A New Era of Cyber

Business leaders in the digital age face remarkably urgent risk factors in an era of automated and fast-moving cyber-threat – from the theft and manipulation of critical data, to the staggering losses caused by interruption to the business. These risks have heightened dramatically in recent years as threats develop and become more advanced, and as digital businesses continue to grow in complexity, diversity, and scale.

In the past, when threat actors were less advanced and when digital activity was more predictable, a traditional approach to security was often adequate to keep cyber-threats at bay. By configuring security tools with static rules and historical attack data, organizations have sought to detect threats by defining 'benign' or 'malicious' in advance – relying on representations of attacks that have either been conceived of in the form of a rule, or that have been observed 'in the wild' and reverse-engineered for future detection.

Yet the increasing frequency of novel external attacks and insider threats, together with the exploding complexity of the digital estate, have gradually disarmed security teams who still rely on traditional controls. These rigid defenses have failed to detect the novel tactics and techniques of sophisticated cyber-criminals, who can now blend into the noise of the network and sweep through large and complex infrastructures in seconds.

Beyond the corporate IT network, security teams must also protect a diverse and fragmented patchwork of SaaS applications, cloud workloads, industrial machinery, and email platforms – all of which come with their own complex and incompatible controls. The interrelation of workforce behaviors across these different environments has rendered point solutions inoperable, as they lack the unified scope required to catch threats unfolding across the entire organization.

Darktrace: The Self-learning Advantage

While traditional defenses continue to define the threat in advance, Darktrace focuses instead on learning the normal 'pattern of life' for individual businesses and spotting subtle deviations indicative of a threat. Like the human immune system, Darktrace's Enterprise Immune System learns 'on the job', from the data and activity that it observes in situ. This means making billions of probability-based calculations in light of new evidence and continuously learning as the business evolves.

The threats that infiltrate your organization will typically not be historical attacks, but rather novel threats that have evaded existing defenses, or inappropriately behaving employees and third parties. By learning a sense of 'self' for your entire organization, Darktrace's Enterprise Immune System discovers subtle, previously unseen patterns and emerging threats that would otherwise go unnoticed – from a novel strain of ransomware, to insider data theft.

The Enterprise Immune System's AI detections are complemented by Autonomous Response and AI Investigation capabilities delivered by Darktrace Antigena and Cyber AI Analyst, respectively. While Antigena instantly interrupts emerging threats with surgical precision, Cyber AI Analyst automatically triages, interprets, and reports on the full scope of security incidents, reducing 'time to meaning' by up to 92%

Darktrace and Zero Trust

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 micro-segmentation, whitelists, 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.

The Enterprise 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 provides a layered security strategy that combines zero-trust controls with autonomous systems that adapt as the business and workforce evolve.

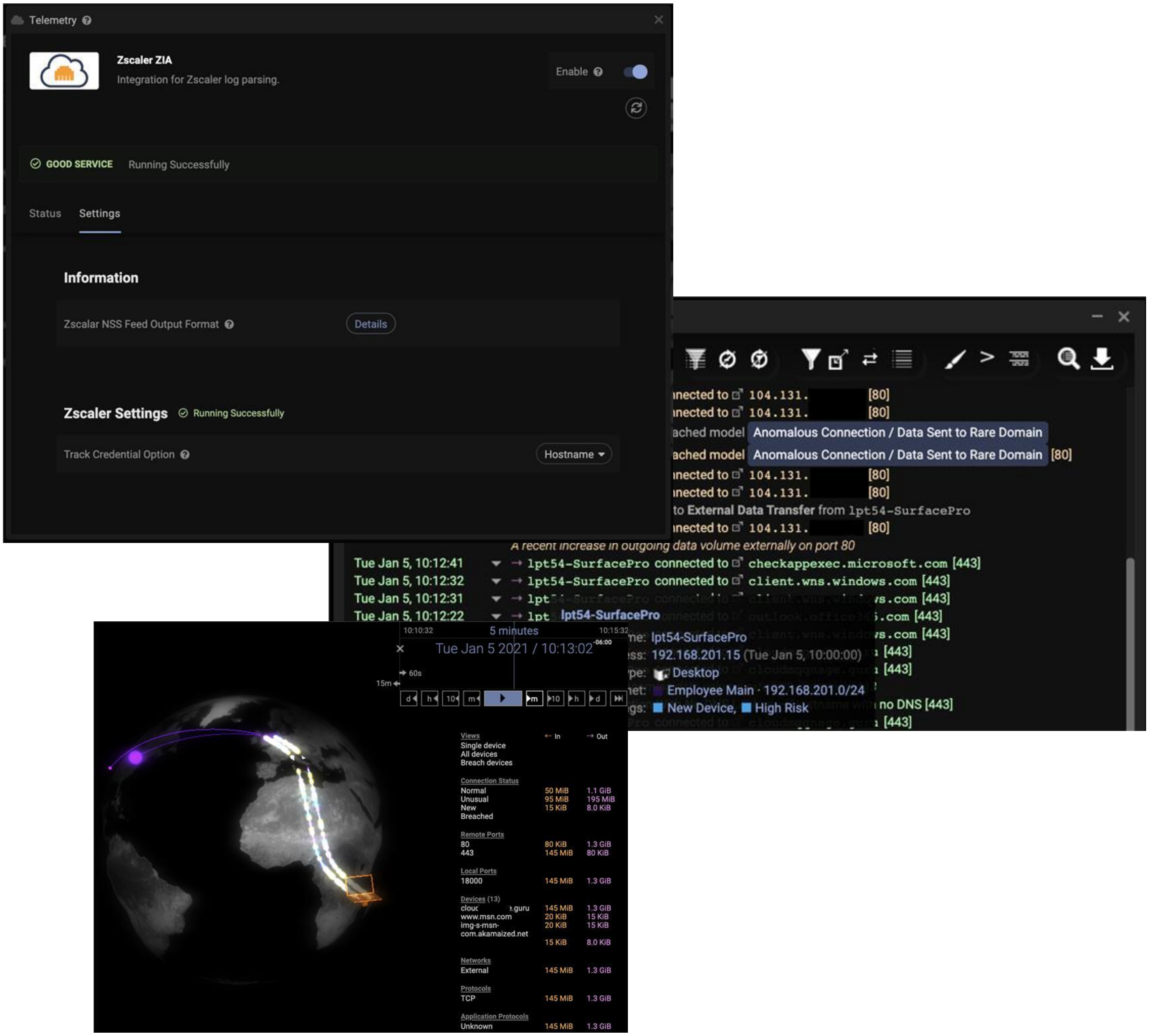
Native Integrations with ZIA & ZPA

Darktrace integrates with ZIA and ZPA to enrich the immune system's analysis with extended visibility of all user behavior that touches Zscaler.

With ZIA, the integration ingests weblogs from a ZIA device to simulate connection data, and web events produced by the Zscaler logging will be associated with a device of the same hostname. If a device of that hostname does not already exist, Darktrace will create a new device. Connection events created from Zscaler logs will be available to core Darktrace analysis and accessible in Advanced Search. With ZPA, Darktrace observes connectivity from the ZPA App Connector to internal resources.

By integrating ZIA and ZPA with the Enterprise Immune System, organizations of all sizes benefit from:

- Interoperability and platform synergies across the stack
- Meaningful enrichment of Darktrace modeling and visibility
- Better informed AI immune system detections
- Inclusion of high-quality Zscaler data in Cyber AI Analyst investigations



Telemetry

Zscaler ZIA

Integration for Zscaler log parsing.

Enable

GOOD SERVICE Running Successfully

Status Settings

Information

Zscalar NSS Feed Output Format Details

Zscaler Settings Running Successfully

Track Credential Option: Hostname

```
nnected to 104.131.[redacted] [80]
nnected to 104.131.[redacted] [80]
ached model Anomalous Connection / Data Sent to Rare Domain
ached model Anomalous Connection / Data Sent to Rare Domain [80]
nnected to 104.131.[redacted] [80]
nnected to 104.131.[redacted] [80]
to External Data Transfer from lpt54-SurfacePro
nnected to 104.131.[redacted] [80]
            A recent increase in outgoing data volume externally on port 80
Tue Jan 5, 10:12:41  → lpt54-SurfacePro connected to checkappexec.microsoft.com [443]
Tue Jan 5, 10:12:32  → lpt54-SurfacePro connected to client.wns.windows.com [443]
Tue Jan 5, 10:12:31  → lpt                                          ws.com [443]
Tue Jan 5, 10:12:22  → lpt  lpt54-SurfacePro                        5.com [443]
                         me: lpt54-SurfacePro                       ws.com [443]
                        ess: 192.168.201.15 (Tue Jan 5, 10:00:00)    [443]
                        pe: Desktop                                  [443]
                        et: Employee Main · 192.168.201.0/24
                        gs: New Device, High Risk                    no DNS [443]
                                                                     [443]
```

10:10:32 5 minutes 10:15:32

Tue Jan 5 2021 / 10:13:02 -06:00

→ 60s

15m ←

Views	← In	→ Out
Single device		
All devices		
Breach devices		
Connection Status		
Normal	50 MiB	1.1 GiB
Unusual	95 MiB	195 MiB
New	15 KiB	8.0 KiB
Breached		
Remote Ports		
80	80 KiB	1.3 GiB
443	145 MiB	80 KiB
Local Ports		
18000	145 MiB	1.3 GiB
Devices (13)		
clouc[redacted].guru	145 MiB	1.3 GiB
www.msn.com	20 KiB	15 KiB
img-s-msn-com.akamaized.net	20 KiB	15 KiB
	15 KiB	8.0 KiB
Networks		
External	145 MiB	1.3 GiB
Protocols		
TCP	145 MiB	1.3 GiB
Application Protocols		
Unknown	145 MiB	1.3 GiB