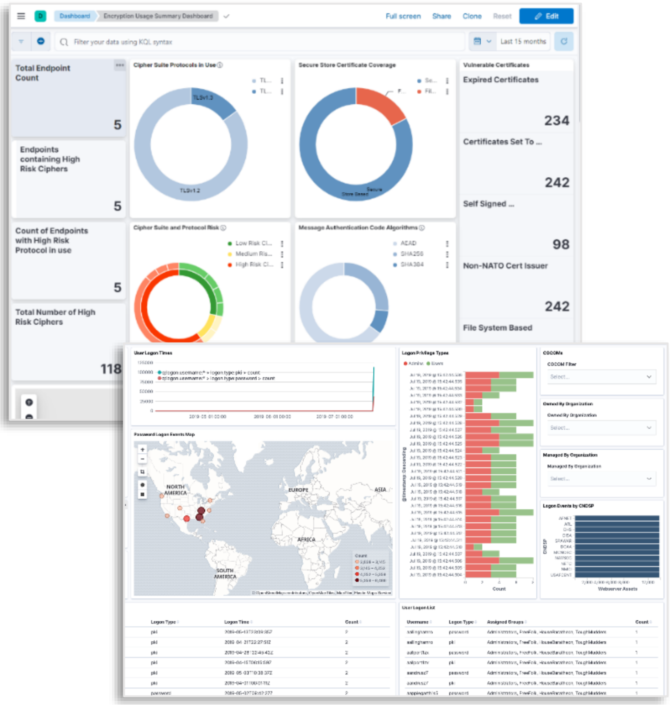
TYCHON

Comply to Connect Use Case

TYCHON Enterprise is an advanced endpoint analytics and remediation platform that aligns to Zero Trust principles. The software delivers real-time endpoint visibility and the capability to proactively monitor, manage, and validate Comply to Connect (C2C) compliance.

TYCHON's dynamic dashboards and streamlined features, enable users to validate security settings, verify users and devices, query endpoint(s), remediate vulnerabilities, add/remove software, quarantine systems, update patches, and more all from a single console. Use proactive validation to strengthen your network access control and decreases your attack surface.



Benefits

Enforcement

Remove and disable unauthorized accounts using strong authentication.

Device Hardening

Monitor for exposures, violations, and escalated privileges.

Reduced Attack Surface

Remove unauthorized software and quarantine non-compliant systems.

Incident Response

Automate reporting, incident response and polymorphic detection.

Key Features

TYCHON SENSOR

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

MESH MODEL

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

OPEN ARCHITECTURE

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

INCIDENT RESPONSE

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

TYCHON JOURNAL

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

DYNAMIC DASHBOARDS

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

END USER ENGAGEMENT

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

Comprehensive C2C Visibility to *defend your network.*

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.