TYCHON

Attack Surface Management Use Case

Attack Surface Management is the continuous discovery, monitoring, evaluation, and remediation of attack surfaces within an organization. Your attack surface is defined as any endpoint within your interconnected network that could be leveraged by an attacker. TYCHON Enterprise, an advanced endpoint analytics and remediation platform, is a powerful Attack Surface Management tool. Leveraging TYCHON Enterprise, our users can search, visualize, remediate, and monitor every endpoint across their enterprise. From discovery to one-click remediation, the TYCHON platform manages every layer of endpoint security to keep analysts in control of their network and minimize attack surface risk.

Benefits

Discover

Identify, classify, and assess all your organization's endpoints, including shadow IT, using natural language questions and dashboards.

Monitor

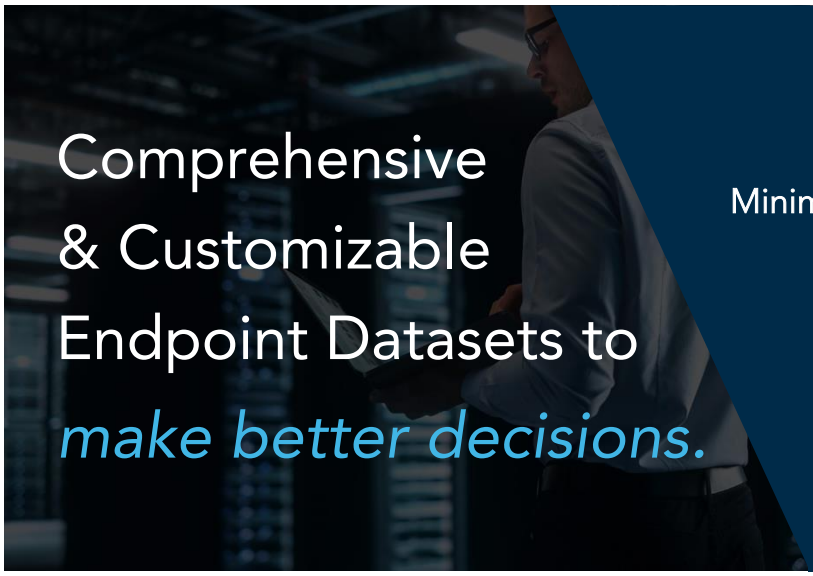
Continuously monitor your endpoints to discover exposures, compliance violations, unknown endpoints, and more.

Evaluate/Prioritize

Use built in analytics, reports, and dashboards to analyze endpoints, evaluate risk levels, and prioritize remediation actions.

Remediate

Take advantage of one-click remediations to ensure patch compliance, disable accounts, quarantine systems, and more.



Comprehensive & Customizable Endpoint Datasets to *make better decisions.*

Minimize Your Attack Surface with TYCHON Enterprise

- Easy to Use
- Powerful Analytics
- Speed & Accuracy

725 Jackson Street, Suite 101 I Fredericksburg, VA

tychon.io | info@tychon.io

TYCHON

Key Features

1 TYCHON SENSOR

Lightweight agent built on a micro service engine framework to optimize integrations and provide superior data quality to fulfill use cases.

- Logins, Permissions, & Users
- File Meta Data & Integrity
- Digital Signatures & Certificates

2 MESH MODEL

Instantly query up to a million endpoints. Unique architecture components built for scalability and fast response.

- Deploy Patches
- Update OVAL / CVE Definitions
- Device Hardening

3 OPEN ARCHITECTURE

Built on an open, flexible framework with embedded micro services using a Client-Server Model with an integrated journal.

- Cloud / Hybrid / On Premise
- Low Bandwidth / Disconnected
- Best In Class Technical Partners

4 INCIDENT RESPONSE

Instantly respond to threats by executing a cleanup, AV update, and services status check across endpoints in a matter of seconds.

- Flexible Endpoint Targeting
- One-Click Response Actions
- IOC Searches

5 TYCHON JOURNAL

Fully indexed record from every endpoint. Monitor and record endpoint and server activity for near-instant identification of threats.

- Master Endpoint Record
- FIPS 140-2 Compliance
- Netflow & DNS History

6 DYNAMIC DASHBOARDS

Interactive dashboards, which display real-time enterprise compliance metrics for up-to-date situational awareness of network risk.

- Continuous Comply 2 Connect
- Cyber Hygiene
- Zero Trust

7 END USER ENGAGEMENT

A direct line of communication from the incident responder to the desktop of end users.

- Custom Banner & Messages
- Outlook Searching
- User Created/Connected Shares