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, quarantine systems, 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 leverages the Data Exchange Layer (DXL) and other messaging fabrics.

TYCHON CAPABILITIES

Investigate

Use natural language questions and PowerShell scripts to query the endpoint. Use interactive dashboards for comprehensive real-time visibility.

Respond

Take advantage of one-click remediation and TYCHON custom signatures to flag, notify, and block endpoint activity.

Monitor

Record, index, and actively monitor endpoints in real-time. Review system activity and gather information about process creation, network connections, changes to file creation and more.

Enforce

Ensure patching compliance and remediate issues when discovered. Disable unauthorized accounts, quarantine non-compliant systems, remove unauthorized software, and more.

Hunt

Investigate suspicious results using robust scripts, fuzzy hashes and more.

Communicate

Communicate directly with your users with persistent customizable desktop banners and popup messages.

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.

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