VECTRA
SECURITY THAT THINKS.®

CASE STUDY

Vectra helps Blackstone reduce threat detections on O365 by over 50x

Blackstone, the world's largest alternative asset manager, aims to build successful, resilient businesses. Investing in a wide range of assets across private equity, real estate, and technology, Blackstone has a proven track record of bringing forth innovative strategies that enable organizations to solve problems and create value.

One of the ways they continue to deliver is by ensuring their own technology platforms excel alongside their mission. In other words, Blackstone utilizes technology to drive its business—and cybersecurity is a key to the equation.

Securing Blackstone's globally dispersed environment is no small task, especially across a threat landscape swarming with potential cyber-attacks.

Kevin Kennedy, Senior Vice President, Cybersecurity at Blackstone, and the rest of Blackstone's Security Operations team are focused on protecting the firm against cyber-attacks. This team of security professionals knows that keeping eyes on glass at all times enables them to quickly identify when something looks off in their environment.

> "Through one simple integration, completed in just a single day, we were able to add over 50 new threat detections against our Office 365 environment."

Kevin Kennedy
Senior Vice President, Cybersecurity
Blackstone

Blackstone

Organization

Blackstone

Industry

Financial Services

Challenge

Maintaining visibility into Microsoft 365 data to keep their organization secure

Selection criteria

An AI-based detection and response solution that quickly identifies critical threats and provides network visibility across O365 environments

Results

- Addition of over 50 new threat detections against the organization's Office 365 environment in one day
- Reduction of alert volume by 90%
- With Vectra's ability to detect threats that breach the prevention layer, the organization can now identify areas that need a stronger security posture

Capturing an Entire View, 24/7/365

One way Blackstone monitors any potentially malicious activity throughout the environment is by centralizing its alert detection and response capabilities.

Kennedy says doing this is "a way for us to ensure that we can measure our intake and everything coming in, which is really important because, if we can get everything in the same spot, we can prioritize it."

The team also emphasizes understanding specific details about threat detections. For example, knowing exactly what each detection means—and how long it takes from the time an event triggers a detection to when the analyst responds and then completes the investigation—are all critical metrics, according to Kennedy.

"All those metrics matter for us because they give us a good sense of where our analysts are spending their time," he says. "We get a really good sense for what our noisiest detections are, and what our higher-fidelity detections are."

> "Vectra's platform has helped us strengthen our cybersecurity defense capabilities and has made our firmwide cybersecurity program more efficient."
>
> **Kevin Kennedy**
> *Senior Vice President, Cybersecurity*
> *Blackstone*

Vectra reduces alert volume by 90% with Detect for Office 365

With threat detection and response being a focal point for Blackstone, deploying Vectra Detect for Azure AD and Microsoft 365 has been a key part of the strategy. Kennedy points out that having visibility into Microsoft 365 data is critical to keeping their organization secure. Blackstone uses Detect for Office 365 to automate and improve the quality of threat detections that the team receives, which is a step up from the native detection features previously used.

One major component that differentiates Vectra from other solutions is that it leverages artificial intelligence to identify threat behaviors in Microsoft 365 data. This facilitates all light detection engineering for Blackstone's Cybersecurity team and maps the detections to the MITRE ATT&CK framework, which provides a good sense of coverage across common attack behaviors. "The signal-to-noise ratio from low fidelity to high fidelity is all done basically upstream by Vectra. Vectra's platform has helped us strengthen our cybersecurity defense capabilities and has made our firmwide cybersecurity program more efficient," Kennedy says.

This has been a significant upgrade for the Blackstone team, especially in terms of time saved. Before Vectra, developing a complicated detection could take up to six months, whereas with Detect for Office 365, "through one simple integration, completed in just a single day, we were able to add over 50 new threat detections against our Office 365 environment," Kennedy says. "Our alert volume has been reduced by 90% since Vectra's ML assesses more features and context in the models, which leads to more accurate detections."

"Before, it was just too noisy and hard to distill," Kennedy adds. "With the Vectra platform, we were able to get that tuned pretty quickly, and now the items that come into our case management tool from Vectra on Office 365 are significantly higher fidelity."

> "Our alert volume has been reduced by 90% since Vectra's ML assesses more features and context in the models, which leads to more accurate detections."
>
> **Kevin Kennedy**
> *Senior Vice President, Cybersecurity*
> *Blackstone*

Leading the Way with a Proactive Approach Against Today's Cyberthreats

Blackstone is taking steps to defend against today's attacks by partnering with Vectra. With Microsoft 365 being a focus area and one where account takeover attacks are quickly becoming one of the largest threats in the cloud, Vectra mitigates this risk by understanding attacker behavior and identifying when a privileged account has been compromised.

Kennedy says that the improvements seen in Blackstone's detection and response capabilities have even helped his team better understand where their prevention systems need attention.

Vectra's ability to detect threats that breach the prevention layer now allows Blackstone to identify areas previously unknown to them that need a stronger security posture.

From the diligent 24/7, centralized approach that Blackstone has implemented with its security operations, to the proactive detection and response monitoring, this investment giant is making all the right moves when it comes to defending against today's cyberthreats.

For more information please contact us at info@vectra.ai.

Email info@vectra.ai vectra.ai