TYCHON

Endpoint Analytics & Remediation Platform

TYCHON is an endpoint analytics and remediation platform that delivers situational awareness across the enterprise by providing real-time endpoint visibility and the capability to proactively monitor, manage, and validate Cyber Hygiene compliance. TYCHON allows organizations to validate security settings at the endpoint in real-time and 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 and operational resilience.

TAKE CONTROL OF YOUR ENDPOINTS

Search

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

Remediate

Resolve security and compliance issues with a single click. Take advantage of TYCHON custom signatures to flag, notify, and block endpoint activity. Ensure patching compliance, disable unauthorized accounts, quarantine non-compliant systems, and more.

Visualize

Powerful analytics through dynamic dashboards. Review automated cyber hygiene data via dynamic, customizable dashboards with accurate reporting on cybersecurity posture and executive level view for senior leadership.

Monitor

Continuous monitoring to discover vulnerabilities and compliance violations. Record, index, and actively monitor endpoints in real-time. Review system activity and gather information about process creation, network connections, changes to file creation and more.

Low overhead sensor and innovative mesh model enables instant queries
from up to 1 million endpoints at a time

TYCHON SENSOR

Monitor thousands of attributes from every endpoint

TYCHON MESH MODEL

Complete targeted searches in milliseconds

OPEN ARCHITECTURE

Deploy third-party integrations and build custom queries

KEY FEATURES

TYCHON SENSOR

Lightweight agent built on a Micro Service engine framework designed to optimize integration with other third-party security vendors and provide superior data quality. Capture thousands of attributes per endpoint and fulfill use cases, such as systems management, cyber hygiene, and more.

- Logins, Permissions, & Users
- File Meta Data & Integrity
- Installed Software & Settings
- Digital Signatures & Certificates
- Licenses, Drivers, & Versions

MESH MODEL

Instantly query up to a million endpoints. Unique TYCHON components, such as Data Management Node (DMN), File Distribution Center (FDC), Dispatcher, and Orchestrator, are built for scalability and fast query response times.

- Deploy Patches
- Update OVAL / CVE Definitions
- Retrieve Files for Forensics
- Device Hardening
- Reducing Attack Surface

OPEN ARCHITECTURE

TYCHON is built on an open, flexible framework with embedded micro services built using a Client-Server Model with an integrated FIPS 140-2 compliant journal for endpoint data capture. Our custom designed compression algorithm allows data to be sent securely and quickly in any type of network condition, even with low bandwidth restrictions.

- Open, Flexible API Framework
- Embedded Micro Services
- Client-Server Model
- Data Roll-up
- Cloud / Hybrid / On Premise
- Low Bandwidth / Disconnected
- Best In Class Technical Partners

RAPID QUERY

Instantly respond to a new threat or IOC, from any vendor, by executing a cleanup, AV update, and services status check across all connected endpoints in a matter of seconds. Accepts both plain English text and full regular expression (REGEX) queries, and employs fail safe measures to guarantee fast and reliable content delivery.

- Flexible Endpoint Targeting
- One-Click Response Actions
- IOC Searches
- Trace
- Memory Analysis & Forensics
- Two Person Integrity

TYCHON JOURNAL

Fully indexed record from every endpoint. Continuously monitor and record endpoint and server activity for near-instant identification of threats – present or past – and the complete view of an incident, root cause analysis, and tracing of network propagation.

- Master Endpoint Record
- FIPS 140-2 Compliance
- Historical Data
- Historical Running Processes
- Fuzzy Hash
- Netflow & DNS History

DYNAMIC DASHBOARDS

Interactive dashboards, which display real-time enterprise compliance metrics for up-to-date situational awareness of network risk. Vital reports with details on privileged users, web server compliance, asset inventory, system authorization, required security services, patching, and overall organization software compliance.

- Continuous Comply 2 Connect
- Cyber Hygiene
- Compliance Validation
- Resource Utilization
- Strong Authentication
- Zero Trust

TYCHON COMMUNICATOR / END USER ENGAGEMENT

Close the gap between detection and response with a direct line of communication from the incident responder to the desktop of end users using the TYCHON Communicator platform.

- Displays Persistent Banner
- Send Custom Messages
- Outlook Searching
- User Created / Connected Shares