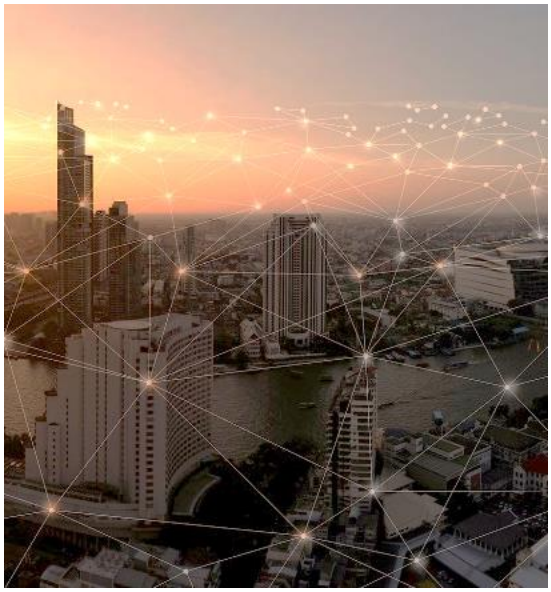
TYCHON

Vulnerability & Patch Management

Use Case



TYCHON Enterprise monitors all vulnerabilities with Common Vulnerability and Exposures (CVE) numbers starting from 2012 up to the current day, using Open Vulnerability and Assessment Language (OVAL). It is a customizable solution that lets you detect and monitor up to date vulnerabilities, then remediate issues with robust patching capabilities.

- **Flexible:** TYCHON Security Content Automation Protocol (SCAP) scan engine runs configurable checks and feeds the results into the central database where it is analyzed.
- **Efficient**: The engine leverages a delta-based model which minimizes scan time by only monitoring unpatched vulnerabilities, reducing network resource use.
- **On Demand**: At any point in time, a user can see the state of a CVE by CVE ID, IAVA, Severity, Risk Score and/or release date via dashboards or queries.

Vulnerability Capabilities

Detect

Identify attack surface exposures to detect system vulnerabilities.

Monitor

Focus on deltas to reduce required check and minimize network impact.

Customize

Target a full array of vulnerabilities to address critical issues earlier.

Visualize

Maintain complete visibility using dashboards to assess vulnerabilities.

Enforce

Remediate issues from a single tool using TYCHON Patch Management.

Risk Analysis

Assess you network with TYCHON's risk analysis to identify exposures.

725 Jackson Street, Suite 101 I Fredericksburg, VA 22401

tychon.io | info@tychon.io

PATCH CAPABILITIES

Manage

Identify vulnerabilities and deploy patches within a single managed interface.

Rollback

Take advantage of feature flexibility by rolling back prior patches if necessary.

Customize

Configure your patch solution to meet the needs of variable requirements.

Schedule

Maintain compliance by scheduling future patches throughout your enterprise.

TYCHON APPROACH TO PATCH MANAGEMENT

When TYCHON identifies systems as vulnerable to a CVE, it can deploy patches to endpoints. TYCHON uses a three-stage approach to patch management, providing corrective options and ensuring that only systems that need a patch receive it.

1. Validation: TYCHON determines if a system is unpatched and/or vulnerable.
2. Deployment and Installation: Where patch binaries or workarounds are customized and automatically deployed based on the results of the vulnerability check.
3. Rollback: If problems arise from the binary installation, it can be reversed/uninstalled.

This comprehensive approach, combined with TYCHON's other valuable features, enables you to manage every layer of endpoint security and stay in control of your network.