DARKTRACE & THREAT VISUALIZER

Product Overview

Darktrace is a network solution for detecting and investigating emerging cyber-threats that evade traditional security tools. It is powered by Enterprise Immune System technology, which uses machine learning and mathematics to monitor behaviors and detect anomalies in your organization's network. The Enterprise Immune System's mathematical approaches do not require signatures or rules and so can detect emerging 'unknown unknown' attacks that have not been seen before.

Darktrace takes passive feeds of raw network traffic from the centers of your networks. Once connected, the technology immediately begins using a range of mathematical approaches to create numerous models of behavior for each individual user and device within the organization. The Enterprise Immune System's self-learning mathematics work from day one, detecting anomalous behaviors on the network. They continue to learn on an ongoing basis - constantly updating as the organization evolves.

Creating powerful 'pattern of life' models of every individual and device on your network allows Darktrace to detect subtle shifts in behaviors, such as the way someone is using technology, a machine's data access patterns, or trends in communications. This may indicate any number of potentially threatening events, such as the theft of a user's credentials, a compromised device, or the actions of a disaffected or negligent employee.

Darktrace monitors over 350 dimensions of user and device activity. This allows it to detect a range of anomalies, including network reconnaissance and traversal, unexpected downloads from unusual internet domains, intranet or file system cloning, sensitive data logins from a new device and location, unusual applications and protocols, or a change in pattern of information uploads. These activities may be worthy of investigation if they represent significant departure from normal behavior.

Threat Visualizer

The Threat Visualizer is Darktrace's graphical and interactive 3D interface, which enables analysts and business executives to intuitively visualize behaviors and investigate anomalies, without requiring an understanding of the advanced mathematics that power the platform.

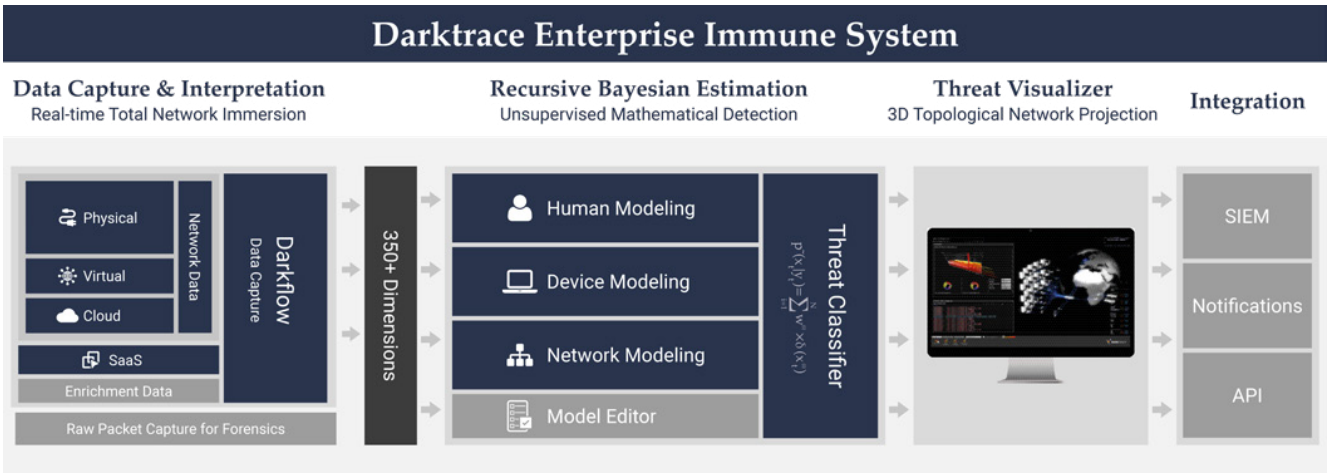
The Threat Visualizer provides users with intelligence-led insights into the relationships and data flows across the network, in real time. When an anomaly emerges, the Visualizer allows users to play back the events leading up to and during the anomaly.

The Visualizer is an interactive tool, allowing analysts to investigate deepening layers of detail and perform very complex queries. The platform also supports analyst investigation at a detailed level and enables the download of the relevant raw network packets for deep forensic analysis in your organization's preferred tool (e.g. Wireshark).

> "Traditionally, when we think about security and protecting ourselves, we think in terms of armor or walls. Increasingly, I find myself looking to medicine and thinking about viruses, antibodies.
>
> Part of the reason why cybersecurity continues to be so hard is because the threat is not a bunch of tanks rolling at you but a whole bunch of systems that may be vulnerable to a worm getting in there. It means that we've got to think differently about our security."
>
> **President Obama, 2016**

Key Features

- Adaptive – evolves with your organization
- Self-learning – constantly refines its understanding of normal
- Probabilistic – works out likelihood of serious threat
- Real-time – spots threats as they emerge
- Works from day one – delivers instant value
- Low false positives – correlation of weak indicators
- Data agnostic – ingests all data sources
- Highly accurate – models human, device and enterprise behavior
- Scalable – all sizes of network, including over a million devices



Mathematics and Machine Learning

The key to the Enterprise Immune System approach is not only to identify meaningful relationships within data, but also to quantify the uncertainty associated with such inference. By understanding this uncertainty, it becomes possible to bring together many results within a consistent framework – the basis of Bayesian probabilistic analysis.

At the heart of Darktrace are four mathematical engines using multiple mathematical approaches, including the breakthrough of Recursive Bayesian Estimation. The first three produce models of behavior for individual people, the devices they use and the enterprise as a whole. When unusual behavior is detected in one or more of these three engines, a candidate alert is sent to an 'umbrella' engine, the Threat Classifier. Its job is to look across the outputs of all models across all time, to filter out false positives and report on genuine abnormalities worthy of investigation, however subtle. The unique combination of multiple Bayesian approaches correlated and moderated by the Threat Classifier makes Darktrace highly accurate in abnormality detection at enterprise scale.

Complementary Technology

Darktrace is designed to complement existing security infrastructure and approaches. Well- configured network border defenses and host defenses are essential, but only partially successful against determined attackers whether external or internal. The use of machine learning for monitoring and detection enables you to respond to attacks and threats, without knowing what to look for ahead of time.

Outputs from the Enterprise Immune System can be routed to existing commercial or bespoke security dashboards or SIEM via your favored mechanism (syslog, SNMP, connectors, file, databases, or API).

Model Editor

Darktrace also benefits from an integrated module for policy and compliance monitoring and enforcement. This supports the definition of additional compliance policies and models that can be tailored to a customer's specific detection requirements (e.g. no Dropbox access, no travel with sensitive IT to certain countries, internal DNS services only, etc.).

Installation and Configuration

Easy to scale

A single Darktrace appliance can take multiple inputs of network traffic and cover up to tens of thousands of individual machines, depending on peak traffic volumes. Multiple Darktrace appliances can cluster to cover geographically distributed networks eliminating the need to move large volumes of data around your network. One of the largest Darktrace deployments covers over a million devices.

Full packet capture

Darktrace consumes raw network traffic, collected by either:

- port spanning your existing network equipment
- inserting/re-using an inline network tap

Simple to install, configure and support

- Single appliance takes up 2U of rack space
- Installed, configured and tested in less than an hour
- All user interfaces accessed via a web browser
- Requires very little support

Your Data Is Your Data

Darktrace network traffic data processing occurs locally on the appliance(s) and is not uploaded to the cloud or to a Darktrace data center. Data is only accessible through the secure connection unless otherwise agreed.

About Darktrace

Darktrace is the world's leading machine learning company for cyber security. Created by mathematicians from the University of Cambridge, the Enterprise Immune System uses AI algorithms to automatically detect and take action against cyber-threats within all types of networks, including physical, cloud and virtualized networks, as well as IoT and industrial control systems. A self-configuring platform, Darktrace requires no prior set-up, identifying advanced threats in real time, including zero-days, insiders and stealthy, silent attackers. Headquartered in San Francisco and Cambridge, UK, Darktrace has 23 offices worldwide.

Contact Us

US: +1 (415) 229 9100
Europe: +44 (0) 1223 324 114
APAC: +65 6248 4516

info@darktrace.com
www.darktrace.com