# Darktrace and Endace

## AI cyber defense and comprehensive Network History to detect and rapidly respond to any security threat.


**PRODUCTS**

**Darktrace Enterprise Immune System**

**EndaceProbe with Application Dock**

### BENEFITS

Darktrace

- Autonomously detects and responds to cyber-threats before they escalate into a crisis
- Continuously learns and adapts its understanding of 'normal' in light of new evidence
- Provides complete visibility of every user and device
- Installs in one hour with no manual tuning required.

EndaceProbe Analytics Platform

- Integrated Network History, high performance packet capture and playback with simple, one-click investigation workflows
- Rapid drill down from the Darktrace Threat Visualizer to Network History for confident root cause identification and resolution.

The ability to detect and respond to unusual behavior, as it emerges, is critical in this era of novel and fast-moving cyber-threats. Deploying Darktrace and Endace helps organizations to understand when benign activity turns 'abnormal' amid the noise of everyday business activity. It allows customers to expedite threat investigations by combining cyber AI technology with historical network data that delivers concrete insights and enables rapid remediation of threats.

Darktrace's Enterprise Immune System is Darktrace's flagship AI cyber defense solution. It combines real-time threat detection with autonomous response technology, network visualization, and advanced investigation capabilities in a unified system that is fast and easy to install. Using proprietary machine learning and AI algorithms developed by mathematicians from the University of Cambridge, the Enterprise Immune System detects and responds to all forms of cyber-threat, including subtle insiders, low-and-slow attacks and fast-moving threats like ransomware, without relying on rules, signatures, or prior assumptions of what 'malicious' activity looks like.

The Enterprise Immune System analyzes raw network traffic across the digital business to learn the normal 'pattern of life' for every user, device, and all the relationships between them. These 'patterns of life' adapt as your network evolves, and become increasingly accurate over time. Rather than pre-defining the threat in advance, the Enterprise Immune System independently detects significant deviations and alerts the organization in real time, taking autonomous action to neutralize the threat and give the security team time to catch up and investigate.

This self-learning approach means that the technology is agnostic to the provenance, delivery mechanism, tactics and function of the cyber-attacker or threat. All significant deviations are seen and correlated, resulting in the detection of genuine threats, without producing floods of false positives.

The Enterprise Immune System also provides security teams with complete network visibility and actionable intelligence via the Darktrace Threat Visualizer interface, which provides a unified view from which anomalous activity can be visualized and investigated in real time. A wealth of information can be variously queried and exposed using the interactive features within the Threat Visualizer, including a dynamic dashboard where users can filter incidents based on their level of severity, and an interactive Play-Back tool which lets users replay incidents and zero in on the real-time context around each event.

The EndaceProbe™ Network Analytics Platform captures, indexes and stores network traffic with 100% accuracy while simultaneously hosting a wide variety of network security and performance monitoring applications in Application Dock™, the EndaceProbe's built-in hosting environment. Customers can thus enhance their cyber resilience by deploying Darktrace virtual sensor instances anywhere they have EndaceProbes deployed on the customer's network. Hosted instances can analyze recorded traffic in real time at full line-rate or analyze recorded Network History for back-in-time investigation.

## Accelerating Security Investigations

The Network History recorded by EndaceProbes can be integrated into the Darktrace Threat Visualizer using the Pivot-To-Vision function of the EndaceProbe's API. Security analysts can pivot from threat alerts in the Threat Visualizer directly to EndaceVision™, the EndaceProbe's built-in investigation tool, to analyze the related, packet-level Network History.

Using the IP address and time range of the trigger event, Pivot-To-Vision focuses the analyst directly on pre-filtered incident data. EndaceVision lets analysts dissect, review and extract the relevant traffic from petabytes of Network History recorded on the network. It enables analysis at the microsecond level with views filtered by Application, IP, Protocol, Top Talkers and many other parameters, allowing rapid insights and accurate conclusions.

## Scaling Deployment with Darktrace Sensors and Application Dock

Darktrace sensors can be hosted on EndaceProbes. Every packet captured and recorded by the EndaceProbe can be simultaneously streamed to hosted Darktrace virtual sensors in real time.

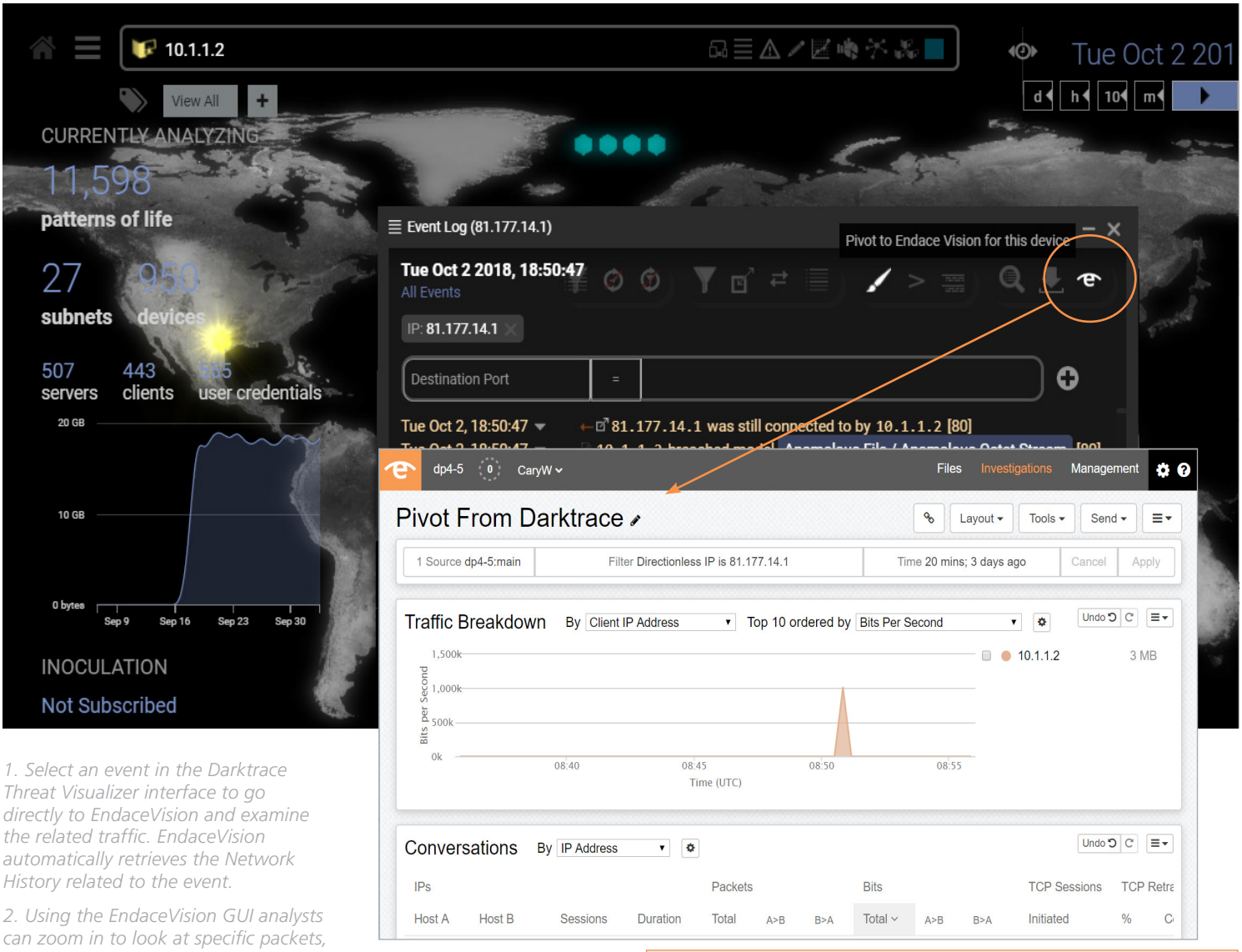
Security Operations teams can dynamically deploy AI-based Darktrace sensor instances anywhere on the network they have EndaceProbes deployed, allowing them to gain advanced threat detection and autonomous response technology on-demand without additional hardware rollouts and leveraging the high bandwidth interfaces of the EndaceProbes.

EndaceProbes are designed to ensure system resources used for capture and recording are separated from the resources used by hosted applications. This means capture performance is never impacted by hosted applications and vice-versa, guaranteeing 100% accurate recording even when Darktrace instances are analyzing heavy traffic loads on core network interfaces.

## Conclusion

By deploying Darktrace's Enterprise Immune System for your cyber AI defense solution, your SecOps teams can Pivot-to-Vision on EndaceProbes and quickly investigate the depth and breadth of any threatening activity on the network. The combined solution extends reach easily, leveraging existing EndaceProbe hardware deployments to enhance cyber resilience and network recording capabilities. The Endace and Darktrace solution combines real-time threat detection and autonomous response technology with definitive network evidence to enable rapid remediation.

## How it Works




*1. Select an event in the Darktrace Threat Visualizer interface to go directly to EndaceVision and examine the related traffic. EndaceVision automatically retrieves the Network History related to the event.*

*2. Using the EndaceVision GUI analysts can zoom in to look at specific packets, or zoom out to look for precursor or post-event activity,*

For more information on the Endace portfolio of products, visit: endace.com/products

For further information, email: info@endace.com