TYCHON

Cyber Hygiene
Use Case

TYCHON Enterprise is an endpoint analytics and remediation platform that enhances your operational resiliency. Manage your system health, reduce vulnerabilities, and improve online security with real-time endpoint visibility, proactive monitoring, and validation via interactive Cyber Hygiene Dashboards.

TYCHON decreases your cyber security risk by enabling you to validate security settings, query specific systems, remediate vulnerabilities, add/remove software, quarantine systems, update patches, and more.

Benefits

Strong Authentication

Enforce your authentication standards by verifying user or device access to secure information.

Reduce Attack Surface

Audit Internet facing, DMZ, and multi-factor based authenticated web servers to ensure policy compliance.

Device Hardening

Ensure endpoints have proper configurations and patches and webservers are within the DMZ.

Incident Response

Quarantine systems in violation of policy, harden settings, and identify unauthorized user accounts.

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 & Customizable Endpoint Datasets to *make better decisions.*

Compliance Enforcement

- Enforce accountability, prevent unauthorized access, and avoid network compromise.

- Proactively address issues through a centrally controlled management solution.

- Prevent exploitation with real-time visibility.

- Ensure situational awareness of network threats and mitigations with interactive, easy to use dashboards.