Tanium Risk Assessment Executive Summary

Prepared for: Software Company

Customer Industry: Business Services

Targeted Group: All Computers

Calculated Risk Score:

415

- Risk Score of 0 represents best in class risk avoidance practice
- Risk score of 1,000 is the worst score representing maximum risks in the environment

Author: lucas.lyon@tanium.com
Created On: 8/12/2025

The Tanium Risk Assessment ("TRA") has been created using Tanium Inc. proprietary software products to analyze customer's endpoint environment. Tanium provides the TRA to customer "as-is" and gives no representation, warranty, indemnity, guarantee, or condition of any kind. To the maximum extent permitted by law, Tanium's total aggregate liability and that of its licensors, suppliers, and partners is expressly limited to five hundred dollars ($500) for any and all damages related to the TRA, regardless of the nature of the claim or theory of liability.

As consideration for receiving this report, customer permits Tanium to use the data contained herein on an aggregated and/or anonymized basis for benchmarking and marketing purposes.

Executive Summary

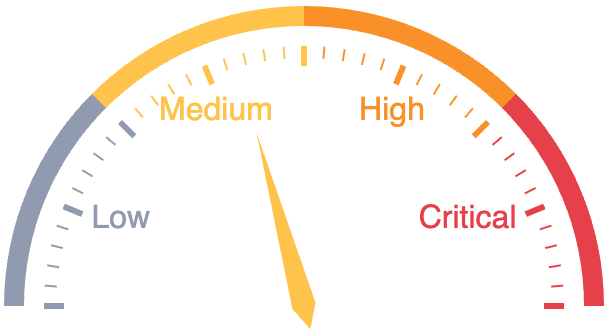
Managing endpoint risk and compliance is more challenging in our digitally driven dynamic world than ever before. Executives accountable for technology, risk, and security must address a range of enterprise and technology risks. These risks are spread across millions of globally distributed, heterogeneous assets. CROs, CISOs, and CIOs must collaborate to respond to ever-increasing audit scrutiny and regulatory compliance requirements and communicate the company's risk position to other executives and board members in an accurate and accessible manner. Tanium delivers an effective foundation for technology risk measurement and management and provides insightful metrics and contextualized data you can trust.

To assist in quantifying the current endpoint security exposure, Software Company has leveraged the power of the Tanium platform to provide an in-depth analysis of the digital environment and an objective security risk score. The analysis measures the operational resiliency and security risk, identifies areas of security vulnerability, and provides a prioritized list of critical actions that can quickly reduce that exposure.

To complete the analysis, Tanium evaluated 1309 endpoints in your environment. Tanium reviewed accessible data in the following areas:

- Critical and high severity vulnerabilities
- Endpoint policy compliance state
- Lateral movement and administrative user account access risks
- Insecure communication protocols
- Encryption and authentication gaps

Tanium determined Software Company's risk score to be:



Risk Score: 415

Highlights about your environment that are driving the score include:

- 1199 endpoints not running identified AV software
- 2417 critical severity vulnerabilities
- 20571 high severity vulnerabilities
- 6322 failed Center for Internet Security (CIS) conditions
- 0 endpoints with hostname collision situations
- 163 endpoints with uptime duration greater than 30 days, which may violate Software Company's reboot or restart requirements
- 1081 endpoints running EOL versions of an OS

The score (0-1000, with 0 being perfect and 1,000 the worst) is calculated by considering the following risk metrics:

1. **System Vulnerabilities -** Most common attacks exploit endpoints with OS or application misconfigurations. To measure the security exposure, the critical and high severity vulnerability risk metrics consider the presence of managed endpoints with critical or high severity vulnerabilities, which puts organizations at greater risk of disruption or breach. During the assessment period on the 43 scanned endpoints, Tanium found **2417 critical severity vulnerabilities** (56.21 per endpoint) and **20571 high severity vulnerabilities** (478.4 per endpoint) with **CVE-2024-24790** being the highest impacting vulnerability. The critical severity vulnerability risk metric contributed **73.4 (22.7%)** points to Software Company's overall risk score, and the high severity vulnerability risk metric contributed **29.3 (9%)** points to Software Company's overall risk score.
2. **Lateral Movement Risk -** Nearly all cyberattacks today involve lateral movement (using stolen credentials to move from endpoint to endpoint). Lateral movement and overly permissive administrative rights enable the propagation of malware, ransomware, and exfiltration of sensitive data. This risk metric considers administrative and access rights based on your Active Directory environment and the identified potential for lateral movement. During the assessment period, Tanium found **0 critical-risk endpoints** (can reach or be reached by 75%-100% of total users or endpoints) and **24 high-risk endpoints** (can reach or be reached by 51-75% of total users or endpoints). These endpoints represent lateral movement risk or unintended administrative access that could be used by attackers to gain access to enterprise resources. This risk metric contributed **90.2 (27.8%)** points to Software Company's overall risk score.
3. **System Compliance -** Industry regulatory requirements (such as PCI, HIPAA, and SOX) and cybersecurity standards (such as ISO27001, CMMC, and FedRAMP) require organizations to harden endpoint configurations. Organizations must also adhere to corporate mandates based on industry-specific and security best practice benchmarks, such as CIS or NIST. This risk metric considers gaps in compliance assessment coverage, which could lead to increased exposure to vulnerabilities. During the assessment on the 31 scanned endpoints, Tanium found **6322 failed industry-standard conditions**. This risk metric contributed **20.4 (6.3%)** points to Software Company's overall risk score.
4. **Insecure Transport Security Protocols -** Organizations use transport layer security protocols, such as Secure Socket Layer (SSL) and Transport Layer Security (TLS), to secure communications and network traffic. Using insecure and outdated protocols (such as SSLv3 and TLSv1) is a security weakness that could leave data and session IDs exposed and vulnerable to exploits. This risk metric considers endpoints currently using insecure transport protocols that could put the confidentiality and integrity of communications at risk. During the assessment period, Tanium found **93 endpoints using insecure and outdated transport layer security protocols** that should be updated to help ensure confidentiality and integrity of communication. This risk metric contributed **106.1 (32.8%)** points to Software Company's overall risk score.
5. **Encryption and Mutual Authentication -** SSL and TLS certificates provide authentication validation to your domains and are critical for ensuring proper encryption and identity verification. Expired SSL/TLS certificates could lead to severe security risks, service outages, and impact on revenue and could expose you to various attacks and viruses. This risk metric takes into account expired SSL/TLS certificates across the endpoints. During the assessment period, Tanium found **6 endpoints with expired certificates** that should be renewed. This risk metric contributed **4.5 (1.4%)** points to Software Company's overall risk score.

Tanium's goal in providing this risk assessment is to assist Software Company leadership in bringing disparate teams together to reduce Software Company's risk exposure as quickly as possible and, in turn, to improve future risk scores.

In addition to this executive summary, a more comprehensive report can be generated that provides details on the risk metrics analyzed, endpoint criticality levels, and additional risk and cyber hygiene metrics. The detailed report also provides details on how the customer environment compares to Business Services industry peers for several security and operational metrics.

Tanium strongly recommends that Software Company engage our Enterprise Services Organization to investigate methodologies and turn-key solutions to remediate the findings efficiently.

About Tanium

Tanium Autonomous Endpoint Management (AEM) offers the most comprehensive solution for intelligently managing endpoints across industries, providing capabilities for asset discovery and inventory, vulnerability management, endpoint management, incident response, risk and compliance, and digital employee experience. The platform supports 34 million endpoints worldwide, including 40% of the Fortune 100, delivering increasingly efficient operations and an improved security posture at scale, with confidence, and in real-time. For more information on The Power of Certainty™, visit www.tanium.com and follow us on LinkedIn and X.