How Darktrace Works Alongside Zero Trust

At a Glance

The Darktrace Immune System:

- ✔ 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

okta DUO cisco paloalto NETWORKS zscaler FORTINET netskope

The Adoption of Zero Trust Architecture

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

This evolution in business dynamics has gradually inverted the traditional model of the network security perimeter, shifting the focus away from the data center to an emphasis on 'identity' and enabling secure, distributed access – anywhere, anytime, and from any device. Zero trust architecture has emerged as one way of supporting this shift, 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.

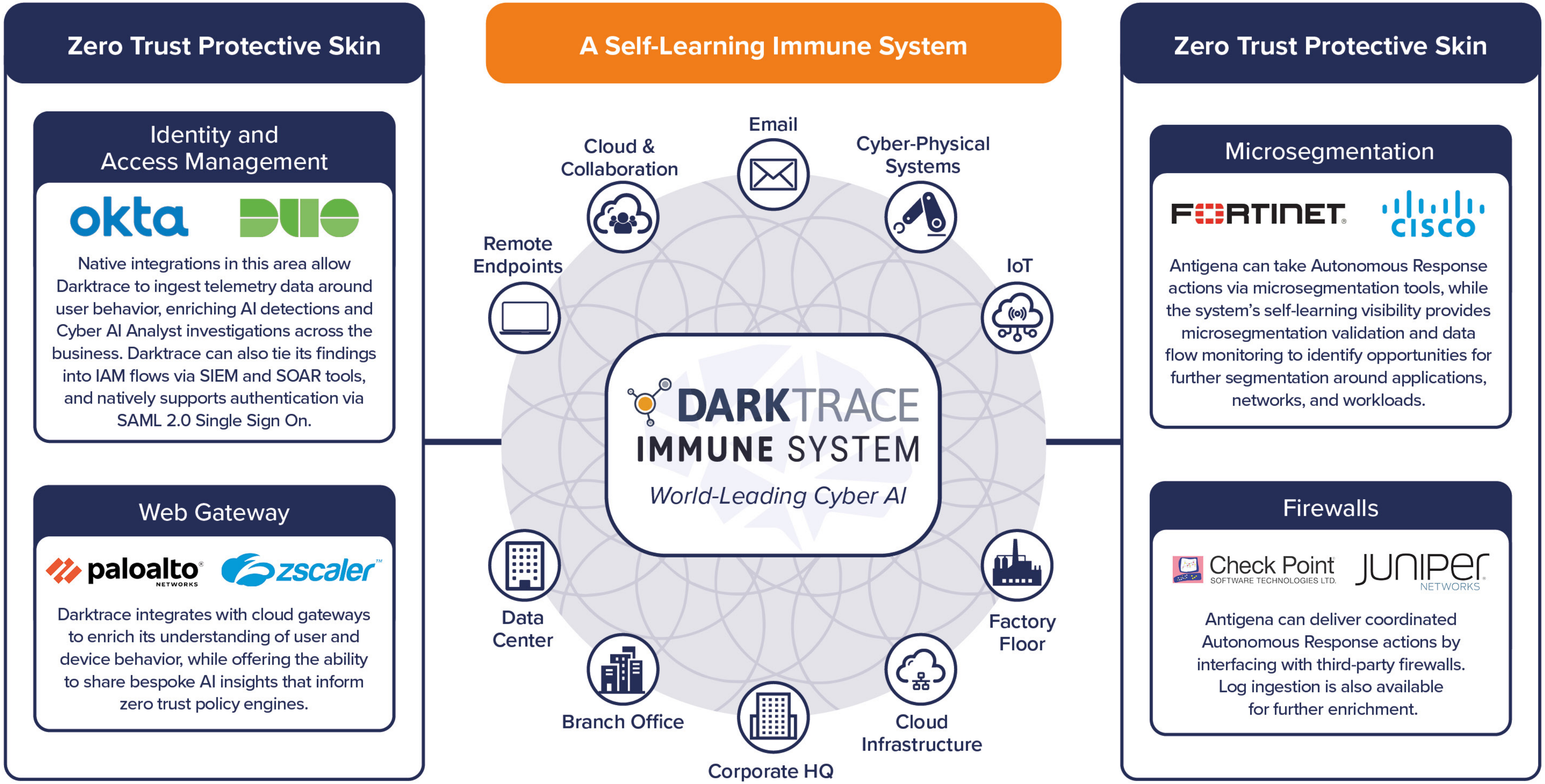
In practice, the zero trust model is typically implemented in the form of security policies, whether via microsegmentation, Web Gateways, or least-privilege access control. In this connection, it is often associated with the Secure Access Service Edge (SASE), SD-WAN, and other security and networking services designed to accommodate the new shape of digital business. While particular implementations will vary, the zero trust model generally uses these services as a coordinated mechanism that allows the minimum access required to accomplish business objectives.

Darktrace and Zero Trust

The Darktrace Immune System 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. Crucially, this continuous monitoring is adaptive in its understanding and pervasive in its scope, delineating normal and abnormal patterns across email, cloud, and collaboration platforms, as well as remote endpoints, IoT, and the corporate network.

By deploying Darktrace alongside a robust zero trust architecture, organizations benefit from a layered security strategy that combines a protective posture of 'default deny' with autonomous smart systems that adapt as the business and workforce evolve, leaving attackers with nowhere to hide.



Zero Trust Protective Skin

Identity and Access Management

Native integrations in this area allow Darktrace to ingest telemetry data around user behavior, enriching AI detections and Cyber AI Analyst investigations across the business. Darktrace can also tie its findings into IAM flows via SIEM and SOAR tools, and natively supports authentication via SAML 2.0 Single Sign On.

Web Gateway

Darktrace integrates with cloud gateways to enrich its understanding of user and device behavior, while offering the ability to share bespoke AI insights that inform zero trust policy engines.

A Self-Learning Immune System

Zero Trust Protective Skin

Microsegmentation

Antigena can take Autonomous Response actions via microsegmentation tools, while the system's self-learning visibility provides microsegmentation validation and data flow monitoring to identify opportunities for further segmentation around applications, networks, and workloads.

Firewalls

Antigena can deliver coordinated Autonomous Response actions by interfacing with third-party firewalls. Log ingestion is also available for further enrichment.

Zero trust is a useful security model designed to protect distributed networks via access policies and a coordinated posture of default deny. As such, it represents the most recent manifestation of an organization's 'protective skin' for attacks that can be identified by policy-driven detection mechanisms. This complements and interoperates with Darktrace's self-learning Immune System that detects and responds to unpredictable threats that get through.

The Darktrace Immune System: Complementing and Enhancing Zero Trust

The Darktrace Immune System complements and enhances the value of zero trust architecture, which in this context serves as yet another manifestation of an organization's protective skin – albeit one that is better suited to today's more fluid working practices. This analogy means that while the security policies implemented as part of a zero trust framework can help prevent predictable attacks, they are far too static to catch the unknown and unpredictable threats that inevitably get through.

By learning normal 'patterns of life' from scratch, the Darktrace Immune System '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 Cyber 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.

This characterization of zero trust as a predominantly preventative approach brings out another important feature and notable limitation of models that focus on trust rather than normal 'patterns of life' – namely, their binary nature. As Neil MacDonald, VP Distinguished Analyst at Gartner, puts the point: "Inevitably trust needs to be extended for the work of digital business and government to get done." Paradoxically, MacDonald suggests, a zero trust model will need to assume trust at some point. An immune system approach, by contrast, is always learning and delineating normal and abnormal patterns of behavior – regardless of whether a user has been granted access or an application has been permitted to run.

HoldingsInc File Transfer GH01 · 92:d1:15:d1:f8:d1
Fri Jan 22 2021 / 22:31:34
5 minutes
source
1 Anomalous Connection / Suspicious Self-Signed SSL
1 Anomalous Connection / Repeated Rare External SSL Self-
1 Compromise / SSL Beaconing to Rare Destination
1 SaaS / AWS / Unusual S3 Resource Modification
1 SaaS / Large Volume of Cloud File Downloads
2 SaaS / Unusual SaaS Sensitive File Access
3 Anomalous Connection / POST to IP Without Hostname
1 Anomalous Connection / Data Sent to Rare Domain
1 Unusual Activ Internal Data Transfer
DARKTRACE
Models, highest score
Filters
Last 7 days
Mon Jan 18, 14:33:00
Tue Jan 26, 14:28:00
All subnets
52
100

Yet, the zero trust model represents a critical part of any dynamic security strategy today, just as our own skin serves as a critical part of the human body's defenses against indiscriminate threats. It is equally critical, therefore, that the Darktrace Immune System 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 Immune System 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

AI Detections, Complete Visibility, and Continuous Monitoring

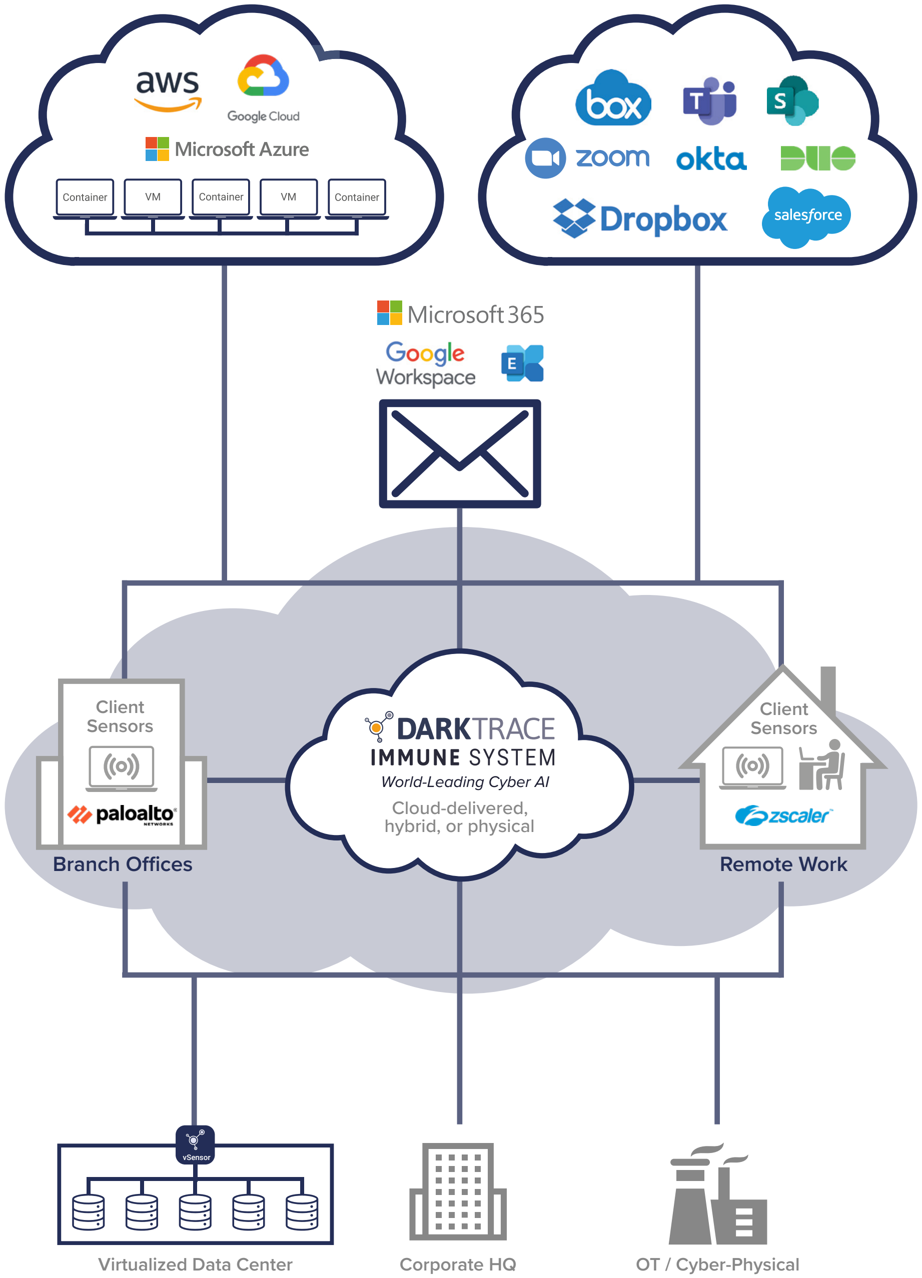
Darktrace provides deep visibility into all user and machine activity down to the packet layer, enabling a full assessment of the data environment and architecture to autonomously discover resident threats or malicious activities flowing over legitimate paths. This delivers unified and adaptive protection across heterogenous, 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; this can help you understand application dependencies and identify opportunities for microsegmentation before the attack."

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



Antigena Autonomous Response

When the Immune System 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

The Darktrace Immune System 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, Metricon Technology Group