Detecting Unknown Ransomware: A Darktrace Case Study

By Emma Foulger

Published: 2022-08-24 · Archived: 2026-04-05 18:52:59 UTC

Protecting a complex, fast-growing retail organization

For this multi-banner grocery holding organization, cybersecurity is considered an essential business enabler, protecting operations, growth, and customer trust. The organization's lean IT team manages a highly distributed environment spanning corporate offices, 100+ stores, distribution centers and thousands of endpoints, users, and third-party connections.

Mergers and acquisitions fueled rapid growth, but they also introduced escalating complexity that constrained visibility into users, endpoints, and security risks inherited across acquired environments.

Closing critical visibility gaps with limited resources

Enterprise-wide visibility is a top priority for the organization, says the Vice President of Information Technology. "We needed insights beyond the perimeter into how users and devices were behaving across the organization."

A security breach that occurred before the current IT leadership joined the company reinforced the urgency and elevated cybersecurity to an executive-level priority with a focus on protecting customer trust. The goal was to build a multi-layered security model that could deliver autonomous, enterprise-wide protection without adding headcount.

Managing cyber risk in M&A

Mergers and acquisitions are central to the grocery holding company's growth strategy. But each transaction introduces new cyber risk, including inherited network architectures, inconsistent tooling, excessive privileges, and remnants of prior security incidents that were never fully remediated.

> "Our M&A targets range from small chains with a single IT person and limited cyber tools to large chains with more developed IT teams, toolsets and instrumentation," explains the VP of IT. "We needed a fast, repeatable, and reliable way to assess cyber risk before transactions closed."

AI-driven security built for scale, speed, and resilience

Rather than layering additional point tools onto an already complex environment, the retailer adopted the Darktrace ActiveAI Security Platform™ in 2020 as part of a broader modernization effort to improve resilience, close visibility gaps, and establish a security foundation that could scale with growth.

"Darktrace's AI-driven approach provided the ideal solution to these challenges," shares the VP of IT. "It has empowered our organization to maintain a robust security strategy, ensuring the protection of our network and the

smooth operation of our business."

Enterprise-wide visibility into traffic

By monitoring both north-south and east-west traffic and applying Self-Learning AI, Darktrace develops a dynamic understanding of how users and devices normally behave across locations, roles, and systems.

"Modeling normal behavior across the environment enables us to quickly spot behavior that doesn't fit. Even subtle changes that could signal a threat but appear legitimate at first glance," explains the VP of IT.

Real-time threat containment, 24/7

Adopting autonomous response has created operational breathing room for the security team, says the company's Cybersecurity Engineer.

"Early on, we enabled full Darktrace autonomous mode and we continue to do so today," shares the IT Security Architect. "Allowing the technology to act first gives us the time we need to investigate incidents during business hours without putting the business at risk."

Unified, actionable view of security ecosystem

The grocery retailer integrated Darktrace with its existing security ecosystem of firewalls, vulnerability management tools, and endpoint detection and response, and the VP of IT described the adoption process as "exceptionally smooth."

The team can correlate enterprise-wide security data for a unified and actionable picture of all activity and risk. Using this "single pane of glass" approach, the retailer trains Level 1 and Level 2 operations staff to assist with investigations and user follow-ups, effectively extending the reach of the security function without expanding headcount.

From reactive defense to security at scale

With Darktrace delivering continuous visibility, autonomous containment, and integrated security workflows, the organization has strengthened its cybersecurity posture while improving operational efficiency. The result is a security model that not only reduces risk, but also supports growth, resilience, and informed decision-making at the business level.

Faster detection, faster resolution

With autonomous detection and response, the retailer can immediately contain risk while analysts investigate and validate activity. With this approach, the company can maintain continuous protection even outside business hours and reduce the chance of lateral spread across systems or locations.

Enterprise-grade protection with a lean team

From cloud environments to clients to SaaS collaboration tools, Darktrace provides holistic autonomous AI defense, processing petabytes of the organization's network traffic and investigating millions of individual events that could be indicative of a wider incident.

Today, Darktrace autonomously conducts the majority of all investigations on behalf of the IT team, escalating only a tiny fraction for analyst review. The impact has been profound, freeing analysts from endless alerts and hours of triage so they can focus on more valuable, proactive, and gratifying work.

> "From an operational perspective, Darktrace gives us time back," says the Cybersecurity Engineer. More importantly, says the VP of IT, "it gives us peace of mind that we're protected even if we're not actively monitoring every alert."

A strategic input for M&A decision-making

One of the most strategic outcomes has been the role of cybersecurity on M&A. 90 days prior to closing a transaction, the security team uses Darktrace alongside other tools to perform a cyber risk assessment of the potential acquisition. "Our approach with Darktrace has consistently identified gaps and exposed risks," says the VP of IT, including:

- Remnants of previous incidents that were never fully remediated
- Network configurations with direct internet exposure
- Excessive administrative privileges in Active Directory or on critical hosts

While security findings may not alter deal timelines, the VP of IT says they can have enormous business implications. "With early visibility into these risks, we can reduce exposure to inherited cyber threats, strengthen our position during negotiations, and establish clear remediation requirements."

A security strategy built to evolve with the business

As the holding group expands its cloud footprint, it will extend Darktrace protections into Azure, applying the same AI-driven visibility and autonomous response to cloud workloads. The VP of IT says Darktrace's evolving capabilities will be instrumental in addressing the organization's future cybersecurity needs and ability to adapt to the dynamic nature of cloud security.

"With Darktrace's AI-driven approach, we have moved beyond reactive defense, establishing a resilient security foundation for confident expansion and modernization."
