TYCHON

CYBER SCORECARD (CSC)

Tychon offers interactive dashboards, which display enterprise metrics with data export capabilities. This feature, known as Tychon Cyber Scorecard (CSC), provides up-to-date situational awareness of risks to the network. CSC delivers instant visibility of critical cyber security policy violations. It encompasses vital security areas such as software patches, system compliance, user logon statistics, and more. This centralized view of critical information enables operators to monitor endpoint compliance in near real-time.

WHY TYCHON?

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.

The Tychon product suite is engineered in partnership with the McAfee® Security Innovation Alliance and is exclusively developed using the SDKs for McAfee® ePO and Data Exchange Layer (DXL).
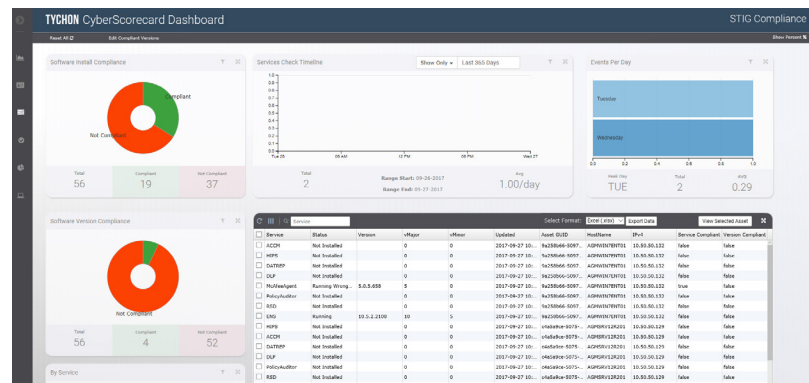
Business Use Cases Include:

- Security Optimization
- Systems Management
- Enterprise Endpoint Visibility (EEV)
- Endpoint Detection & Response (EDR)
- Cyber Scorecard (CSC)

CAPABILITIES

The Tychon Cyber Scorecard feature is made up of six individual dashboards, each with their own interactive graphs and statistics.

- Running Processes
- Windows Registry
- Outlook Email

- Network Activity
- Installed Products
- Startup & Services

In addition, Tychon offers a Cyber Scorecard Summary page which provides a rollup view of the top ten performance metrics on one screen.

McAfee®
COMPATIBLE

TYCHON

CLEAR QUESTIONS. STRAIGHT ANSWERS. QUICK RESPONSE.

EASY TO USE

Simple navigation and a centralized location for information

Interactive charts and graphs, allowing you to easily filter results to quickly identify issues

Customizable views and easy access to data filters, such as compliant versions or DMZ ranges

Exportable views of detailed data to identify problems and immediately act against threats

PRODUCT FEATURES

Fully Indexed Record of Every Endpoint with Tychon Host Based Journal™

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. Fully indexed, FIPS 140-2 encrypted record of each endpoint (144 data points over 12 journal groups) requiring only 30mb yearly on average.

Automatic Response with Tychon RapidQuery™

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.

End User Engagement with 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).

Application Communication Whitelisting with Tychon Host Firewall Orchestrator™

Fully leverage McAfee HIPS and whitelist your entire application portfolio using the intelligent three-step wizard. Tychon simplifies HIPS administration and delivers defense-in-depth by minimizing the attack surface and mitigating data exfiltration.

Vulnerability and Patch Remediation

Includes full support for distributing software patches to Windows, Mac, and Linux machines and remediate known vulnerabilities enterprise-wide in seconds.

McAfee Data Exchange Layer (DXL) Integration

DXL has extended Tychon by providing a means for near-instantaneous global communication with endpoints and the ability to scale across enterprise wide deployments.

Third-Party Application Integration with DXL

Tychon broadcasts messages across DXL that can be picked up and acted on by third-party applications and appliances that also communicate across the DXL fabric. These can range from NAC appliances or firewalls to SIEM and beyond, opening a world of new possibilities for automation and autonomous action.