TYCHON

ENTERPRISE DETECTION & RESPONSE (EDR)

Tychon offers Endpoint Detection and Response (EDR) capabilities necessary to strengthen your endpoint security solution. Our EDR solution allows security analysts to proactively identify suspicious activities, providing more robust anomaly detection and endpoint visibility. When it comes to security, information is key and real-time information is critical for protecting your network. Remove security blind spots on your network by identifying high risk vulnerabilities and exploits using natural language queries and customizable content. Tychon, with McAfee's Security Suite®, offers a comprehensive and integrated EDR solution with automation, taking security to the next level.

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

Ask the Enterprise: Through Tychon RapidQuery execute on a list of frequently asked questions to quickly obtain a wide range of information:

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

Find the Anomaly: Further investigate suspicious results through robust custom scripts, fuzzy hashes, advanced questions, and WMI queries.

Take Action: Remediate findings after asking the question. Found an unwanted process? Kill the process from within the question results.

Automate the Work: Schedule key questions to reoccur so that analysts and operators can be freed up to perform HUNT operations and defend the network. With Cyber Scorecard user logons, Windows patch status, system configuration compliance, and web server compliance are automatically reported back and presented in an easy to consume interface.

Unify the Stack: Leveraging DXL, Tychon communicates with other OpenDXL partners and allows for autonomous, rapid, and robust responses taking security operations to the next level. Detected threats can trigger automatic endpoint isolation, remediation, and user notification.

TYCHON

CLEAR QUESTIONS. STRAIGHT ANSWERS. QUICK RESPONSE.

TAKE ACTION WITH TYCHON

- Query endpoints using natural language to access asset inventory, utilization data, and more.
- Scan and report on asset data with little to no network impact.
- Create custom query and remediation scripts.
- Access near real-time data on patches, versions, logon statistics, and other compliance metrics.

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.