TYCHON

Enterprise Endpoint Management Use Case

TYCHON Enterprise delivers situational awareness by providing real-time endpoint visibility and the capability to proactively monitor, manage, and validate Cyber Hygiene compliance. Our solution allows organizations to validate security settings at the endpoint in real-time, query specific system(s), remediate vulnerabilities, quarantine systems, and more all from a single console. TYCHON's proactive compliance validation decreases the enterprise attack surface and expands your organization's defense-in-depth.

Benefits

Search

Use natural language questions and PowerShell scripts to query the endpoint. Use interactive dashboards for comprehensive real-time visibility at scale.

Visualize

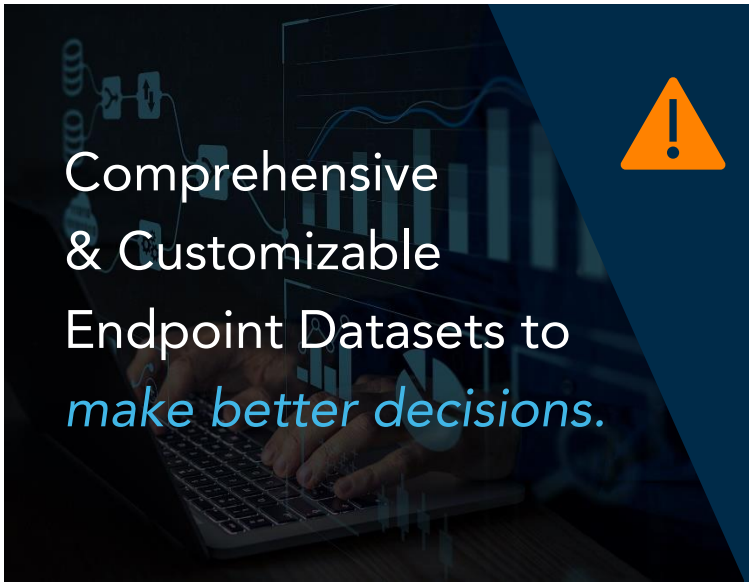
Review automated cyber hygiene data via dynamic, dashboards with accurate reporting on cybersecurity posture and executive level views for leadership.

Remediate

Use custom signatures to flag, notify, and block endpoint activity. Disable unauthorized accounts, quarantine non-compliant systems, and more.

Monitor

Record, index, and actively monitor endpoints in real-time. Review system activity and gather information about process creation, network connections, and more.



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

Do More with TYCHON Enterprise

- Detect Indicators of Compromise (IOCs)
- Generate persistent customizable banners or create one time or recurring tasks to notify users of enterprise actions (quarantines, outbreaks, maintenance).
- Flag and block endpoint activity by file, process, user, and traffic.

725 Jackson Street, Suite 101 I Fredericksburg, VA 22401

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 built 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