TYCHON

ENTERPRISE ENDPOINT MANAGEMENT

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

TYCHON's Enterprise Endpoint Management Platform delivers situational awareness across the enterprise by providing real-time endpoint visibility and the capability to proactively monitor, manage, and validate Cyber Hygiene compliance. TYCHON delivers this through dynamic products that allow organizations to validate security settings at the endpoint in real-time and query specific system(s), remediate vulnerabilities, add/remove software, quarantine systems, update patches and more all from a single console. TYCHON's proactive compliance validation decreases the enterprise attack surface and expands your organization's defense-in-depth and operational resilience.

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).

TYCHON PLATFORM

TYCHON Core

Host Firewall Orchestrator: Simplifies HIPS/ENS firewall administration and whitelisting

Host Sentinel Security: Detection and hunting platform with custom signatures.

Communicator: Communicate directly with your users via mass notifications

TYCHON Rapid Query

Incident Response: Use common questions, WMI queries and PowerShell scripts to query endpoints and perform remediation.

Automated DoD Cyber Hygiene Dashboards: View interactive dashboards with real-time enterprise compliance metrics with pivotable configurations and data export capability

TYCHON Endpoint

Continuously monitor endpoint and server activity for instant identification of threats and complete view of an incident, root cause analysis, and tracing of network propagation.

TYCHON Data Collector

An optional data ingestion engine for endpoint information. Use it to receive all endpoint data from DXL brokers and unburden the ePO from endpoint DXL traffic.

DO MORE WITH TYCHON

- Detect Indicators of Compromise (IOCs)
- Generate persistent customizable banners or create one time or recurring tasks to notify users of enterprise actions (system quarantine, possible outbreaks, maintenance activities).
- Flag, notify, and block endpoint activity by file, process, user, and traffic.

725 Jackson Street, Suite 101 I Fredericksburg, VA 22401

McAfee COMPATIBLE

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

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
- Trace

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