

# How Darktrace Works Alongside Zero Trust

## At a Glance

- ✓ Complements, enhances, and interoperates with zero trust architecture
- ✓ Illuminates and interrupts novel attacks and insider threats that operate over legitimate paths or evade policy-based defenses
- ✓ Natively integrates with IAM tools, Web Gateways, and firewalls
- ✓ Validates zero trust policies and identifies opportunities for microsegmentation via real-time visibility and continuous monitoring

## The Adoption of Zero Trust Architecture

The 'zero trust' model of security has become an increasingly popular framework for organizations seeking to protect their environments amid digital transformation efforts and new ways of working.

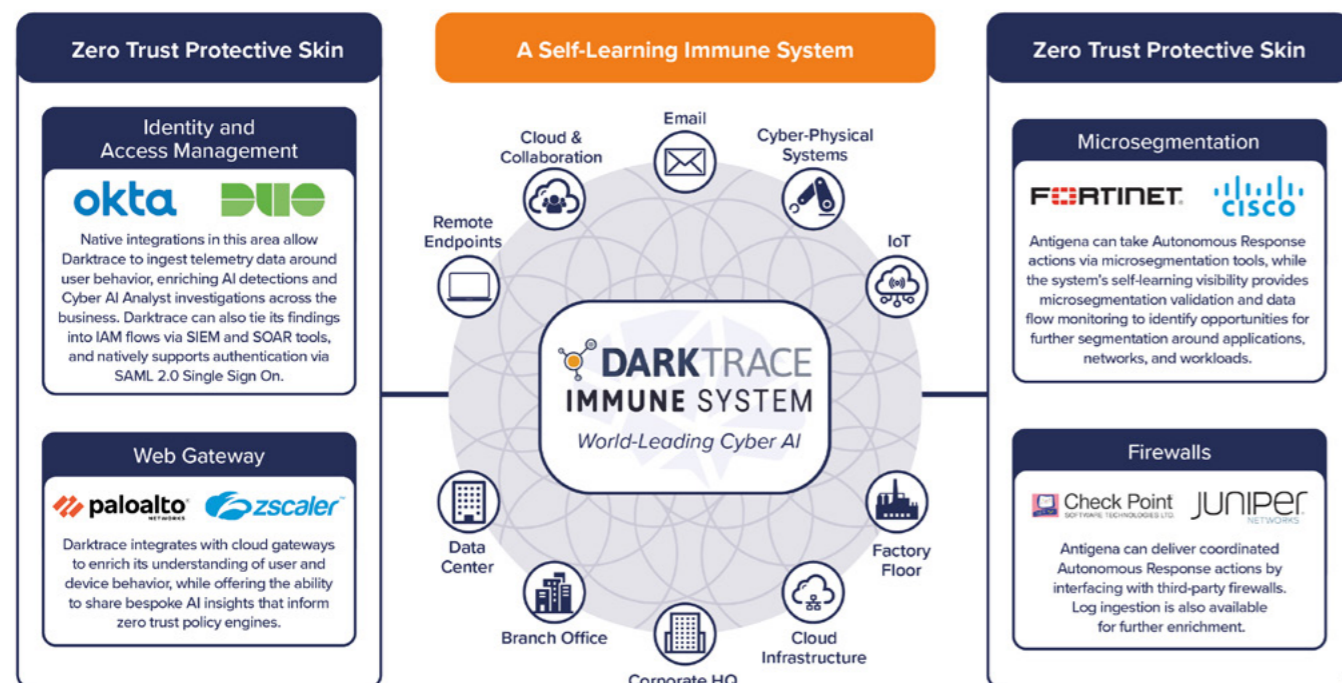
The concept of 'zero trust' replacing the implicit trust of the legacy device model with a more dynamic approach that assumes breach and verifies intelligently, while restricting access and operations accordingly.

In practice, this is typically implemented in the form of security policies, whether via microsegmentation, Web Gateways, or least-privilege access control. It is often associated with the Secure Access Service Edge (SASE), SD-WAN, and other security and networking services designed to accommodate the new shape of digital business.

## Darktrace and Zero Trust

Darktrace complements and enhances zero trust postures with self-learning AI that identifies, interrupts, and investigates unpredictable cyber-threats that get through, even if they operate over legitimate paths. This includes advanced external attacks like ransomware, zero-days, and supply chain risks, as well as compromised, careless, or malicious insiders with privileged access.

Darktrace interoperates with zero trust technologies via native integrations, while validating current zero trust policies and informing future microsegmentation efforts with continuous, real-time visibility across the entire organization.



# How Darktrace Works Alongside Zero Trust

## How Darktrace Complements Zero Trust Policies

While the security policies implemented as part of a zero trust framework can help prevent predictable attacks, they remain too static to catch the unknown and unpredictable threats that inevitably get through.

By learning normal 'patterns of life' from scratch, Darktrace 'assumes breach' as well, yet with an adaptive self-learning approach that allows the system to detect, investigate, and respond to unforeseeable cyber-threats that evade zero trust policies, from novel external attacks to insider threats.

Without pre-defining 'benign' or 'malicious', Darktrace AI learns an evolving sense of 'self' bespoke to each organization it safeguards, continually revising its understanding in light of new evidence across cloud, email, endpoints, and the corporate network. This enables the system to spot subtle deviations and novel threats, deliver Autonomous Response actions to interrupt attacks with surgical precision, and investigate and report on the full scope of security incidents.

The zero trust model represents a critical part of any dynamic security strategy today. It is critical that Darktrace can complement, enhance, and natively interoperate with a zero trust architecture. While this architecture aims to deliver a pre-programmed measure of secure connectivity, the Darktrace complements zero trust by delivering real-time visibility and adaptive AI defense in the following ways:

- AI detections, complete visibility, and continuous monitoring
- Autonomous Response
- Autonomous investigations



# How Darktrace Works Alongside Zero Trust

## AI Detections, Complete Visibility, and Continuous Monitoring

Darktrace provides deep visibility into all user and machine activity down to the packet layer, enabling a full assessment of the data environment and architecture to autonomously discover resident threats or malicious activities flowing over legitimate paths. This delivers unified and adaptive protection across heterogeneous, hybrid, and service-based microsegmentation architectures, including across email, cloud, and collaboration platforms, as well as remote endpoints, IoT, ICS, and the corporate network.

When organizations combine a robust zero trust architecture with Darktrace's self-learning AI, attackers have nowhere to hide. Zero trust policies furnish the protective skin that prevents low-hanging fruit from gaining a foothold, while Darktrace illuminates behavior across the entire organization to spot unpredictable threats that get through.

This ensures that your defenses will identify every threat – even if they leverage trusted paths or credentials – while providing a critical feedback loop between Darktrace's adaptive understanding and zero trust policies in place. By providing unified visibility that adapts to the business as it evolves, Darktrace can validate zero trust policies, inform future microsegmentation efforts, and incorporate telemetry from IAM tools and Web Gateways into a broader understanding of the organization.

**“Detecting anomalies and enabling response requires visibility to the entirety of your data and the totality of your network. Darktrace not only focuses on threat detection but also on providing visibility into traffic flow within your environment.”**

Dr. Chase Cunningham, VP & Principal Analyst, Forrester, Mitigating Ransomware with Zero Trust

# How Darktrace Works Alongside Zero Trust

## Antigena Autonomous Response

When Darktrace detects an emerging threat, Darktrace Antigena responds in seconds, interrupting the attack by enforcing 'normal' and sustaining standard working practices by design. Autonomous Response provides robust support for zero trust postures by neutralizing the full range of known and unknown threats, regardless of whether they've been contained by zero trust policies in place. The system can take action via surgical, self-directed actions, via native integrations with firewalls and network devices, and via an open API, in light of adaptive AI detections and even custom policies defined by the user.

Autonomous Response can be deployed to cover email and collaboration tools, delivering machine-speed protection of the dynamic workforce across corporate cloud services. This could mean leveraging Antigena to neutralize targeted email attacks in Gmail or Outlook, or instantly interrupting malicious user behavior in SharePoint, Teams, or Zoom.

## Autonomous Investigations

Darktrace not only detects and contains unpredictable cyber-threats, but also automatically investigates the full scope of security incidents with Cyber AI Analyst. Trained on expert human analyst behavior, Cyber AI Analyst automatically stitches together disparate security events into a single security incident. It then communicates its findings in the form of a concise, digestible narrative that can be instantly shared with relevant stakeholders in the organization or actioned elsewhere in the security workflow.

By adapting on the fly, the AI can quickly interpret and report on security incidents characterized by innovative attack techniques that would be impossible to capture with static playbooks. This adds an intelligent AI investigation layer that sits behind and across your zero trust architecture, continually probing and querying suspicious patterns even after validation of trusted accounts, workloads, devices, and networks. Suspicious behavior in Okta or Duo, for example, might trigger an autonomous investigation that incorporates real-time data across the organization.

**“For us, Darktrace is always set on auto pilot. It's autonomous – AI Analyst and Antigena just work as expected for high-risk incidents and we let it do its thing.”**

Syed Hussaini, Cyber Security Analyst, Metrixon Technology Group

