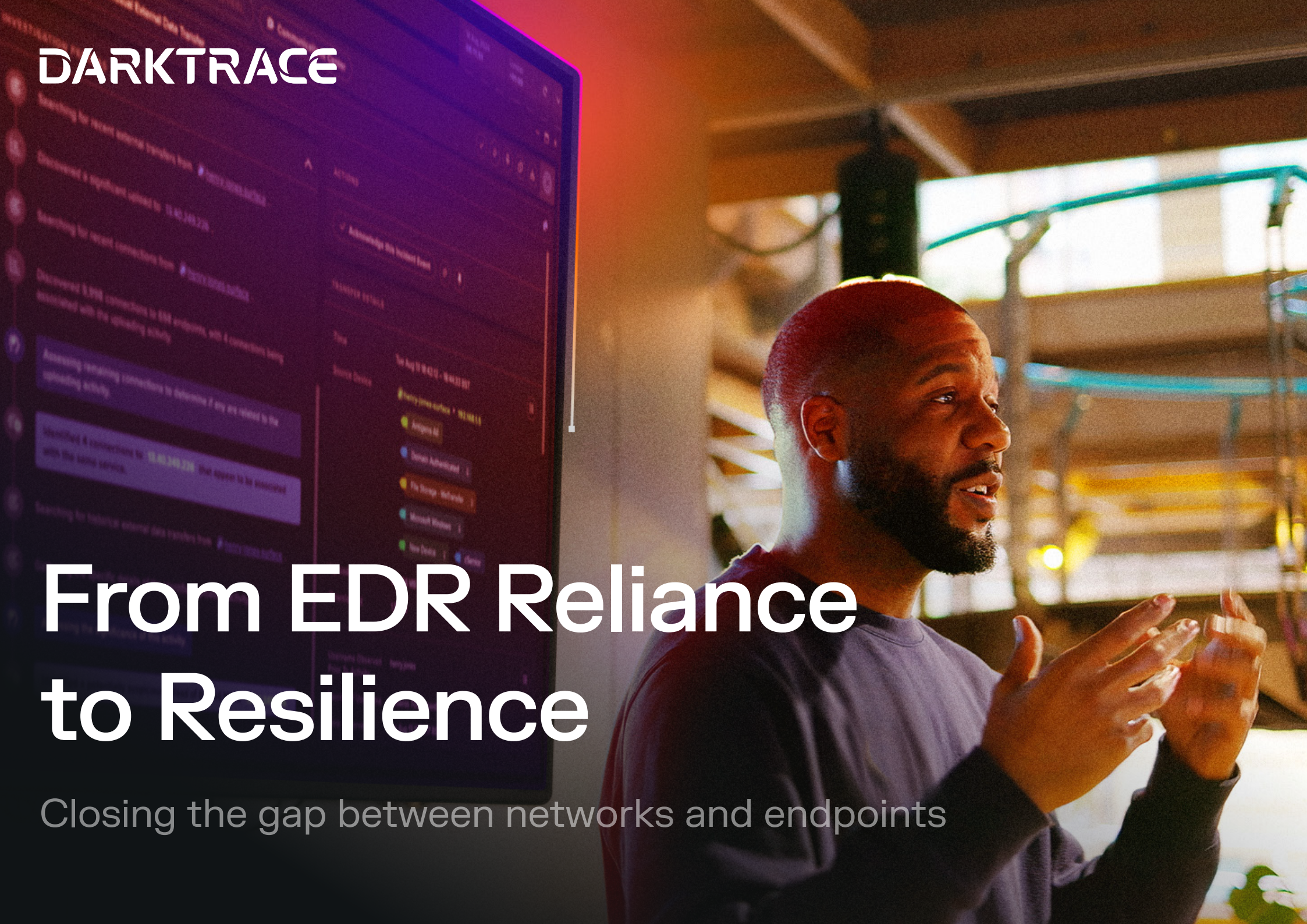
DARKTRACE



From EDR Reliance to Resilience

Closing the gap between networks and endpoints

At a glance

EDR and XDR are essential, but they were never designed to defend against the full scope of modern, multi-domain threats. Attackers exploit seams between endpoints, networks, cloud services, and OT environments — the very places where visibility fades and point solutions struggle to connect the dots.

This e-book is about rethinking how organizations build resilience. It explores why endpoint-centric defenses alone cannot keep up, and how unifying endpoint process data with network telemetry creates a stronger foundation for threat detection, investigation, and response. Along the way, we'll highlight examples of attacks that bypassed endpoint tools, the strain these gaps place on SOC teams, and the path forward with mixed telemetry.

EDR/XDR is necessary but incomplete
These tools protect endpoints well, but lack visibility across unmanaged devices, agentless environments, and network-based attacks.

Mixed telemetry closes investigation gaps
By combining network activity with endpoint process data, analysts gain a unified view that reduces false positives, accelerates triage, and contains threats earlier.

Resilience requires a new SOC foundation
Self-learning, adaptive platforms anchored in network visibility provide the context and efficiency needed to reduce analyst burnout, cut MTTR, and cover blind spots across domains.

Why EDR is necessary but not complete

Most enterprises today have invested in Endpoint Detection and Response (EDR) or its more recent evolution, Extended Detection and Response (XDR).

EDR is **purpose-built** for the endpoint. It monitors host-level processes, memory, and logs, and it enables containment and remediation at the device level.

XDR emerged from EDR vendors to attempt to **solve the sprawl problem** by correlating alerts from multiple security tools into a single platform. But in practice, most XDR offerings remain EDR-centric. They extend visibility outward but are still anchored from an endpoint agent.

57% of organizations are planning on adding Network Detection and Response (NDR) capabilities to their XDR toolset

Gartner, 2023

Coverage gaps

When detection is anchored in endpoint telemetry, blind spots persist across networks, unmanaged devices, cloud workloads, and identity systems. EDR-centric XDR can't see lateral movement or activity in agentless environments like OT, leaving critical infrastructure uncovered.

Fragmented response

Most NDR tools lack endpoint context, forcing analysts to pivot between consoles to piece together an attack. This manual effort slows investigations, increases MTTR, and leaves threats that move between endpoints and networks undetected.

EDR is focused on...

'Known bad' threats, this means they will only create an alert once activity on the endpoint matches that 'known' criteria or pre-defined rule/signature.

EDR doesn't understand...

What is normal or abnormal for a host; it follows the rules based on known attacker behavior. This is fine for threats that we already know about, but it leaves gaps in coverage for threats that have never been seen before, or from attacks that exploit legitimate tools to hide in plain sight.

The result...

Ransomware, data exfiltration, and multi-stage campaigns succeed despite strong endpoint coverage. EDR remains highly effective at monitoring host activity, but modern adversaries don't confine themselves to endpoints; they exploit the seams between domains, where visibility fades and analysts struggle to connect the dots.

Proof points
Where EDR visibility ends

EDR evasion with agent-killers

Attackers use tools like EDRKillShifter and EDRSilencer to disable endpoint agents, instantly blinding endpoint-only defenses. These tactics show how easily adversaries can neutralize agent-based security, regardless of sophistication.

CISA's red team lessons

A CISA assessment of U.S. critical infrastructure found that overreliance on EDR left critical gaps at the network layer. Adversaries maintained persistence for months without triggering host-based alerts, proof that isolated visibility isn't enough.

Zero-day exploitation in the network layer

During the 2024 Ivanti Connect Secure exploitation, network telemetry detected anomalies 11 days before public disclosure, revealing credential misuse and C2 activity invisible to endpoint tools. NDR provided the visibility needed to contain the threat early.

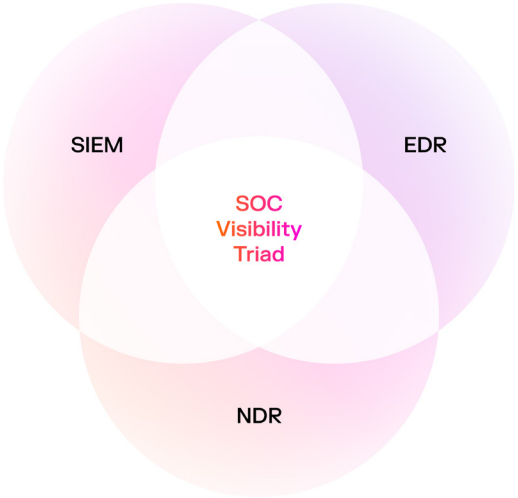
Building a resilient defense

EDR is foundational but only when connected to full network visibility does it become part of a complete, resilient security architecture. Even XDR solutions, while broader in scope, still rely heavily on host-based monitoring and often lack native network visibility.

Unified visibility across endpoints, networks, cloud, OT, and identities.

Integrated telemetry from both managed and unmanaged assets.

Adaptive systems that understand normal behavior and detect the unknown.



Bypassing EDR
Post-exploitation activities of Ivanti CS/PS appliances

Attack example

This Ivanti campaign shows that attackers know where endpoint visibility ends. They exploit unmanaged network assets, move laterally, and hide in encrypted traffic. But for defenders, the real challenge doesn't stop with detection - it lands on the people in the SOC who must make sense of it all.

Initial beaconing to rare external IP observed. Endpoint agents weren't in play here, as the compromised Ivanti appliance is a network asset, not a traditional endpoint. Only network visibility exposed the early anomaly.

Secondary beaconing to another unusual host detected. Adversaries expanded footholds through the network layer. With no agent coverage, EDR tools would have had nothing to correlate against.

Exploit validation activity using OAST services identified. Attackers confirmed exploitation using out-of-band channels. These checks never touched the endpoint stack, highlighting why network telemetry is critical.

Large POST transfers of .dat/.sys files to an external server revealed host data exfiltration. Sensitive system files were exfiltrated over the network. Endpointtools monitoring host processes couldn't see this outbound traffic.

Malicious Rust ELF payloads delivered from AWS S3 endpoints. Payload delivery leveraged a cloud service. Even if EDR was present elsewhere, these implants bypassed host-based defenses by entering through the network edge.

Web shells and JavaScript stealers deployed to harvest credentials. Credential theft activity unfolded in a network appliance context, not a user endpoint. This means identity compromise originated outside EDR visibility.

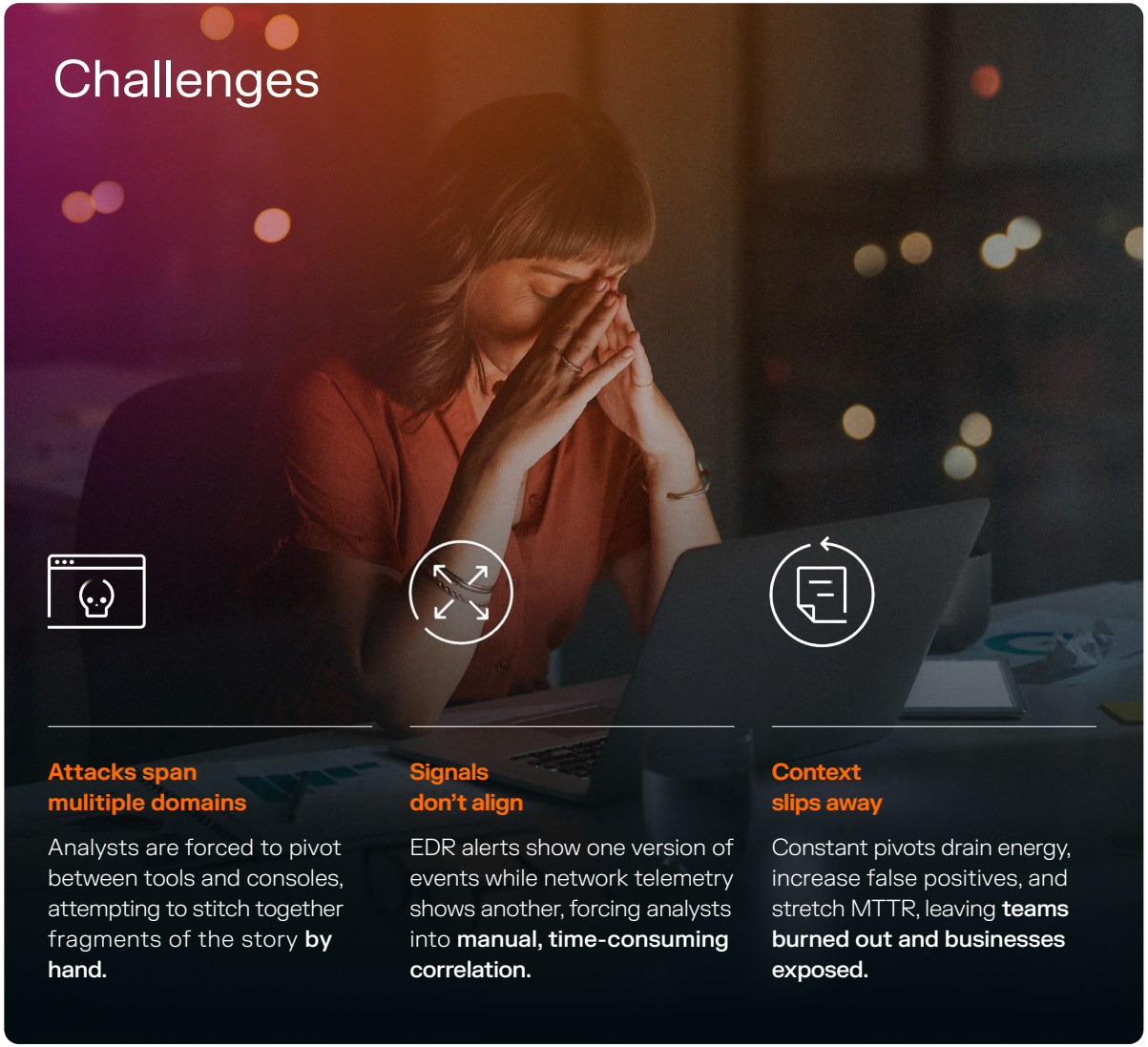
Network scanning and lateral movement observed inside the environment. Classic example of unmanaged assets being traversed by an attacker. EDR cannot instrument these devices, leaving analysts blind without NDR.

Encrypted command-and-control traffic tunneled over DNS, followed by cryptominer delivery. Covert network channels allowed persistence. Endpoint-based monitoring cannot reliably spot encrypted DNS misuse - this requires anomaly detection at the network layer.

Network telemetry surfaced these anomalies days before public disclosure of the vulnerabilities. Detection arrived not from signatures or endpoint logs, but from behavioral anomalies in network traffic, showing why multi-domain coverage is necessary.

The breaking point for the SOC

Blind spots, burnout, and business risk



Beyond visibility

Attacker-centric detection methods struggle to detect novel threats because they rely on static rules and historical attack data, focusing on identifying 'known bad'. These tools often miss malicious activity that looks legitimate on the surface like:

- Living off the Land (LotL)
- Abuse of valid credentials
- Insider threats
- Authorized third-party applications

More complexity = more problems

In OT environments most vendors focus on asset visibility or rule-based detection, without modeling how attackers can traverse from IT to OT, exploit exposed CVEs, or disrupt critical operations through misconfigured segmentation.

Without true convergence modeling, defenders are left with siloed views and incomplete threat coverage.

The solution
Building resilience with mixed telemetry

The solution to these challenges involves bringing together the lowest level of endpoint process data and network telemetry into a single stream. By fusing these data sources at the collection point:

Faster investigations
unify endpoint process data and network activity to accelerate analysis.

Single view of incidents
trace process activity and lateral movement without stitching together fragments from multiple tools.

Improved outcomes
reduce false positives, shorten triage cycles, and strengthen containment.

Importantly, this capability **does not replace** existing EDR or XDR investments - it augments them. Endpoint defenses remain foundational, but when paired with network-level insight, their coverage extends across unmanaged devices, cloud workloads, and encrypted traffic.

The result is a security stack that reflects the reality of modern threats rather than the limits of endpoint-centric visibility.

Rethinking the SOC foundation

To move beyond piecemeal defenses, security teams need a foundation that can anchor the entire SOC. That foundation is the network. Every endpoint, cloud workload, OT device, and identity ultimately leaves its trace in network traffic. By treating the network as "home base," organizations gain a common lens through which every other domain can be understood.

This foundation doesn't mean one-size-fits-all. Every organization has a unique digital estate a different mix of cloud services, legacy infrastructure, remote endpoints, and OT environments. Static, pre-defined detections can't anticipate every novel attack path or configuration drift. What's needed is adaptability: a system that can learn the normal patterns of your environment, evolve with it, and highlight anomalies as they emerge.

Building on network visibility as the anchor, a unified platform brings critical benefits:

Adaptability through continuous self-learning, even as environments and threats change.

Efficiency by consolidating detection and response across domains, reducing vendor sprawl.

Resilience by correlating telemetry in real-time, cutting through noise, and surfacing the incidents that matter.

Why Darktrace?

Darktrace is an industry recognized leader in NDR because of its Self-Learning AI ™ that understands normal for your entire network, intelligently detecting anomalies and containing sophisticated threats without historical attack data.

This approach, based on advanced, unsupervised machine learning, enables Darktrace to catch novel, unknown, and insider threats that traditional tools miss, and other vendors can't detect.

As attacks now span email, cloud, OT, SaaS, and endpoints, Darktrace has taken a major step forward: unifying telemetry and context across these domains and applying AI-driven investigation at scale. By combining process-level endpoint data with network visibility, Darktrace enables security teams to see the full attack lifecycle and act on it autonomously, reducing blind spots, investigation time, and analyst burden.

"Darktrace isn't just technology. It's a tool for **building trust whilst justifying and supporting smart growth** across our System and Cybersecurity landscape.

- **CIO**
  Government Services

Check out

Darktrace / Endpoint Solution Brief

Download brief ↗

Get a demo

See what Darktrace finds in your environment

Book a demo ↗