A CPP PERSPECTIVE

STOP LOOKING IN THE REARVIEW MIRROR: DARKTRACE BRINGS THREATS INTO FULL VIEW

By Michael Haydanek, CPP Account Executive

Cyber threats today don't knock on the front door—they slip through the back. While legacy tools still chase known signatures and predefined rules, today's adversaries are using AI, living-off-the-land (LOTL) techniques, and insider access to quietly breach, move laterally, and exfiltrate data. To stay protected, organizations need more than prevention—they need **continuous, adaptive detection powered** by machine learning.

This is exactly where **Darktrace** is leading the charge, redefining what real-time cybersecurity looks like.

THE LIMITATIONS OF TRADITIONAL SECURITY: WHY REACTIVE ISN'T ENOUGH

For decades, organizations have depended on a mix of firewalls, endpoint protection, and SIEM tools to defend against cyberattacks. But today's threats don't follow old playbooks. From credential stuffing to ransomware payloads hidden in encrypted traffic, the bad actors are faster, smarter, and far more agile.

Most breaches today aren't a failure of tooling—they're a failure of **detection**. Static defenses don't adapt to changes in behavior. That's why **Darktrace's Self-Learning AI** is so critical: it doesn't need to know what the threat is—it only needs to know what looks different from your organization's "normal."

With legacy tools, you're spotting threats in the **rearview mirror**—after the damage has been done. With Darktrace, you're watching through the **windshield**, with proactive anomaly detection that sees danger as it unfolds.

DARKTRACE: AI THAT UNDERSTANDS YOUR BUSINESS, NOT JUST YOUR NETWORK

Darktrace is fundamentally different. It builds a constantly evolving model of your unique environment—users, endpoints, cloud workloads, SaaS platforms, and even storage—and uses anomaly detection to identify threats **as they unfold**, not after damage is done.

> *The autonomous response from Darktrace Antigena doesn't just reduce risk. It redefines response time, shrinks the blast radius of attacks, and gives your team confidence that threats are handled—even while they sleep.*

Whether it's:

- A user accessing finance systems outside of typical hours
- A device communicating with a rare domain
- A backup system showing signs of unauthorized data movement

Darktrace recognizes the anomaly and automatically responds—quarantining users, pausing connections, or alerting SOC teams **before a breach escalates**.

REAL-TIME DETECTION WITH AUTONOMOUS REMEDIATION

Detection is only half the battle—what matters is how fast you can act. That's where **Darktrace Antigena** takes over. When a threat is detected, Antigena **automatically initiates remediation** steps to contain and neutralize the risk without waiting for human intervention.

Whether it's:

- Blocking a connection to a suspicious domain
- Slowing down or isolating a compromised device
- Pausing access to sensitive data for anomalous users

Darktrace Antigena responds in seconds, stopping threats before they can spread—**even during off-hours or without analyst input**.

This kind of autonomous response doesn't just reduce risk. It redefines **response time**, shrinks the blast radius of attacks, and gives your team confidence that threats are handled—even while they sleep.

INTELLIGENT DETECTION MEETS INTELLIGENT STORAGE: THE ROLE OF HPE ALLETRA MP

Cybersecurity doesn't stop at the endpoint or firewall. Increasingly, attackers target **critical infrastructure**—especially storage.

That's why some of the smartest security teams pair Darktrace with **HPE Alletra MP**, a next-gen storage platform with built-in analytics and real-time observability. When Darktrace detects unusual access patterns or suspicious east-west movement, Alletra MP provides the context: **who accessed what, when, and how much data was touched**.

Together, they close the loop between **detection and root cause**, reducing response times and preventing repeat incidents.

REDUCE SIEM NOISE: RECLAIM YOUR BUDGET

With Darktrace acting as your first line of detection, many organizations reduce the load on traditional SIEM tools—saving on log ingestion, license fees, and engineering hours. For environments flooded with low-value alerts, Darktrace often replaces multiple siloed tools by:

- Detecting and scoring anomalies in real time
- Automating early-stage incident response
- Enabling leaner, more effective SOC operations

Add in the intelligence from HPE Alletra MP, and you're able to **detect, diagnose, and respond faster—with fewer tools and less overhead**.

REAL-WORLD IMPACT: WHAT OUR CLIENTS ARE SEEING

Organizations that implement Darktrace and HPE Alletra MP report:

- 95% reduction in false positives
- Faster triage and incident response times
- Increased confidence in their SOC decisions
- Significant cost reductions in SIEM and legacy tool licensing

WHY WORK WITH CPP ASSOCIATES?

At CPP Associates, we don't just deploy tools—we build smart, integrated cybersecurity strategies. Our clients leverage **Darktrace and HPE Alletra MP** together to gain **true visibility, proactive protection, and resilient infrastructure**—without adding unnecessary complexity.

Ready to stop looking in the rearview mirror and start focusing on what's ahead? Let's have a conversation about how we can strengthen your security posture—starting today.

ABOUT CPP ASSOCIATES

Founded in 2008, CPP Associates is an award-winning IT Solution Provider serving mid- to enterprise sized organizations throughout the U.S. Northeast region. Our solution portfolio includes the most urgent technology needs today, including ***Cloud Optimization****,* ***Intelligent Automation*** *(Front Office/Back Office),* ***Modern Infrastructure****,* ***Cyber Protection and Recovery****, and* ***Managed IT Services****.*

With a 2:1 ratio of engineers to sales staff (the reverse of what is typical in the industry), we lead with technical acumen, a stringent analytical focus, and a vendor-agnostic perspective. With the highest level certifications and strong, long-standing relationships with the leading IT manufacturers – such as ***Hewlett Packard Enterprise****,* ***Microsoft****,* ***Fortinet****,* ***Palo Alto Networks****,* ***Morpheus, Automation Anywhere,*** *and* ***Arctic Wolf*** *– we provide our customers with unparalleled expertise and "concierge-level" consulting and support 24/7/365.*

Our proprietary ***"Infrastructure Anywhere Assessment"*** *factors in more than 100 variables to determine the ideal approach for our clients to deploy "cloud-like" infrastructure to maximize agility with increased utilization while at the same time, meeting demanding business requirements with a focus on technology, service level, security, and costs. Keeping with our philosophy that "****high tech without high touch"*** *will ultimately fail, we are proud of the powerful human connection we establish with our clients which leverages the synergies of trust and respect and drives our respective success.*

cpp
Infrastructure. Anywhere.

CPP Associates, Inc
6 Route 173
Clinton, NJ 08809, USA
866-277-4621
www.cppassociates.com