Darktrace Proof of Value

Darktrace offers you the opportunity to evaluate the power and benefits of Darktrace's award-winning cyber AI technology, at no charge to your organization.

A Darktrace Proof of Value (POV) is a 30-day free trial designed to demonstrate the Industrial Immune System in action. The POV also gives you the opportunity to view your OT and IT environment through the Threat Visualizer, Darktrace's 3D visibility, detection, and investigation user interface. The 30-day trial commences when the appliance goes live, and a dedicated Account Executive and Cyber Technologist will guide you through the POV experience.

POV Benefits

Detect Threats You Didn't Know About

Darktrace quickly forms an evolving understanding of the 'pattern of life' of your OT and IT environment. It will automatically detect threats and anomalous behaviors that other tools miss.

Visibility

As part of the POV, Darktrace provides complete visibility of the digital environment in which it's deployed. With access to the Threat Visualizer, you can also visualize, investigate, and play back cyber-threats or incidents.

Threat Intelligence Reports (TIRs)

As well as access to the Threat Visualizer, you will receive three Threat Intelligence Reports (TIR) during a Darktrace POV. Produced by Darktrace's world-class Cyber Analyst team, the TIRs summarize and assess the discoveries made each week of the POV, and help your teams and executives understand and evaluate your organization's current threat level, and assist with decision-making.

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 Darktrace (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 in your environment	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 digital environment in real time	CT	Technical sponsor
Week 3	• TIR 2 Review Meeting • Presentation of commercial proposals for full 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

Installation Process

Our technical team will work with you to decide on the best deployment location. We understand that availability and safety are critical and will work with you to ensure these aren't disrupted.

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.