Darktrace PREVENT/End-to-End and Your Data

Darktrace PREVENT/End-to-End (E2E) is a major component of Darktrace PREVENT, a product family, which aims to proactively harden defenses and minimize cyber risk.

With a unique AI-powered view across your digital estate, Darktrace PREVENT/E2E provides continual insight to reduce risk, remediate vulnerabilities, and defend the organization's most critical assets. This data sheet outlines which data feeds E2E needs to operationalize these preventative security measures.

The system builds up a corpus of contextual data from network, email, (Azure) Active Directory and SaaS services, supplemented with insight into CVEs and vulnerabilities from third-party security integrations, to gain a deep understanding of the potential weak spots that exist across your organization.

This information builds upon the pattern-of-life analysis generated by Darktrace DETECT including historic connectivity, email communications, endpoint interaction and user patterns to provide real-world propagation routes.

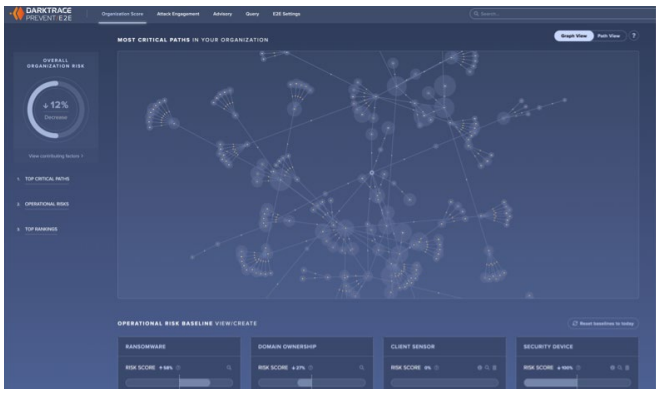

Figure 1: PREVENT/E2E shows your organizations most critical attack paths.

Figure 2: PREVENT/E2E allows you to identify top risk pathways for specific devices.

DARKTRACE

Darktrace PREVENT/End-to-End and Your Data

Component	Required/Recommended?	What data is used for	How the data is retrieved
Network data	Required	• The formation of network-based attack paths, using communication patterns observed within physical or virtual network traffic • Calculation of multiple Device-based metrics	DETECT/Network
Email data	Required	• The formation of User-based attack paths • The calculation of Exposure score metrics for email-enabled accounts • E2E Attack Engagements • Calculation of multiple User-based metrics	DETECT & RESPOND/Email or Via Microsoft Graph API authentication
On-prem AD data	Required if no AzureAD data, else recommended	• The formation of Account-based attack paths • Retrieving hierarchy data • Retrieving Titles, Roles, and Permissions • Calculation of multiple Account-based metrics	LDAP querying of the AD server from a Darktrace master using a Read-only service account
AzureAD data	Required if no on-prem AD data, else recommended	• The formation of Account-based attack paths • Retrieving hierarchy data • Retrieving Titles, Roles and Permissions • Calculation of multiple Account-based metrics	Granting Darktrace API access to the Microsoft Graph API and Azure Management API
Azure Subscription(s) data	Recommended	• Retrieving IaaS and PaaS data within Azure (including VMs, databases and other services used to build applications)	Grant Darktrace API access to Microsoft Graph API and Azure Management API, plus adding the Reader Role to each Subscription for the Darktrace PREVENT/E2E Azure application
3rd Party Integrations	Recommended	• CVE data • Detailed OS data • "Last Updated" data	Dependent on integration, typically granting Darktrace relevant access to the 3rd Party provider's API

darktrace.com
info@darktrace.com

Scan to LEARN MORE