Darktrace Proof of Value

A Proof of Value (POV) is an easy, four-week trial of Darktrace's Enterprise Immune System technology. It allows you to evaluate the power of Darktrace's self-learning technology within your own environment, at no cost.

Our experienced team will install a Darktrace appliance into an agreed point in your network, and have it up and running within 1-2 hours. From there, you will be given access to Darktrace's award-winning Threat Visualizer interface. We will demonstrate the value of our machine learning approach, and highlight the types of anomalies that Darktrace detects.

POV Benefits

Identification of Anomalies and Potential Threats

Darktrace will immediately begin to flag anomalies or potential threats, based on its understanding of what is 'normal' on your network. Meaningful results are experienced within days of installation. The POV allows you to evaluate how the self-learning technology is finding events and behaviors that would otherwise go unnoticed within the noise of the network, and identify potentially threatening events.

Network Visibility

You will gain access to Darktrace's intuitive Threat Visualizer user interface, which graphically visualizes your entire network within minutes. Complimentary user interface training will allow you to use the Threat Visualizer yourself to view events, focus on areas of interest, and investigate incidents.

Three Threat Intelligence Reports

You will receive three Threat Intelligence Reports (TIRs), which detail the anomalies that the Darktrace Enterprise Immune System has found, explain the significance of each event, and summarize the findings in an easy-to-understand Executive Summary. TIRs are authored by Darktrace's world-class cyber security analysts.

POV Timescale

Schedule	Steps	Darktrace resource	Your company resource
Pre POV	• Schedule installation date • Allocation of dedicated Cyber Technology Specialist (CT)	Account Executive (AE), CT	Technical sponsor
Day 1	• CT arrives on site to install the Darktrace appliance (1-2 hours) • Passive data collection and validation begins, using port spanning via your existing network equipment	CT	Technical sponsor
Week 1	• Machine learning is activated • Darktrace immediately starts analyzing and modeling network data, learning about what's 'normal' for each user and device on your network	CT	Technical sponsor
Week 2	• TIR 1 Review Meeting • User interface familiarization deep dive	CT, AE	Technical sponsor
	• Gain access to the 3D Threat Visualizer interface • See what is happening within your network in real time	CT	Technical sponsor
Week 3	• TIR 2 Review Meeting • Presentation of commercial proposals for full network deployment	CT, AE	Executive sponsor, technical sponsor
	• As week 2 • Continue to familiarize yourself with the Threat Visualizer • See and respond to real-time alerts	CT	Technical sponsor
Week 4	• TIR 3 Review Meeting • Presentation of standard Darktrace Terms and Conditions sheet	CT, AE	Executive sponsor, technical sponsor
	• POV finishes • Schedule TIR Summary Review (optional) • Commercial next steps agreed	CT, AE	Executive sponsor, technical sponsor

Resources Required for Success

Secure Connection

Darktrace appliances connect back to Darktrace Central Management (‘Call Home’) over a secure and encrypted dual-factor authentication channel in order to receive new mathematical models and software updates. For managed deployments and POVs, this also enables you to leverage the experience of Darktrace cyber analysts. Customers maintain total control of the connection, which is initiated and maintained from the appliance and can be started, terminated or audited at any time. For the purposes of carrying out continual health checks, we request that a connection is maintained during normal business hours.

Mapping Data

To take full advantage of the unsupervised machine learning on hosts with dynamic IP addressing, the DHCP signal from server to client must be contained in the data feed. This helps build the most granular understanding of particular machine and user behavior. For deployments beyond the Proof of Value, other forms of mapping data can be used to permit integration with many industry-standard log systems.

If DHCP data from the network is not available, please ask your Darktrace contact for secondary options.

A Joint Commitment: TIR Reviews

Darktrace commits to providing a POV at no cost and without obligation, from installation through to subsequent services and consultancy with our cyber specialists. In addition, each Threat Intelligence Report is produced exclusively for your organization, detailing specific anomalies that are discovered during the POV.

For every Threat Intelligence report delivered, a TIR Review Meeting or Call is held with your account team, helping you understand the results of the POV and evaluate those findings. In order to get the full value from this commitment, Darktrace requires that the appropriate personnel are involved in each step of the process.

Privacy & Legal Considerations

- Data collection is passive.
- 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.
- If the customer takes advantage of Darktrace’s deep packet analytics services, Darktrace analysts will leverage the ‘Call Home’ service to and from the appliance(s) to remotely inspect the primary local Darktrace UI (Threat Visualizer) for threat intelligence reporting (TIRs) and, where necessary, forensically extract from it sample packet capture data to aid threat identification. In addition, the Darktrace Operations team utilize ‘Call Home’ for health check monitoring and system software updates.
- Data is securely deleted if you do not wish to proceed beyond the POV.
- The appliance does not affect network and business operations.
- A shrink wrap legal agreement is required to activate the appliance