

# TYCHON

## USE CASE: SECURITY OPTIMIZATION

### CONTACT US

**web:** [tychon.io](http://tychon.io)

**email:** [info@tychon.io](mailto:info@tychon.io)

TYCHON secures enterprises with a powerful customizable tool suite for advanced persistent threats (APT) and polymorphic-malware hunting, asset identification, file discovery, root cause analysis, and system forensics. Arming you with speed, scale, capacity, and performance at previously unattainable levels, TYCHON continuously monitors and records client and server endpoint activity for real-time identification of threats. These tools provide a complete view of an incident (present or past), its cause, and the ability to trace network propagation, 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 the Data Exchange Layer (DXL).

### CAPABILITIES



#### Security Optimization

Leverage TYCHON to gain access to an array of insights about endpoints



#### McAfee Integration

Benefit from a single-entry point for centralized control of your assets



#### Script Repository

Customize your environment and simplify the process of working with vendors to ensure compliance



#### Endpoint Control

Gain enterprise control from a central console across multiple domains on or off the network

### TAKE ACTION WITH TYCHON

- Get the complete view of current security posture and stay up to date on the status of your endpoints.
- Deploy patches, modify security settings, and enable/disable services all with a single click.
- Take one-click action to:
  - Quarantine Machines
  - Kill Processes
  - Delete Files
  - Enforce Policy
  - Hunt for Threats
  - Uninstall Applications
  - Manage Asset Compliance
  - Monitor Event Logs
  - Feed data to Splunk® ArcSight™, McAfee® ESM, TIE, and ATD in real time
  - Ingest data from third party databased and cloud services

## 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

### AUTOMATED DOD CYBER HYGIENE SCORECARD

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 PKI and DMZ, asset inventory, system authorization, HBSS/ESS Services, patching and overall organization software compliance.

- ▶ Strong Authentication
- ▶ 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 Journaling for Polymorphic Detection

### PARTNER 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 and Open DXL
- ▶ SIEM/ESM Feeds
- ▶ API/SDK

### ARCHITECTURAL FEATURES

The TYCHON architecture was built using a Client-Server Model with a 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.

- ▶ Client-Server Model
- ▶ CSC and Data Roll-up
- ▶ No Scans required
- ▶ Targeting System Efficiencies

### MCAFEE INTEGRATION

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 the Data Exchange Layer (DXL).

- ▶ ePO: Single Pane of Glass, Centralized Control, Data Roll-up Support, Policy Enforcement, Access Control
- ▶ DXL: Sharing Information with other Vendors