

NCG

20,940

AI investigations conducted autonomously in a single month

97%

of all potential incidents resolved autonomously in a single month

15,835

analyst investigation hours saved over a 24-day period

NCG has transformed its cyber defenses with Darktrace's AI-driven visibility and autonomous response, cutting investigation times from weeks to minutes, reducing analyst stress, and strengthening security across seven colleges.

"The deployment was seamless. No blocked learners, no disabled accounts, no complaints. It just worked and it made us look brilliant."

■ Chris Weeks

Director of Information and Data Services,
NCG

A fragmented environment within a rising threat landscape

NCG is one of the UK's largest education providers, serving more than 30,000 learners across seven colleges. With a commitment to improving lives and driving economic prosperity through accessible, exceptional learning, NCG depends on secure, reliable digital systems to support its students and staff.

Chris Weeks, Director of IDS, is responsible for ensuring the resilience and security of this multi-site ecosystem — all while navigating sector-wide funding constraints, rising cyber threats, and increasing regulatory expectations. When Weeks first stepped into the role in 2022, he had his work cut out for him. Years of mergers and inherited infrastructure created a sprawling environment with multiple domains, siloed systems, and inconsistent levels of security maturity across campuses.

"We had a number of gaps," Weeks recalls. "Identity, content, disaster recovery, business continuity, resilience — all of it."

Lean team stretched by growth, complexity, and compliance

After a series of mergers and absorbing the full IT footprint of each new institution — without staffing increases, NCG was supporting 16 domains, each with its own quirks and vulnerabilities. But the company lacked holistic visibility across those domains into user behavior, network activity, cloud usage, or third-party risk.

Despite the massive user base and attack surface, NCG had just one dedicated security lead. With outdated policies, three separate backup systems, and no unified detection or response capability, the workload was overwhelming and investigations into potential threats could take weeks.

With increasing mandates for the education sector to achieve specific certifications and comply with frameworks, the UK government-backed Cyber Essentials certification became a mandate for the education sector. Bringing NCG's policies and procedures up to speed to align with NIST and the ISO frameworks, pass yearly audits, gain Cyber Essentials certification, and meet insurer requirements would require significant improvements.

A mission too important to jeopardize

NCG exists to "enable social mobility and economic prosperity through exceptional education. Every outage, every compromise, every delayed recovery has real-world impact on students' futures. We only need one compromised account to bring us down," Weeks says.

To protect NCG's learners and operations, Weeks and his team began a comprehensive effort to strengthen the group's cyber posture and prepare for the future.

"It was a revelation. Darktrace's ability to interrupt threats at machine speed, even when our team wasn't watching, immediately addressed our staffing challenge."

■ Chris Weeks

Director of Information and Data Services,
NCG

An AI-powered foundation for visibility and trust

After evaluating several solutions, Weeks says the Darktrace ActiveAI Security Platform™ stood out as the clear winner. "With our staffing resource, we needed a solution with autonomous capabilities. Darktrace was leaps ahead of everything else when it came to AI. No other solution could deliver the same level of value and functionality."

A proof of value that changed everything

During the extended proof of value – a necessity given public-sector procurement rules – Weeks and the team saw immediate outcomes.

For the first time, they could see activity across all campuses, all users, and all systems within a single location. What had once been siloed became unified. "Darktrace showed us things we simply didn't know existed," says Weeks, surfacing suspicious behavior such as strange login patterns, malicious downloads, attempts to bypass firewalls, and external compromised accounts trying to reach NCG colleagues.

The promise of autonomous detection and response wasn't theoretical. Cases that once required days or weeks of manual investigation were now analyzed in seconds by the Darktrace AI autonomous engine, complete with natural-language reports.

"It was a revelation," Weeks says. "Darktrace's ability to interrupt threats at machine speed, even when our team wasn't watching, immediately addressed our staffing challenge."

A seamless implementation that built confidence

The Darktrace rollout could not have gone better, shares Weeks. "The deployment was seamless. No blocked learners, no disabled accounts, no complaints. It just worked and it made us look brilliant."

Creating a cyber-aware culture beyond IT

Darktrace has enabled a more engaged, more confident workforce. "It's created development pathways we never had before," says Weeks. "Instead of ignoring suspicious emails or flooding IT with questions, employees began clicking Darktrace's analysis button to validate messages in real time. "Outside IT, it's one of the most powerful tools we've got."

Resilience, clarity, and a new sense of control

AI slashes threats – and analyst overload

Darktrace's Self-Learning AI now manages most of the tedious manual work required to identify, investigate, and responds to threats, freeing NCG's analysts to focus on solving other problems and genuine incidents instead of sifting through endless alerts.

Within one month alone, Darktrace Cyber AI Analyst™ autonomously investigated 20,940 potential incidents, resolving 97% of those events on its own and only sending 3% to security analysts for further investigation. The impact was enormous, saving the security team 15,835 investigation hours within a single month.

If analysts do need to triage an incident themselves, all the information they need is at their fingertips: what occurred, why it happened, and precisely what steps to take to neutralize the threat. "Prior to Darktrace, it could take weeks to get access to all the information we needed to properly investigate the nature of an incident. Now it's minutes, sometimes seconds," Weeks says.

Stopping attacks before they reach staff

Voucher scams. Executive impersonation emails. Compromised vendor accounts. "They just don't get through anymore," Weeks says. "Seeing them blocked before they even reach the inbox is incredibly satisfying." In one case, a long-trusted supplier's account was compromised, and Darktrace flagged it instantly, preventing a potentially damaging breach and allowing NCG to notify the partner.

"With Darktrace we have the visibility to deeply analyze every facet of the audit, allowing us to make more informed, strategic decisions in conjunction with our auditors."

■ Chris Weeks

Director of Information and Data Services,
NCG

Reducing student-driven threats

NCG's learners are digitally savvy, and occasionally mischievous. Darktrace / NETWORK™ provided immediate insight into attempts to:

- Access the dark web
- Download malicious tools
- Circumvent firewalls and proxies
- Misuse credentials

"We can now see when users are accessing the dark web or downloading malicious files and show curriculum staff exactly why our user base operates on the Principle of Least Privilege, further helping to reduce our risk." This visibility enabled NCG to refine Active Directory group policies, adjust firewall rules, and create safe flexibility for certain curriculum areas when needed.

Securing board-level support and funding

Weeks began presenting monthly Darktrace reports directly to the Executive team and external board members. "The engagement was unbelievable," he says. "The evidence Darktrace provided allowed our Executive team to understand what was happening and why it mattered. Visualising blast radius containment and showing the Darktrace dashboard resonated in a way traditional reports never had."

Darktrace's visibility uncovered ransomware remnants on legacy servers at a newly merged college – something no one knew existed and of which were present before Darktrace was deployed. "Without Darktrace, we would never have uncovered the ransomware files sitting on that old server," shares Weeks. This discovery helped his team secure investment for a new back-up platform, improved disaster recovery testing, and broader resilience initiatives. "It allowed us to show precisely why we needed change," Weeks says.



Powering Cyber Essentials certification and effortless audits

When the UK National Security Center mandated Cyber Essentials accreditation within the education sector, Weeks says Darktrace was instrumental in demonstrating NCG meets the criteria. "We sailed through, in large part due to the capabilities of Darktrace."

Once a stressful process, Weeks says audits are now opportunities to engage in more strategic priorities thanks to Darktrace taking care of so many procedural and technical requirements.

"With Darktrace we have the visibility to deeply analyze every facet of the audit, allowing us to make more informed, strategic decisions in conjunction with our auditors," explains Weeks. "I've looked at the scope for our next audit, and it's a delight. Darktrace covers so many of the elements we'll be asked to demonstrate."

A simple, scalable model for future growth

When NCG launched a new 40,000-square-foot higher education site in Canary Wharf, Weeks says, "Darktrace was the easiest part of the process. The hardware arrived within days. Knowing that we can spin up new sites and have Darktrace ready instantly is incredibly empowering."

Delivering peace of mind – on and off the clock

The human impact of using Darktrace has been profound, particularly for Weeks and his security team. "Whether we're on holiday, sleeping, or focused on other work, we know that Darktrace has our backs."

Before Darktrace, any time Weeks stepped away, he worried that a threat might be unfolding and go unnoticed. Today, that anxiety is gone. "I can be on annual leave in the Highlands of Scotland, get off the motorbike for a coffee, check my phone, and instantly know there's been an incident, that Darktrace has already handled it, and that my team is discussing it. That peace of mind is everything."

Scaling AI confidence across the group

NCG's transformation is ongoing, and Darktrace is now central to its long-term strategy. As NCG grows its higher education footprint, Darktrace will secure new locations from day one.

Greater proactive defense

Darktrace's Self-Learning AI is enabling NCG to shift from reacting to threats to hardening its environment proactively. As AI takes on triage and early-stage investigation, Weeks's team is free to focus on forward-looking initiatives: identity modernisation, policy improvements, smart segmentation, and more.

Extending protection across a growing partner network

Because Darktrace gives NCG deep insight into compromised third-party accounts, the organisation is now a quiet guardian in its wider ecosystem, notifying partners when their security falters. "It's more than a safety net. It lets us help our partners before the damage spreads."

For Weeks and his team, the transformation isn't just measured in metrics – it's felt in the way they show up each day: informed, prepared, and no longer carrying the weight of the unknown. "Darktrace has changed how we work, how we think, how we make decisions. It's given us real confidence that we're ready for whatever comes next."



■ 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.