TYCHON

Compliance Validation
Use Case

TYCHON Enterprise is an advanced endpoint analytics and remediation platform that delivers situational awareness by providing real-time endpoint visibility and the capability to proactively monitor, manage, and validate Cyber Hygiene compliance. TYCHON delivers this through dynamic interactive dashboards that allow you to validate security settings at the endpoint and query specific system(s) to remediate vulnerabilities, add/remove software, quarantine systems, update patches and more all from a single console. This proactive compliance validation decreases your attack surface and expands your organization's defense-in-depth.

Benefits

Strong Authentication

Remove and disable unauthorized accounts.

Device Hardening

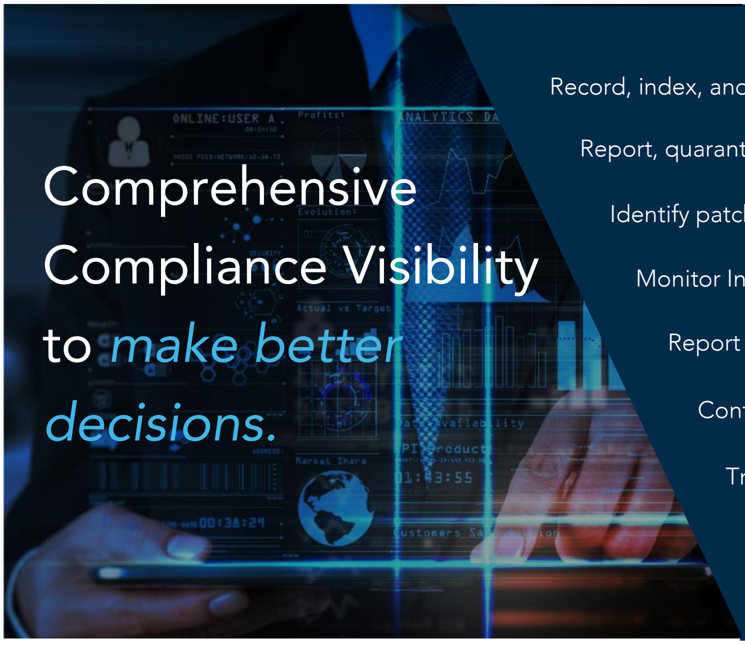
Quarantine non-compliant systems.

Reduced Attack Surface

Remove unauthorized software.

Incident Response

Automated response and polymorphic detection



Comprehensive Compliance Visibility to *make better decisions.*

Record, index, and actively monitor in real-time.

Report, quarantine, and remove outdated operating systems.

Identify patch vulnerabilities and remediate immediately.

Monitor Internet facing webservers inside and outside DMZ.

Report and remove all unauthorized user accounts.

Control standards for installed software and OSs.

Track and enforce proper IA control configurations.

Manage required endpoint security configurations.

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