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, the TYCHON endpoint analytics and remediation platform provides robust endpoint situational awareness with rapid response.

TYCHON is a software company that develops advanced endpoint analytics and remediation technology that enables commercial and government organizations to bridge the gap between security and IT operations. TYCHON participates in McAfee's Security Innovation Alliance and TYCHON is engineered using the software development kits for McAfee ePO and leverages the Data Exchange Layer (DXL) and other messaging fabrics.

CAPABILITIES

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

REAL-TIME INCIDENT RESPONSE

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.

- Efficient IOC Searches
- One-Click Response Actions
- Two Person Integrity
- Target Endpoint by System Tree
- Netflow
- Trace

CYBER HYGIENE 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.

- Strong Authentication
- Zero Trust
- Device Hardening
- Reducing Attack Surface
- Improved Detection and Response to Attacks

END USER ENGAGEMENT - TYCHON COMMUNICATOR

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. Send custom messages to one, some or all users (e.g. inform users that their machines are temporarily quarantined.)

- Displays Persistent Banner
- Send Custom Messages to any Endpoint

TYCHON ENDPOINT 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.

- FIPS 140-2 Compliance
- Historical Data
- Compressed Messaging to Reduce Bandwidth
- Fuzzy Hash
- Netflow

API INTEGRATION

TYCHON's robust set of APIs makes integration with other endpoint or network capabilities straightforward and rapid via custom content creation, expanding data recording fields, and more.

- External Server Feeds
- DXL, Open DXL, Kafka
- SIEM Feeds
- API/SDK

ARCHITECTURAL FEATURES

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 Framework
- Embedded Micro Services
- Client-Server Model
- Data Roll-up
- No Scans required
- Targeting System Efficiencies

TECHNICAL PARTNERS

TYCHON partners with the best in class industry leaders and service providers to provide enriched endpoint data that is visible, accessible, understandable, trusted, interoperable, and secure.

- McAfee
- Elastic
- Palo Alto
- ThreatQ and more