Darktrace Open Architecture: Plugging Cyber AI into Your Digital Ecosystem

The Darktrace Immune System is a cloud-native platform that delivers self-learning protection, AI Investigations, and seamless integrations via an open and extensible architecture.

**Key Benefits**

- Enable one-click integrations for seamless extension
- Share bespoke AI insights with SIEM, SOAR, and downstream ticketing systems
- Extend visibility via native integrations with endpoint and zero-trust technologies
- Activate Autonomous Response via active integrations with firewalls and preventative controls
- Extensive API support for data ingestion and asset and alert output for use across your security ecosystem

Unifying enterprise defenses in the face of evolving threats and exploding complexity has never been more critical nor difficult to achieve. Today’s digital business is characterized by distributed users, diverse applications, and disjointed point solutions that are nearly impossible to harmonize. Yet with Cyber AI, security teams can protect their dynamic workforce across multiple siloes, while enhancing the value of existing investments through shared intelligence and active integrations.

The Darktrace Immune System harnesses an open architecture to seamlessly plug into a diverse ecosystem as it evolves. With one-click integrations, the platform can instantly ingest new forms of telemetry, share bespoke AI insights across established workflows, and interoperate with a wide range of technologies to deliver Autonomous Response across email systems, inline defenses, and collaboration platforms. Beyond the growing number of one-click integrations, the Darktrace Immune System has multiple methods of data ingestion and output to best fit your ecosystem.

The Darktrace Immune System is the core technology that powers the platform as it detects, interprets, and responds to cyber-threats across the business. Darktrace’s open architecture enables one-click integrations that plug Cyber AI into your diverse digital ecosystem.
Leveraging the Darktrace Immune System via Integrations:

The Darktrace Immune System can easily ingest enrichment data from other systems to best model user and device behavior, track users and devices, or add context during investigations within the solution. Darktrace offers native support for industry standard data ingestion formats, many of which are used in the integrations listed below.

Further, beyond existing one-click integrations, the Darktrace Immune System also has extensive ingest and alert output capabilities and a powerful API that provides access to intelligence from the platform around assets or devices, alert or model breach data, Cyber AI Analyst Incidents, and even packet captures and Advanced Search data for integration into your security workflows, be they data lakes, SIEMs, SOARs, or other systems.

The diagrams below outline some of the most common one-click integrations and methods available for activation in the UI today and, secondly, a guide on areas of the organization that may benefit from these, as well as areas of ingest and output capabilities with common security and IT solutions. Please refer to documentation available on our Customer Support Portal for specific integrations as well as the API guide and contact us for help with custom API workflows or if you don’t see a product integration below that you’d like us to consider.
**Organizational Capabilities**

### CxO & Management

**Risk Profile**
Leadership can tailor the platform to cover specific business risks via custom models that inform AI detections and Antigena actions.

**Executive Reporting**
Management benefits from one-click Executive Threat Reports that track high-level trends over time, while weekly Cyber AI Analyst Incident Reports summarize the most relevant incidents in your environment.

### Internal SOC

**Triage & Investigation**
Cyber AI Analyst automatically investigates every security event the immune system detects, and internal security analysts can consume the Incident Reports it produces and conduct further investigation as needed.

**Situational Awareness**
Darktrace provides unified and bespoke visibility across the business to inform your analysis of other tools in the stack.

### Threat Hunting Team

**Deep Investigation**
While Cyber AI Analyst provides a high-level overview of relevant incidents, human Threat Hunting teams can also investigate low-level anomalies and proof hypotheses via Darktrace’s in-depth Threat Visualizer.

**Export Data**
Threat Hunting teams can also export data – for example, all DNS traffic – into other tools for further analysis.

### Capabilities

### SIEM & SOAR

**Share AI Insights**
Native integrations via API and syslog allow Darktrace to feed AI detections and Cyber AI Analyst Incidents to SIEMs for analysis and correlation, as well as SOAR solutions to trigger response playbooks.

**Telemetry Ingestion**
Darktrace can poll SIEM and SOAR solutions to ingest enrichment data, and SOAR playbooks can be configured to trigger custom models and Cyber AI Analyst investigations in Darktrace.

### Ticketing System / Case Management

**Forward Cyber AI Output**
Darktrace’s detections and Cyber AI Analyst Incidents can be fed to downstream ticketing systems in various formats (e.g. CEF, LEEF, and JSON), in alignment with custom thresholds defined by the user.

**Interact with Cyber AI Output**
Users can acknowledge or comment on Darktrace detections or Cyber AI Analyst Incidents from within the UI of the ticketing or case management system.

### Firewalls, NACLs & Preventative Controls

**Autonomous Response**
Darktrace Antigena can trigger Autonomous Response actions via integrations with firewalls and preventative controls for attacks that have gotten through.

**Log Ingestion**
Darktrace can also ingest logs from firewalls and network devices to extend visibility as needed.
Asset / Inventory Management

Darktrace can export asset CSV lists and auto-detected device types into asset management systems. It also displays a 2D network topology to provide granular visibility in this area.

Improve Asset Tracking

Darktrace can also interoperate with asset management systems to import VIP devices, tag devices, label subnets, and improve device tracking more generally.

Networking / IT Ops

Enhance Visibility

Networking and IT Ops teams can enrich the platform by adding subnet labels and custom tags given their knowledge of the network, while supporting integrations (e.g. LDAP) that enhance Darktrace's visibility.

Leverage AI Granularity

Darktrace's granular insights also enable IT teams to inventory CSV, obtain PCAPs for troubleshooting, and gain substantial visibility for debugging.

Organizational

Security Engineers

Augment Detections

Security engineers can augment the platform by maintaining threat models, creating custom use cases, and merging Threat Intelligence with Darktrace's AI analysis as needed.

Harness Darktrace Data

They can also leverage alerts, raw data, and other information in Darktrace by feeding it to other tools that would benefit from bespoke, real-time intelligence.

External MSSP

Manage Darktrace

If applicable, an external MSSP can manage Darktrace with analyst resources (Levels 1 and 2), maintain threat models, and input Threat Intelligence if needed.

Feed the Stack

The external MSSP can also share Darktrace’s output with other MSSP tools, SOAR solutions, and downstream ticketing or case management systems.

Networking

VPN & Zero-Trust Technologies:

Extend Workforce Coverage

By integrating with VPN and zero-trust services, Darktrace can extend its visibility across an increasingly distributed workforce. Native integrations and custom templates are available for any service in this area.

Endpoints

Client Sensors

By deploying Client Sensors, Darktrace can extend its visibility of network connections to desktops in branch offices or off the VPN.

Integrate with EDRs

Darktrace can also ingest EDR alerts as a weak indicator that informs our AI analysis across the business. EDR alerts can also trigger Cyber AI Analyst investigations, without the need for an underlying Darktrace detection.

Asset / Inventory Management

Real-Time Visibility

Darktrace can export asset CSV lists and auto-detected device types into asset management systems. It also displays a 2D network topology to provide granular visibility in this area.

Improve Asset Tracking

Darktrace can also interoperate with asset management systems to import VIP devices, tag devices, label subnets, and improve device tracking more generally.