

# TYCHON

## SYSTEMS MANAGEMENT

Tychon provides enterprises with a unified and 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. Our solution provides a complete and real-time view of endpoints across the enterprise, enabling your staff to scale further, improve effectiveness, identify issues, remediate known vulnerabilities, add or remove software, and patch out-of-date software all from a single console.

### 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

**Asset Visibility through RapidQuery:** Tychon records, indexes, and actively monitors endpoints locally in real-time. Endpoint events and data continuously recorded by Tychon are completely configurable and include:

- Running Processes
- Windows Registry
- Outlook Email
- Network Activity
- Installed Products
- Startup & Services
- Kernel Drivers
- Adapters
- Files & Hashes
- Event Logs
- User/Group Accounts
- Fuzzy Hash

**Host Based Endpoint Journal:** Tychon has a DVR-like capability for client or server, physical or virtual endpoints that provides an always-on endpoint monitoring, recording, and indexing capability.

**Context Triggered Piecewise Hashing (Fuzzy Hash):** Tychon generates, records, and indexes a fuzzy hash of all files on disk providing comprehensive searching and rapid termination for variants of IOCs and vulnerabilities yet to be discovered.

**Remediation:** Tychon provides a proactive vulnerability mitigation platform that alleviates risk by informing users with an actionable dashboard of the wellness of the enterprise.

## TAKE ACTION WITH TYCHON

- Better understand and secure the environment of your enterprise with a single console.
- Automate day-to-day systems management processes and eliminate the human element.
- Take one-click actions to uninstall applications, quarantine machines, and find similar files.
- Do more with less. Streamline your internal operations by:
  - Identify and retire or eliminate outdated or unused software and tools, and orphaned or disconnected servers
  - Identify candidate servers for virtualization
  - Save money on audits, staffing, maintenance fees, training, and software licensing
  - Uninstall applications
  - Migrate with ease to new software applications or operating systems

## 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.