TYCHON

COMPLIANCE VALIDATION

TYCHON's Endpoint Security Suite 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 interactive dashboards that allow organizations to validate security settings at the endpoint in real-time and query specific system(s) to 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.

TYCHON is a software security 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 product suite is engineered using the software development kits for McAfee ePO and the Data Exchange Layer (DXL).

COMPLIANCE VISIBILITY

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

Account Auditing
Report and remove all unauthorized accounts

System Authorization
Report, quarantine, and remove outdated operating systems

Baseline Compliance
Control standards for installed software and operating systems

Properly Patched Systems
Identify patch vulnerabilities with the capability to remediate instantaneously

Computer Configuration
Track and enforce proper IA control configurations

Web-Server Configurations
Monitor internet facing webservers inside and outside approved DMZ

Required Security Modules
Manage endpoint required security module configuration

TYCHON COMPLIANCE ENFORCEMENT

▶ Strong authentication – Remove and disable unauthorized accounts
▶ Device hardening – Quarantine non-compliant systems
▶ Reduce attack surface – Remove unauthorized software
▶ Detection and response to adversary activity – Automated response and polymorphic detection

McAfee® COMPATIBLE

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

CYBER HYGIENE SCORECARD 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 PKI and DMZ, asset inventory, system authorization, HBSS 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 even with low bandwidth restrictions.

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

MCAFEE INTEGRATION

TYCHON is engineered in partnership with the McAfee Security Innovation Alliance and is exclusively developed using the SDKs for McAfee ePO and DXL. TYCHON is thoroughly tested, authorized and digitally signed by McAfee as 'McAfee Compatible'.

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