# TYCHON

## USE CASE OVERVIEW

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

**TYCHON** is an advanced enterprise endpoint management platform designed to be the 'gold source' for enterprise endpoint data. TYCHON provides complete **Enterprise Endpoint Asset Visibility**, **Automated Continuous Endpoint Monitoring (ACEM)**, dynamic **Cyber Hygiene Dashboards**, and enterprise query and response to its customers at unparalleled speed and scale.

TYCHON's automated Cyber Hygiene Dashboards deliver instant visibility of critical cyber security situational awareness and policy violations in vital areas to include privileged users, Web PKI/authentication and DMZ, asset inventory, system authorization, security services, patching, and overall organizational software compliance.

## BUSINESS USE CASES

TYCHON's unique features address the following business needs:

### AUTOMATED CONTINUOUS ENDPOINT MONITORING

Automate the Cyber Hygiene Dashboards and achieve real-time visibility and control of every endpoint across the enterprise.

### CONFIGURATION MANAGEMENT

Unify and streamline your asset identification, software inventory, endpoint configuration management, and real-time compliance tracking.

### CYBER HYGIENE

Instant visibility of critical cyber security policy violations, encompassing vital security areas such as software patches, compliance, privileged users, and more with one centralized view of critical information.

### SECURITY OPTIMIZATION

Secure enterprises with a powerful customizable tool suite for advanced persistent threats (APT), polymorphic-malware identification, asset inventory, file discovery, root cause analysis, and system forensics.

### COMPLIANCE VALIDATION

Achieve situational awareness across the enterprise with real-time endpoint visibility and the capability to proactively monitor, manage, and validate Cyber Hygiene compliance using dynamic interactive dashboards.

### ENDPOINT DETECTION & RESPONSE (EDR)

Proactively identify suspicious activities with robust anomaly detection and endpoint visibility using custom scripts, fuzzy hashes, questions, and WMI queries.

# 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