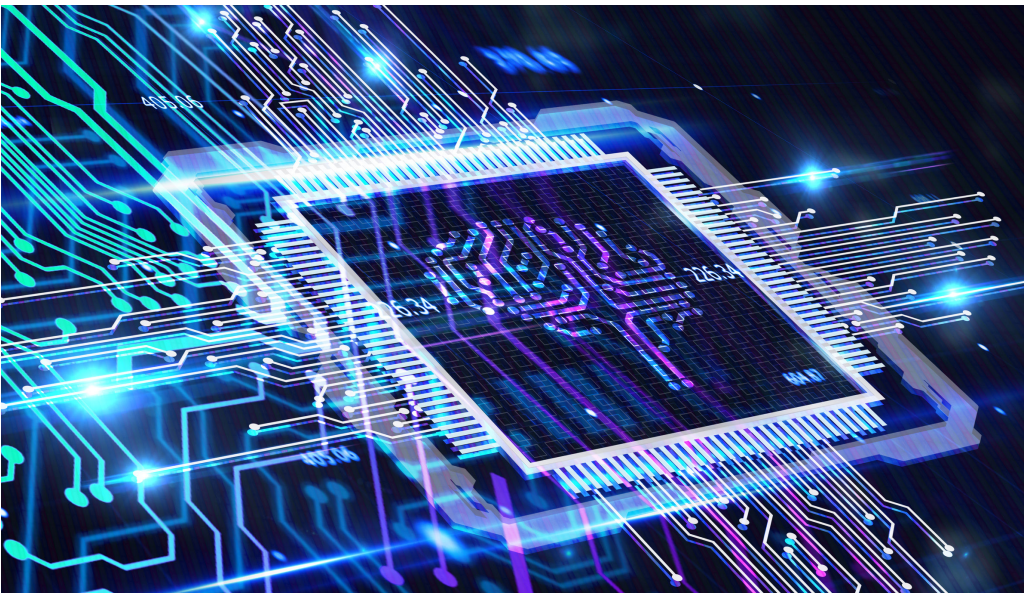
Solution: The Cognito NDR platform

Greenhill was an early adopter of Cognito Detect™ AI software, which runs on the Cognito® network detection and response (NDR) platform from Vectra®.

Cognito Detect leverages AI to instantly identify and stop cyberattackers in cloud and data center workloads, SaaS offerings like Microsoft Office 365, and user and IoT devices.

"Most threats we deal with aren't solved by traditional tools like antivirus software or anything that has a signature," Shaffer says. "Real threat actors know how to get past them. We're interested in figuring out what smart actors are doing. That's where Vectra AI and machine learning come into play."

Cognito Detect uses AI-derived machine learning algorithms to automatically detect, prioritize and respond to in-progress attack behaviors that pose the highest business risk – across cloud, data center, IoT, and enterprise networks.



"Cognito for Office 365 is a windfall in light of how attackers are compromising and taking over accounts. As a long-time Vectra customer, I have confidence in identifying and stopping privilege escalation and account takeovers in Office 365."

John Shaffer
CIO
Greenhill

By automating manual and mundane Tier-1 and Tier-2 security tasks like attacker detections and triage, Cognito Detect significantly reduces the security operations workload at Greenhill.

"The automation from Cognito has made a big difference," says Shaffer. "After sorting through tons of security logs, alert fatigue set in. Now, we focus on investigations and proactive threat hunting instead of chasing-down logs."

For more conclusive incident investigations and AI-assisted threat hunting, Cognito Detect extracts metadata from all network traffic and enriches it with detailed security context about each attack, including all compromised users, accounts, devices, and whether the attack is part of a larger campaign.

When Shaffer first deployed Cognito Detect, it immediately alerted him to some odd traffic patterns on the bank's network that turned out to be the firm's own vulnerability scanner.

"To a lot of systems, that would look like threat actor doing a scan on the network," Shaffer notes. "This illustrates why it's important to know what's happening in the network."

"The AI-based algorithms from Vectra learn the difference between normal behavior and malicious behavior, saving time and effort for our security staff."

John Shaffer
CIO
Greenhill

Stopping data breaches in Office 365

Running on the Cognito NDR platform, Cognito Detect for Office 365 ingests activity logs from multiple Office 365 SaaS services like Azure Active Directory, SharePoint, OneDrive, Exchange, and Teams.

With a deep understanding of Office 365 application semantics, Cognito Detect for Office 365 applies AI-derived machine learning algorithms to proactively detect and respond to hidden cyberattackers and stop data breaches.

To identify credential abuse and account takeovers, Cognito Detect for Office 365 analyzes malicious behavior patterns in logins, file creation and manipulation, data loss protection configuration, and mailbox routing configuration and automation changes.

Detections are correlated to user account privileges and prioritized based on risk, giving Greenhill a complete attack narrative to quickly respond and mitigate attacks and stop data breaches.

For more information please contact a service representative at info@vectra.ai.

Protect investments and reduce the workload

To accelerate response time, the Cognito NDR platform integrates and shares threat insights and context with third-party security solutions – including EDR, SIEMs, SOAR tools, firewalls, and NAC – for end-to-end threat management and visibility.

However, the two solutions that Greenhill relies on most are NDR from Vectra and EDR from CrowdStrike.

"Every day is a race to stay ahead of threat actors," says Shaffer. "We need the fastest way to pinpoint attacker behaviors on the network and immediately shut down attacks on the endpoint. Vectra gives us a head start in the network and CrowdStrike speeds across the finish line at the endpoint."

Correlating and analyzing security information from Vectra and CrowdStrike is required to gauge the full scope of an attack, stop it from spreading, and avoid a data breach, according to Shaffer.

"Vectra doesn't send out overwhelming volumes of alerts like so many security systems do," he adds. "The data is direct and it doesn't require rules to be written. Over time, the AI-based algorithms from Vectra learn the difference between normal behavior and malicious behavior, saving time and effort for our security staff."

"Vectra gives us a head start in the network and CrowdStrike speeds across the finish line at the endpoint."

John Shaffer
CIO
Greenhill

Email info@vectra.ai vectra.ai