TYCHON

USE CASE OVERVIEW

TYCHON is an advanced endpoint analytics and remediation platform designed to be the 'gold source' for enterprise endpoint data. TYCHON provides complete **Enterprise Endpoint Asset Visibility**, **Automated Continuous Endpoint Monitoring**, dynamic **Cyber Hygiene Dashboards**, and enterprise query and response to its customers at unparalleled speed and scale. TYCHON's automated Cyber Hygiene Dashboards deliver instant visibility of critical cyber security situational awareness and policy violations in vital areas to include privileged users, Web PKI/authentication and DMZ, asset inventory, system authorization, security services, patching, and overall organizational software compliance.

BUSINESS USE CASES

Attack Surface Management

Continuous discovery, monitoring, evaluation, and remediation.

Auto. Continuous Endpoint Monitoring

Automate the Cyber Hygiene Dashboards to achieve real-time control of every endpoint.

Compliance Validation

Achieve situational awareness across the enterprise with real-time visibility.

Configuration Management

Unify and streamline endpoint configuration management and real-time compliance tracking.

Cyber Hygiene

Enhance operational resiliency with instant visibility of critical cyber security violations.

Enterprise Endpoint Management

Search, visualize, remediate, and monitor every endpoint across the enterprise.

Incident Response & Hunt Operations

Proactively identify suspicious activities with robust anomaly detection

Patch Management

Deploy customizable patches to endpoints to mitigate vulnerabilities.

Security Optimization

Secure your enterprise with a powerful customizable tool suite.

Vulnerability Management

Detect attack surface exposures and system vulnerabilities with efficient delta-based model.

TYCHON

ATTACK SURFACE MANAGEMENT

Leverage TYCHON to achieve continuous discovery, monitoring, evaluation, and remediation of attack surfaces. Use built in analytics, reports, and dashboards to analyze assets, evaluate risk levels, and prioritize remediation actions.

- Classify and Assess Assets
- Discover Exposures
- Evaluate Risk Levels
- Prioritize Remediations

AUTOMATED CONTINUOUS ENDPOINT MONITORING

TYCHON fully automates 100% of the DoD Cyber Hygiene Scorecard in compliance with DoD OPORD 16-0080. TYCHON's Rapid Query (RQ) feature provides real-time visibility and control of every endpoint across the enterprise to provide robust endpoint situational awareness.

- Automated Scorecard
- Quick Remediation
- Ensure HBSS/ESS Compliance
- Executive Level Views

COMPLIANCE VALIDATION

Achieve complete compliance visibility by recording, indexing, and monitoring endpoints in real-time, quarantining outdated operating systems, identifying patch vulnerabilities, monitoring Internet facing webservers inside and outside approved DMZ, removing unauthorized accounts, controlling standards for baseline compliance, enforcing proper IA control configurations, and managing endpoint required security modules.

- System Authorization
- Properly Patched Systems
- Webserver Configuration
- Account Auditing
- Baseline Compliance
- Computer Configuration
- Security Modules

CONFIGURATION MANAGEMENT

TYCHON offers a streamlined user experience for asset identification, software inventory, endpoint configuration management, real-time compliance tracking, managing software installations, rapidly deploying security updates, preparing OS system migrations, interactive end user notifications, and system resource utilization all from a single console.

- Two Party Authorization
- Roll Up Reporting
- Context Triggered Piecewise Hashing
- Proactive Remediation
- Host Based Endpoint Journal

CYBER HYGIENE

Manage your system health, reduce vulnerabilities, and improve online security with real-time endpoint visibility, proactive monitoring, and validation through Cyber Hygiene Dashboards. Decrease cyber security risk by allowing organizations to validate security settings at the endpoint in real-time and query specific systems to remediate vulnerabilities, add/remove software, quarantine systems, update patches, and more.

- Strong Authentication
- Device Hardening
- Reduce Attack Surface
- Detection & Response
- Enforce Accountability
- Centrally Controlled Solution
- Real-Time Visibility

TYCHON

ENTERPRISE ENDPOINT MANAGEMENT

Retrieve intelligence from endpoints at speed and scale using natural language questions and PowerShell scripts. Use interactive dashboards for comprehensive real-time visibility and resolve security and compliance issues. Employ continuous monitoring to discover vulnerabilities and compliance violations in real-time.

- Search
- Visualize
- Remediate
- Monitor

INCIDENT RESPONSE & HUNT OPERATIONS

Proactively identify suspicious activities, providing more robust anomaly detection and endpoint visibility. Remove security blind spots on your network by identifying high risk vulnerabilities and exploits using natural language queries and customizable content.

- Complete View of Current Security Posture
- Communicate with Partners
- Always-On Monitoring with DVR-like capability

PATCH MANAGEMENT

Identify systems as vulnerable to a CVE and deploy patches to mitigate the vulnerability using a three-stage approach to patch management. 1) Validate - determine if a system is unpatched or applicable to a vulnerability. 2) Deploy & Install - customize patch binaries or workarounds to fit the specific needs. 3) Rollback - if problems arise from the binary installation or workaround deployed, they can be reversed/uninstalled.

- Detect & Deploy
- Validate & Enforce
- Rollback Flexibility
- Customizable Solution
- Schedule Future Patches

SECURITY OPTIMIZATION

Powerful customizable tool suite for advanced persistent threats (APT) and polymorphic-malware hunting, asset identification, file discovery, root cause analysis, and system forensics. Continuously monitor and record client and server endpoint activity for real-time identification of threats, providing a complete view of an incident (present or past), its cause, and the ability to trace network propagation, all from a single console.

- Security Optimization
- Script Repository to Customize & Simplify
- Endpoint Control

VULNERABILITY MANAGEMENT

Monitor all vulnerabilities with a CVE number starting from Year 2012, using OVAL and XCCDF. Run checks on customizable days and times and feed the results into the central database where it is analyzed. See the state of a CVE by a multitude of search types which include the CVE ID, IAVA, Severity, and more.

- Delta-Based Model to Reduce Scan Times
- Customizable Targeting
- Risk Analysis to Eliminate Exposures & Uncertainty