Enterprise Immune System

The Enterprise Immune System harnesses scalable, self-learning AI to understand the digital DNA of an organization and illuminate unpredictable cyber-threats at an early stage. By learning the normal 'patterns of life' of every person and device in a business, the technology discovers novel attacks and insider threats that others miss, while delivering complete visibility across cloud and collaboration tools, remote endpoints, IoT, and the corporate network.

Key Benefits

- ✔ Learns normal 'on the job' to detect unknown and unpredictable cyber-threats
- ✔ Protects the dynamic workforce against zero-days, ransomware, and insider threats
- ✔ Covers the full digital DNA of an organization across cloud, endpoints, IoT, and network
- ✔ Interfaces with Cyber AI Analyst to trigger autonomous investigations at scale
- ✔ Interoperates with existing defenses via native, one-click integrations

Limitations of the Traditional Approach

The traditional approach to cyber defense manifests itself in many forms, from classic SIEMs and niche cloud-native defenses, to 'next-gen' platforms with bolted on machine learning and analytics. These tools serve an important function in any security strategy, operating as an organization's 'protective skin' for basic threats that can be identified by simple detection mechanisms.

Yet in every case, these technologies share the same design principles and limitations. Whether they rely on rules, policies, or historical attack data, they are far too static and retrospective to detect new and creative techniques. Equally, siloed point solutions create a complex and disjointed security stack, while failing to connect the dots on attackers who hide across systems or evade detection with legitimate credentials.

Protecting the Dynamic Workforce

Powered by self-learning AI, the Enterprise Immune System learns normal 'patterns of life' to protect against unknown and unpredictable cyber-threats. Unlike static and siloed defenses, self-learning AI is adaptive in its understanding and pervasive in its scope. This enables the system to identify the full range of cyber-threats that deviate from normal patterns, wherever they emerge in a business.

Darktrace's unique approach provides an especially critical form of protection for the dynamic workforce, which from a security perspective has become more distributed, agile, and unpredictable than ever. By extending the power of self-learning AI across the full digital DNA of an organization and its workforce, even the most subtle and persistent attacks have nowhere to hide.

Figure 1: Darktrace provides complete, self-learning protection across the digital business.

Self-Learning

The Enterprise Immune System relies on self-learning AI to understand the dynamic behaviors and relationships in an enterprise. This means learning 'normal' from scratch, without any prior assumptions, and adapting continuously as the business and workforce evolve. Self-learning protection of this kind enables the system to adapt to the inherent flux of digital business, while illuminating the earliest signs of a threat as it deviates from the multidimensional norm – whether the attack is known or unknown, internal or external, subtle or fast moving.

Pervasive

The dynamic workforce operates in a wide range of systems and services, from cloud and collaboration tools, to email, network, and remote endpoints distributed across far-flung corners of the globe. This diverse digital patchwork makes organizations easier to attack and even harder to defend. For this reason, self-learning AI must be pervasive and unified, ensuring protection extends to wherever employees operate and data lives. The Enterprise Immune System provides complete visibility of the dynamic workforce – no matter where they work or the nature of their applications.

Autonomous

The Enterprise Immune System operates autonomously, learning continuously without human input or intervention. By revising its understanding in light of new evidence, Darktrace can keep your business safe at the speed at which you wish to modernize, ensuring that any changes in working practices or internal systems are instantly incorporated into the AI's adaptive understanding of the environment. This autonomous design principle enhances human teams while attuning detections to real-world changes that manual processes inevitably miss.

Darktrace Cyber AI Analyst: Augmenting the Human

The Enterprise Immune System not only discovers unpredictable threats as they emerge, but also interfaces with Cyber AI Analyst to enable autonomous investigations at speed and scale. Trained on expert analyst behavior, Cyber AI Analyst automatically stitches together disparate security events into a digestible security narrative that can be instantly shared with the relevant stakeholders in your 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.

What Our Customers Say About Us

"Darktrace's ability to identify threats that go missed by other security tools is nothing short of ground-breaking. Armed with this AI platform, we are assured that we can move forward with our technology roadmap without compromising on security."

Nathan Hillery, CIO, Law In Order

"Darktrace truly aligns with our business risks and security needs. We've been able to expand coverage of our dispersed workforce and take advantage of an autonomous platform that really does the work for us."

Mark Herridge, CISO, Calligo

Use Cases for Self-Learning Cyber AI

Insider Threat and Account Takeover

Insider threat represents one of the more dangerous and common attack vectors in the enterprise. These originate from disgruntled, careless, or compromised employees who abuse their access to internal systems in varying degrees of severity and malice.

With self-learning AI, the Enterprise Immune System 'understands the dynamic human' behind corporate credentials, devices, and workloads, enabling the AI to identify when trusted accounts are being used carelessly or for more malicious purposes.

In one case, a recently terminated – and disgruntled – employee who had been working from home managed to retain trusted VPN access to critical servers. After being fired, they logged back in and sought to delete as many sensitive files as they could find. Darktrace immediately picked up on the subtly unusual activity and Cyber AI Analyst generated a full Incident Report before they could do damage.

Attacks on Cloud, IoT, and Collaboration Tools

Today, the majority of organizations host their critical data and applications in the cloud, whether in AWS and Azure for development and infrastructure, or Microsoft 365, SharePoint, and Salesforce for core business operations. This large-scale journey to the cloud has drastically expanded the attack surface, even as the rapid adoption of IoT devices and remote working practices continues to furnish threat actors with additional vectors of attack.

Static and siloed defenses are simply no match for the unfamiliar risks, complexity, and speed of digital business, but the Enterprise Immune System is empowering organizations to embrace digital transformation with confidence. Darktrace's self-learning AI routinely discovers threats in this area that other tools miss – whether it be a Microsoft 365 compromise across Outlook and Teams, exposed IP in a customer's Azure environment, or a Mirai malware infection on an Internet connected surveillance camera.

Zero-Days, Malware, and Ransomware

Attacks that leverage zero-day vulnerabilities or novel strains of malware and ransomware are incredibly difficult to detect with approaches that rely on historical attack data. This includes static tools that use signatures, threat intelligence, or supervised machine learning trained on historical examples.

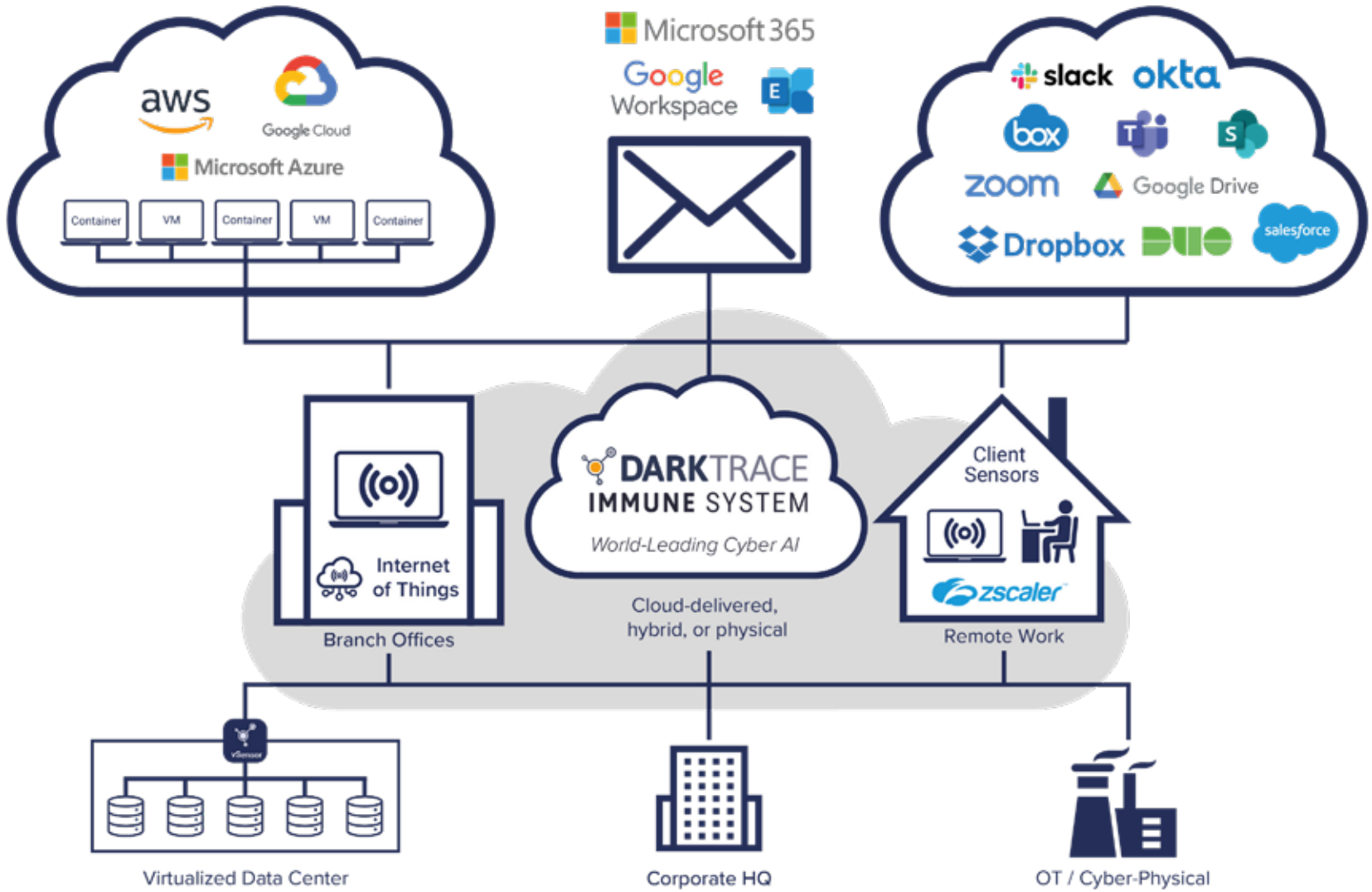
Self-learning AI that adapts to the unknown is the only technology that can discover zero-day attacks, which inevitably deviate from normal 'patterns of life' if analyzed at a sufficiently granular and comprehensive level of detail. Known ransomware families and strains of malware will equally be surfaced in seconds, as they deviate from the norm as well.

When APT41 launched a global campaign exploiting a zero-day vulnerability, Darktrace instantly detected and reported on the attack across multiple customers, well before any associated signatures had become available. This ensured that the attack was swiftly contained before it could escalate.

Figure 2: Cyber AI illuminates and visualizes the full scope of a ransomware attack

Immune System Coverage

The Enterprise Immune System provides scalable, self-learning protection of your dynamic workforce as it evolves – from cloud and collaboration tools, to the corporate network and remote endpoints off the VPN.



Immune System Integrations

The Enterprise Immune System harnesses an open and extensible architecture to seamlessly plug into your diverse ecosystem as it evolves. With one-click integrations and custom templates, the platform can instantly ingest new forms of telemetry and share bespoke AI insights across established workflows.

Darktrace Immune System Platform

By learning normal patterns and discovering novel threats, the Enterprise Immune System represents a core capability of a broader self-learning platform. The product not only interfaces with Cyber AI Analyst to enable autonomous investigations, but also feeds an adaptive Autonomous Response framework via Darktrace Antigena. With Antigena, the platform can respond to self-learning detections and neutralize emerging attacks with dynamic and surgical precision. All three capabilities are grounded in our fundamental Cyber AI technology and can be seamlessly extended to protect industrial environments, cyber-physical systems, and email platforms.