DARKTRACE

Product Data Sheet

The Enterprise Immune System and Threat Visualizer

Product Overview

The Enterprise Immune System is a network solution for detecting and investigating emerging cyber threats that have evaded network border and endpoint defenses. By applying advanced mathematics to model behaviors in your enterprise, it monitors behaviors and detects anomalies in your organization's computer and user activities. 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 is delivered as an appliance that 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 machine within the organization. The Enterprise Immune System's self-learning mathematics start working 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 even 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.

Examples such as 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 uploading are all detectable through mathematical modeling. These activities may be worthy of investigation if they represent a significant departure from normal behavior.

Threat Visualizer

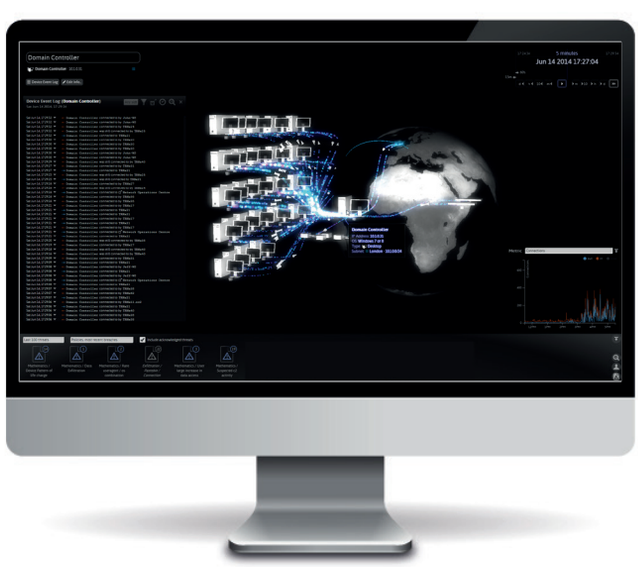
The Enterprise Immune System is complemented by the Threat Visualizer, a graphical and interactive 3D interface designed specifically to enable analysts and business executives to intuitively visualize behaviors and investigate anomalies, without requiring an understanding of the advanced mathematics that power the platform.

Key Features

- Advanced threat detection, including new and unique cyber-attacks
- Based on sophisticated machine learning and mathematics
- Signature-free approach allows detection of emerging or targeted attacks that have not been seen before
- Works in real-time to provide alerts as threats arise
- Powerful visualization platform enables threats to be analyzed and investigated intuitively
- Network appliance installed passively into infrastructure within one hour

The Threat Visualizer provides users with intelligence-led insights into the relationships and data flows across the network, in real time and at any point in its connected history. When an anomaly emerges, the Visualizer shows the events leading up to and during the anomaly, allowing you to playback the questionable sequence of events as they happened.

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).



Complementary technology

The Enterprise Immune System 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 addition of signature-free monitoring and detection provides an opportunity to respond to attacks that are new or tailored to your organization, 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).

Mathematical foundations

The key to this new mathematics 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 the Darktrace product 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 entire enterprise of which they are a part. 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.

Darktrace Policy and Compliance Module

The Enterprise Immune System also benefits from an integrated module for policy and compliance monitoring and enforcement. This supports the definition of additional compliance policies 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.).

Your data is your data

The Enterprise Immune System does all of its processing and outputs within your data centers. It does not send data to the cloud or get accessed by Darktrace employees, unless specifically agreed with the organization in advance. Customer data and intelligence outputs are not shared with a wider user community.

Installation and configuration

Full packet capture

The Enterprise Immune System 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

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.

DARKTRACE ENTERPRISE IMMUNE SYSTEM