DARKTRACE | Technologent®

Technologent

94%

of all potential incidents autonomously resolved over three-month span

168

security analyst investigation hours saved in one month

1m 33s

to autonomously respond to potential incidents

As both a Darktrace solution provider and customer, Technologent strengthened its cybersecurity operations with AI-driven autonomous response while guiding customers through their own AI-powered security journeys.

"As a practitioner, you have to get it right all the time. But threat actors only have to get it right once. We needed a tool that could help us be proactive and take action against potential threats even when we weren't at the helm."

■ **Jon Mendoza**
CISO, Technologent

When protecting the business means protecting trust

As a global IT solutions provider trusted by Fortune 1000 organizations, reputation is foundational to Technologent's business. Any security lapse would have far-reaching consequences, not just for internal operations, but for customer trust and market credibility.

For that reason, says Technologent's CISO, Jon Mendoza, cybersecurity is inseparable from the company's mission. "We practice what we preach and are committed to continuously improving our security posture."

Like many organizations, Technologent faced a fragmented security landscape. Traditional tools provided visibility at the perimeter and endpoint level, but offered limited insight into internal, east-west network activity. This created blind spots around lateral movement, internal activity, and anomalous behavior that didn't trigger signature-based controls.

Compounding the challenge was scale. Technologent's lean teams support both internal operations and customer-facing engagements. Continuous manual monitoring was not realistic. The organization needed a way to maintain vigilance without increasing headcount or overwhelming already-busy teams.

Rethinking security with Self-Learning AI

Mendoza first began following Darktrace in 2017, when AI in cybersecurity was still in the early stages. He found Darktrace's use Self-Learning AI particularly compelling with its ability to understand what's "normal" for every user, device, and workload, rather than relying on predefined rules or historical threat intelligence.

"As a practitioner, you have to get it right all the time. But threat actors only have to get it right once," Jon says. "We needed a tool that could help us be proactive and take action against potential threats even when we weren't at the helm."

Technologent initially engaged with Darktrace as a solution provider, introducing the solution to customers seeking adaptive, autonomous security. Over time, seeing the technology mature and deliver consistent results in customer environments, Mendoza made a deliberate decision: if he was going to advocate for Darktrace, Technologent needed to run it internally.

"If I can't say in good conscience that I would buy it myself, then I'm being disingenuous," he explains. "Using it internally lets me show customers how we actually operationalize the technology; how it cuts down headaches and makes us demonstrably more secure."

Deployment journey: A phased approach to autonomy

Darktrace seamlessly integrated into Technologent's existing environment. "If this was going to take weeks of effort, we would have hesitated," Mendoza says. "But Darktrace made deployment straightforward, and the support we received made a big difference."

The team initially deployed Darktrace / NETWORK™ in Human Confirmation mode. This phased approach gave IT and security teams the opportunity to observe how the AI modeled normal behavior and surfaced anomalies without automatically taking action.

"It was very much a 'show me first' mindset," says Mendoza. "The IT team wanted to see effectiveness before trusting autonomy. And that was okay. I was confident we'd get there."

This gradual rollout proved critical in building trust across teams. Darktrace quickly demonstrated value by delivering continuous east-west visibility that Technologent didn't have before. The platform detected unexpected internal scans, unusual credential usage, and anomalous data transfers, providing context that traditional tools missed.

In one notable incident, Darktrace alerted the team to a large internal download that was consuming bandwidth during the final days of a quarter. While not malicious, it was impacting critical business operations. "We would have blamed the service provider or stared at firewall logs," Jon recalls. "Darktrace showed us exactly what was happening, and we solved the problem quickly.

As confidence grew, Technologent enabled Autonomous Response mode, allowing Darktrace to take precise, proportionate action to contain threats in real time, allowing analysts to prioritize genuine threats over noise.

Operational confidence replaces alert overload

By relying on Darktrace Autonomous Response as its first line of defense, Technologent significantly reduced manual triage and investigation, saving 168 security analyst investigation hours within a single month.

Darktrace analyzes the millions of individual events that contribute to a wider incident, determines if they warrant further investigation, and then either resolves routine anomalies or escalates those few incidents that require human judgment.

Over a three-month period, Darktrace autonomously resolved 94% of all potential incidents, escalating just 6% to Technologent's analysts for further investigation.

With **24/7 proactive protection,** Technologent has achieved meaningful improvements across technology performance, operational efficiency, and business resilience, including:

- Reduced alert fatigue for security and IT teams
- Accelerated containment of anomalous behavior
- Around-the-clock internal visibility across users and devices
- Reclaimed time for proactive initiatives, rather than reactive firefighting

From managing risk to influencing revenue

The benefits of using Darktrace extended far beyond the SOC.

For IT operations, improved visibility meant faster troubleshooting and fewer disruptions. For leadership, it reinforced confidence that risk was being actively managed. And for sales teams, it became a powerful credibility accelerator.

“When customers ask how we solve these problems, I can show them our actual environment. Not a demo. Not a lab. Our real-world data. That changes the conversation,” says Mendoza. “It shifts my role from simply selling to truly understanding the customer and meeting them where they are. That’s huge.”

A partnership built around people

For Technologent, the success of the deployment was shaped as much by the human experience as the technology itself. From the outset, Darktrace approached the engagement not as a transactional rollout, but as a true partnership, grounded in responsiveness, empathy, and an understanding of the real-world pressures teams faced.

“Darktrace just made it easy,” says Mendoza. “They supported us throughout the whole process. That mattered, not just because the technology worked, but because it helped me bring the team along. It made this feel like a no-brainer.”

What stood out most to Jon was the consistency of that support. “It wasn’t just about onboarding or a deployment checklist,” he explains. “It was very much a ‘we’re here, what do you need?’ mindset.”

Throughout the rollout, Darktrace team members took time to understand Technologent’s operational realities, from resource constraints to customer-facing responsibilities. That included direct access to knowledgeable people who were invested in Technologent’s success, whether through live conversations, in-person engagement, or ongoing collaboration beyond implementation.

Evolving together for what comes next

Looking ahead, Technologent plans to continue evolving its security strategy alongside Darktrace. Identity remains a top concern, as does the rise of generative and agentic AI in the hands of threat actors. At the same time, Jon sees enormous potential in AI-driven SOC operations and deeper automation across the stack.

“What once felt like science fiction is starting to come together,” he says. “In the next 18 months, I think we’re going to be blown away by what these platforms can do.”

The relationship with Darktrace has extended well beyond deployment. Through opportunities such as advisory participation and direct engagement with product teams, Technologent has been able to share feedback and influence how the platform continues to evolve.

“It never felt like Darktrace just wanted to sell us something,” says Mendoza. “They listened to us as a customer and as a partner. That means a lot.” That human-first approach continues to reinforce Technologent’s confidence, not only in the technology, but in the partnership itself. And for a company that stakes its reputation on guiding others through complex technology decisions, that trust is invaluable.

> “Cybersecurity is still a people business. Knowing someone will pick up the phone, listen, and actually help you solve a problem, that makes a difference.”
>
> ■ **Jon Mendoza**
> CISO, Technologent

About Darktrace

Darktrace is a global leader in AI cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace’s platform and services are supported by 2,700+ employees who protect nearly 10,000 customers globally. To learn more, visit www.darktrace.com.

North America: +1 (415) 229 9100 | Europe: +44 (0) 1223 394 100 | Asia-Pacific: +65 6804 5010 | Latin America: +55 11 4949 7696

darktrace.com | info@darktrace.com