# TYCHON

## USE CASE: CONFIGURATION MANAGEMENT

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

TYCHON provides enterprises with a streamlined user experience for asset identification, software inventory, endpoint configuration management, real-time compliance tracking, managing software installations, rapidly deploying security updates, preparing OS system migrations, interactive end user notifications, and system resource utilization. Our solution provides a complete and real-time view of endpoints across the enterprise, enabling your staff to scale further, improve effectiveness, identify issues, remediate known vulnerabilities, add or remove software, and patch out-of-date software all from a single console.

TYCHON is a software company that develops advanced enterprise endpoint management 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 the TYCHON Enterprise Endpoint Management Platform is engineered using the software development kits for McAfee ePO and leverages the Data Exchange Layer (DXL) and other messaging fabrics.

## CAPABILITIES

### Two Party Authorization

Secure advanced features and actions by requiring two party approval

### Visibility

Record, index, and actively monitor endpoints locally in real-time.

### Roll Up Reporting

Leverage TYCHON to quickly and easily generate roll up reports

### Remediation

Alleviate risk using a proactive vulnerability mitigation platform

### Context Triggered Piecewise Hashing

Generate, record, and index a fuzzy hash of all files on disk

### Host Based Endpoint Journal

Benefit from always-on monitoring and indexing with DVR-like capability

## TAKE ACTION WITH TYCHON

- Better understand and secure the environment of your enterprise with a single console.
- Automate day-to-day systems management processes and eliminate the human element.
- Take one-click actions to uninstall applications, quarantine machines, and find similar files.
- Do more with less. Streamline your internal operations by:
  - Identify and retire or eliminate outdated or unused software and tools, and orphaned or disconnected servers
  - Identify candidate servers for virtualization
  - Save money on audits, staffing, maintenance fees, training, and software licensing
  - Uninstall applications
  - Migrate with ease to new software applications or operating systems.

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