TYCHON

USE CASE:
PATCH MANAGEMENT

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

TYCHON is an advanced endpoint analytics and remediation platform helps clients search, visualize, remediate, and monitor every endpoint across their enterprise.

When TYCHON identifies systems as vulnerable to a CVE, TYCHON can **deploy patches** to endpoints to mitigate the vulnerability. TYCHON uses a **three-stage approach** to patch management, providing corrective options and ensuring that only systems that need a patch receive it. Stage 1 is Validation. During Validation, TYCHON determines if a system is unpatched or applicable to a vulnerability. Stage 2 is Deployment and Installation, whereby patch binaries or **workarounds** are customized to fit the specific needs of each customer and automatically deployed based on the results of the vulnerability check. Finally, Stage 3 is Rollback, where, if problems arise from the binary installation or workaround deployed, they can be reversed/uninstalled.

TYCHON is specifically designed and developed to provide comprehensive enterprise endpoint asset visibility and automated continuous endpoint monitoring. From compliance monitoring to patch verification, the TYCHON platform manages every layer of endpoint security to keep analysts in control of their network.

BENEFITS

Detect & Deploy

Utilize Vulnerability Management to detect system vulnerabilities and deploy patches.

Validate & Enforce

Ensure patch compliance and remediate issues when discovered.

Rollback

Take advantage of feature flexibility by rolling back patches if necessary.

Manage

Identify vulnerabilities and deploy patches throughout your enterprise within a single managed interface.

Customize

Configure your patch solution to meet the needs of variable requirements.

Schedule

Maintain compliance by scheduling future patch efforts throughout your enterprise.

TAKE ACTION WITH TYCHON

- Zero day resolutions with the option to deploy workarounds before patches when necessary.
- Efficient tool designed to function with minimal network impact.
- Flexibility to deploy patches manually or automatically.
- Aligns to CVEs, IAVAs, and KBs.

TYCHON

KEY FEATURES

TYCHON SENSOR

Lightweight agent built on a Micro Service engine framework designed to optimize integration with other third-party security vendors and provide superior data quality. Capture thousands of attributes per endpoint and fulfill use cases, such as systems management, cyber hygiene, and more.

- Logins, Permissions, & Users
- File Meta Data & Integrity
- Installed Software & Settings
- Digital Signatures & Certificates
- Licenses, Drivers, & Versions

MESH MODEL

Instantly query up to a million endpoints. Unique TYCHON components, such as Data Management Node (DMN), File Distribution Center (FDC), Dispatcher, and Orchestrator, are built for scalability and fast query response times.

- Deploy Patches
- Update OVAL / CVE Definitions
- Retrieve Files for Forensics
- Device Hardening
- Reducing Attack Surface

OPEN ARCHITECTURE

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 API Framework
- Embedded Micro Services
- Client-Server Model
- Data Roll-up
- Cloud / Hybrid / On Premise
- Low Bandwidth / Disconnected
- Best In Class Technical Partners

RAPID QUERY

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, and employs fail safe measures to guarantee fast and reliable content delivery.

- Flexible Endpoint Targeting
- One-Click Response Actions
- IOC Searches
- Trace
- Memory Analysis & Forensics
- Two Person Integrity

TYCHON 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.

- Master Endpoint Record
- FIPS 140-2 Compliance
- Historical Data
- Historical Running Processes
- Fuzzy Hash
- Netflow & DNS History

DYNAMIC 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.

- Continuous Comply 2 Connect
- Cyber Hygiene
- Compliance Validation
- Resource Utilization
- Strong Authentication
- Zero Trust

TYCHON COMMUNICATOR / END USER ENGAGEMENT

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.

- Displays Persistent Banner
- Send Custom Messages
- Outlook Searching
- User Created / Connected Shares