

# TYCHON

## Attack Surface Management

Attack Surface Management is the continuous discovery, monitoring, evaluation, and remediation of attack surfaces within an organization. Your attack surface is defined as any asset within your interconnected network that could be leveraged by an attacker. TYCHON, an advanced endpoint analytics and remediation platform specifically designed to provide comprehensive enterprise endpoint asset visibility and automated continuous endpoint monitoring, is a powerful Attack Surface Management tool. Leveraging TYCHON, our users can search, visualize, remediate, and monitor every endpoint across their enterprise. From asset discovery to one-click remediation, the TYCHON platform manages every layer of endpoint security to keep analysts in control of their network and minimize attack surface risk.

### BENEFITS



#### Discover

Identify, classify, and assess all your organization's assets, including shadow IT, using natural language questions and automated dashboards.



#### Monitor

Continuously monitor your assets to discover exposures, compliance violations, unknown assets, and more as your attack surface changes.



#### Evaluate/Prioritize

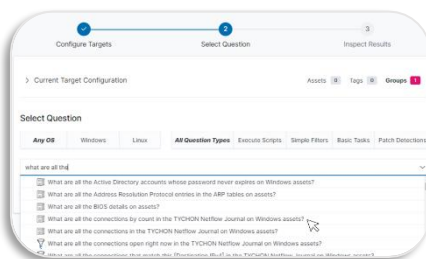
Use built in analytics, reports, and automated dashboards to analyze individual assets, evaluate risk levels, and prioritize remediation actions.



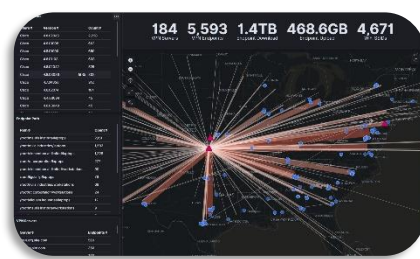
#### Remediate

Take advantage of one-click remediations to ensure patch compliance, disable unauthorized accounts, quarantine non-compliant systems, and more.

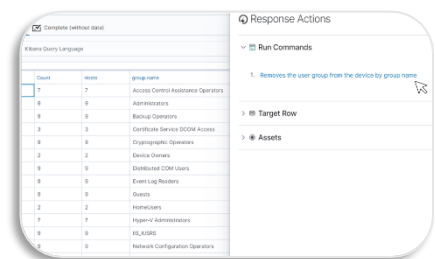
### TAKE ACTION WITH TYCHON



Easy to Use



Powerful Analytics



Speed & Accuracy

## 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