Big Bazar

At a Glance

- Self-Learning AI protects Microsoft Azure environment
- Protects endpoint devices for a hybrid workforce
- Antigena Email stops impersonation attacks

Big Bazar is a Dutch retail chain carrying gifts, décor, kitchenware, tools and more. Since its inception in 2007, the company has grown rapidly, and now serves the Netherlands and Belgium with over 130 stores.

Self-Learning AI in the Cloud

Before Darktrace, Big Bazar relied heavily on native cloud security. While this proved sufficient for stopping many 'known' attacks, it became clear that Big Bazar would still be vulnerable to attackers using sophisticated, novel techniques. Ransomware was a key concern, with numerous stories emerging of other major retailers falling victim to devastating attacks.

Big Bazar's IT Manager, Evert Zaal was increasingly worried by the lack of visibility he had over a widening digital environment. "We became a bigger target for attackers with the introduction of email and a cloud-based portal for our stores," he explains, "Microsoft Defender gave us good level of protection from known viruses, but we felt we needed an extra layer of defense with AI."

Darktrace protects the entire Microsoft product suite, including the data centers hosted in Azure which Evert and the team at Big Bazar rely upon to sustain their retail chain's online presence. Its easy integration with Microsoft Defender allows Darktrace to share data with Big Bazar's existing security tools and elevate their threat detection and investigation efforts with Self-Learning AI.

"With Autonomous Response active across the entire digital estate, our network, endpoints and email & cloud systems are protected under a single umbrella."

Evert Zaal, IT Manager, Big Bazar

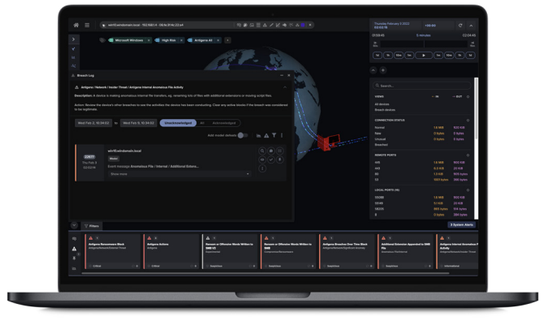
DARKTRACE

Big Bazar

Extending Darktrace Coverage to the Endpoint

As Big Bazar adapted to hybrid working, the security team quickly recognized the value of extending Darktrace's coverage to remote endpoints. Self-Learning AI uses its unique understanding of each user and device to spot subtle behavioral shifts which might indicate emerging threats. Antigena Endpoint then takes targeted action to neutralize serious attacks within seconds, without the need for human intervention.

Evert was concerned that employees accessing corporate devices for personal use might unknowingly become insider threats and allow an attack through: "The biggest threat is and always will be the end-user. But with Antigena Endpoint, we now have far more insight into device and user behavior, and are protected with a 24/7 response." The autonomous action taken against malicious behavior on these devices is precise and proportionate, meaning normal business activity continues undisrupted as threats are stopped.



Darktrace's findings and autonomous actions are shown in the Threat Visualizer

Protecting the Inbox with Antigena Email

Prior to Big Bazar's adoption of Darktrace, the potential for a serious cyber-attack wasn't simply theoretical. They were the target of numerous impersonation emails circumventing rules-based security tools and reaching company Directors. Once Evert had employed Darktrace's Antigena Email and it began detecting the most sophisticated and well-disguised of these impersonation emails, however, he realized the problem had been even worse than he thought: "The amount of attempted email attacks we receive on a daily basis is immense. You never really realize it until a system like Darktrace gives you full insight into your inbox and shows you the full extent of what it's keeping out."

When attackers impersonate or even hijack email addresses which are trusted by an organization, they become incredibly difficult for rules-based security to spot. Antigena Email uses its deep understanding of a user's normal behavior to detect when these account takeovers have taken place and keep malicious mail out of the inbox.

With the same self-learning approach operating across its cloud, email and endpoints, the security team's workflow is simplified, and attacks that span across different areas of the digital estate are stopped at every turn. "The effects were immediate," Evert recalls, "within one week of Darktrace going live, the impersonation attacks constantly targeting my CEO had disappeared, and we had stopped several threats on our network."

"The amount of attempted email attacks we receive on a daily basis is immense. You never really realize it until a system like Darktrace gives you full insight into your inbox and shows you the full extent of what it's keeping out."

Evert Zaal, IT Manager, Big Bazar