TYCHON

USE CASE OVERVIEW

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

Tychon LLC is a software company founded by former U.S. Department of Defense (DoD) cybersecurity experts. The TYCHON Enterprise Endpoint Management Platform was born from their vision to break down the silos between IT management and security operations teams to provide real-time visibility across all enterprise endpoints. The TYCHON Enterprise Endpoint Management Platform enables these groups to work from a single data set displayed through dynamic dashboards, known as the Automated DoD Cyber Hygiene Scorecard, that are drillable and provide instant access to the answers needed with speed, scale, accuracy, capacity, and performance at previously unattainable levels. 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).

BUSINESS USE CASES

TYCHON's unique features address the following business needs:

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.

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.

ENTERPRISE ENDPOINT VISIBILITY (EEV)

Eliminate blind spots, expose risks, and protect your network leveraging TYCHON's real-time monitoring, historical data tracking, and Rapid Query features.

CONFIGURATION MANAGEMENT

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

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.

ENDPOINT DETECTION & RESPONSE (EDR)

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

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
- Netlfow
- 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

McAfee
COMPATIBLE