TYCHON

USE CASE: ENTERPRISE ENDPOINT VISIBILITY

CONTACT US
web: tychon.io
email: info@tychon.io

Enterprise Endpoint Visibility (EEV) is essential to eliminate blind spots, expose risks, and protect your network. TYCHON addresses the challenge facing most enterprises to get this visibility in real-time, while balancing reliable, relevant data with a scalable architecture. The TYCHON solution meets this need with the ability to see, manage, and secure every endpoint across the enterprise achieving complete visibility in a multitude of operating environments, with real-time access to endpoint data and granular control of what information is important to you. With a comprehensive list of top questions to ask your enterprise, the ability to quickly see potential areas of risk and take action is easier than ever. Paired with TYCHON's other features, TYCHON provides robust endpoint situational awareness with rapid response.

TYCHON is an endpoint analytics and remediation platform that helps clients search, visualize, remediate, and monitor every endpoint across their enterprise. From compliance monitoring to patch verification, the TYCHON platform manages every layer of endpoint security to keep analysts in control of their network.

BENEFITS

Real-Time Monitoring

Catalog and check against signatures or inquiries using a local endpoint journal.

Historical Tracking

Build timelines of events by questioning journal information.

Ask the Enterprise

Execute frequently asked questions to quickly obtain a range of information.

Find the Anomaly

Investigate suspicious results through robust scripts, fuzzy hashes & more.

Remediation

Remediate findings after asking the question. Found an unwanted process? Kill the process from within the question results.

Automate the Work

Schedule key automation tasks to reoccur so that analysts and operators can perform HUNT operations and defend the network.

TAKE ACTION WITH TYCHON

- Query endpoints using natural language to access asset inventory, utilization data, and more.
- Scan and report on asset data with little to no network impact.
- Create custom query and remediation scripts.
- Access near real-time data on patches, versions, logon statistics, and other compliance metrics.

TYCHON

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