readyworks

Cybersecurity Threat Assessment

THE PROBLEM: Manual processes for IT asset lifecycle management (ITALM) expose companies to cybersecurity risks.

To reduce the risk of cyber-attacks, IT teams require complete visibility of assets from "cradle to grave." They need a real-time view of hardware, where it is located, who is using it, associated applications, OS versions, and how data is being handled. They need to stay on top of OS updates and patching, as well as end of support for servers and devices. Failure to update these systems leaves companies open to data breaches and ransomware attacks. For regulated industries like financial services and healthcare, these breaches can also result in multi-million-dollar fines from regulators.

Unfortunately, most companies are still applying manual processes and mountains of spreadsheets to ITALM, which significantly increases the risk of missing security vulnerabilities and mitigating risks quickly.

THE SOLUTION: READYWORKS

ReadyWorks, a digital platform conductor, integrates data from all your IT and business systems to identify security risks including missing patches, end-of-life systems, missing agents, and misconfigurations. ReadyWorks uses this information to orchestrate workflows to minimize the risk of cybersecurity attacks.

BUSINESS IMPACT:

- **Improved security:** Identify security vulnerabilities and ensure all hardware is accounted for and all systems are up to date.
- **Improved compliance:** Ensure compliance with industry regulations and internal policies. This is particularly important for businesses in regulated industries such as healthcare, finance, and government.
- **Lower costs:** Automated data integration reduces labor costs to identify and mitigate security risks.
- **Risk avoidance:** Reduce the risk of sensitive data being exposed or ransomware attacks that can harm your company's reputation and result in significant financial impacts.

readyworks

WITH READYWORKS:

- Merge data from all sources to gain a real-time view of hardware, where it is located, who is using it, associated applications, OS and software versions, configuration settings, and how data is managed.
- Quickly identify vulnerable devices that require a security patch. Identify which patches need to take priority and receive immediate attention.
- Identify EOL systems and automate migration and decommissioning workflows.
- Confidently respond to security and compliance audits with highly accurate, validated, asset data.
- Automate workflows to communicate and enforce security policies.
- Identify missing devices or ones that need to be returned and automate workflows to address these devices.
- Orchestrate workflows to ensure proper handling of devices that are being decommissioned and/or disposed of.

WHAT'S INCLUDED:

- Bi-directional connectors to collect asset information from data-sources including, CMDBs, global policy systems, configuration platforms, identity management systems, ITSM tools, and security alert systems. (10 connectors included in standard subscription.)
- Outbound orchestration to update source systems of record.
- Automated workflows for patch management and migration of EOL systems.
- Automated workflows to notify stakeholders of cybersecurity threat scenario.
- Automated workflows for escalations on security violations.
- Communication templates to device owner to acknowledge issue and take corrective action.
- Full suite of asset inventory and audit response reports.
- Configurable dashboards and reporting.
- Guided implementation followed by ongoing support and training.

Request your cybersecurity threat assessment today.

GO TO READYWORKS.COM/IT-SECURITY-ASSESSMENT