IT Infrastructure Risk & Hygiene Report

Client: [Sample Client] | **Date:** 10 December 2025 | **Generated by:** **NEO**

🚨

CRITICAL INFRASTRUCTURE

136

Server End of Support

Core servers or databases operating past vendor support, creating a high vulnerability risk.

🛡️

HIGH-RISK TOOLS

103

Unauthorized & P2P Tools

Network scanners, packet sniffers, and torrenting clients detected on non-IT assets.

💻

WORKSTATION RISK

2,236

EOL & Obsolete Software

Endpoints running End-of-Life software like IE10 and Silverlight, creating attack vectors.

🎮

PRODUCTIVITY LOSS

2,785

Distraction & Bloatware

Consumer gaming clients (Steam) and streaming apps impacting focus and network bandwidth.

☕

FINANCIAL LIABILITY

22

Oracle Java SE Installs

Oracle Java installs expose the business to 'per-employee' licensing, a significant audit risk.

⚖️

SHADOW IT / DATA RISK

117

Unmanaged AI & Freemium Tools

Use of consumer AI (ChatGPT) and unlicensed freemium tools creates data leakage and audit risks.

SECTION 1: SOFTWARE HYGIENE & SHADOW IT

Security Threats & Unauthorized Tools

PRODUCT NAME	DESCRIPTION	INSTALL COUNT	THREAT CATEGORY
Nmap / Npcap	A utility for network discovery and security auditing.	15	NETWORK RECON
Wireshark	A widely-used network protocol analyzer.	7	PACKET SNIFFING
Advanced IP Scanner	A fast and free network scanner.	10	NETWORK SCANNING
qBittorrent	A peer-to-peer (P2P) file-sharing application.	5	P2P / MALWARE VECTOR
uTorrent	A popular client for the BitTorrent protocol.	2	P2P / ADWARE RISK
Piriform Recuva	A freeware data recovery utility.	2	DATA EXFILTRATION RISK
PuTTY	An SSH and telnet client.	60	UNMANAGED ACCESS
Rufus	A utility to format and create bootable USB drives.	1	DEVICE CONTROL BYPASS
Mullvad VPN	A commercial VPN service.	1	NETWORK POLICY BYPASS

ANALYSIS

The presence of powerful network reconnaissance tools and torrenting clients on non-IT assets presents a significant internal threat. These tools can be used to map the network for lateral movement attacks or introduce malware. Data recovery tools like Recuva can bypass security controls, and unmanaged access tools like PuTTY and Mullvad VPN create unmonitored backdoors.

RECOMMENDATIONS

- Implement application control (e.g., AppLocker) to block the execution of all unauthorized security and P2P tools.
- Restrict the use of these tools to specific, authorized IT security personnel only.

- Investigate the Mullvad VPN install as a potential unauthorized remote access backdoor.

Shadow IT & "Free-for-Personal-Use" (Audit Risks)

PRODUCT NAME	DESCRIPTION	INSTALL COUNT	LICENSE RISK CATEGORY
TeamViewer	A popular remote access and remote control software.	21	COMMERCIAL USE
WinRAR	A trialware file archiver and compressor utility.	12	TRIAL / COMMERCIAL
WinZip	A commercial file archiver and compressor.	4	COMMERCIAL
AnyDesk	A remote desktop application.	9	COMMERCIAL USE
Docker Desktop	A platform for developing and running containerized applications.	4	SUBSCRIPTION REQUIRED
PDF Architect 9	A modular PDF editor with paid features.	2	PAID MODULES
Screaming Frog SEO Spider	An SEO tool with a limited free version.	1	COMMERCIAL USE
CCleaner	A utility used to clean potentially unwanted files.	3	BUSINESS LICENSE REQUIRED

ANALYSIS

56 installations of "Freemium" software were detected. TeamViewer and AnyDesk are the highest risks; vendors actively monitor corporate IP addresses for commercial usage of "free" versions and will issue audit demands. Docker Desktop now requires a paid subscription for companies of this scale, representing a direct compliance failure.

RECOMMENDATIONS

- Audit the TeamViewer and AnyDesk users; if valid business cases exist, purchase Enterprise licenses. If not, uninstall immediately.
- Replace WinRAR and WinZip with the corporate standard (e.g., 7-Zip) to eliminate licensing noise.

- Verify Docker Desktop users are properly licensed or migrate them to a free alternative like Rancher Desktop.

Productivity & Distractionware

PRODUCT NAME	DESCRIPTION	INSTALL COUNT	IMPACT
Valve Steam	A digital distribution platform for video games.	12	GAMING / HIGH RISK
Epic Games Launcher	A storefront and launcher for PC games.	8	GAMING / HIGH RISK
Discord	A VoIP and instant messaging social platform.	25	SHADOW COMMUNICATION
Telegram Desktop	An encrypted, cloud-based instant messaging service.	9	SHADOW COMMUNICATION
WeChat	A Chinese multi-purpose messaging and social media app.	16	SHADOW COMMUNICATION
Spotify	A digital music streaming service.	68	BANDWIDTH
Larian Studios Baldur's Gate 3	A high-end, resource-intensive role-playing video game.	3	GAMING / RESOURCE DRAIN
Electronic Arts The Sims 4	A popular life simulation video game.	2	GAMING / RESOURCE DRAIN
Path of Exile	An online action role-playing game.	2	GAMING / BANDWIDTH
Zhorn Software Caffeine	A utility that prevents a PC from locking or sleeping by simulating a keypress every 59 seconds.	81	POLICY BYPASS
Microsoft Xbox / Game Bar	A built-in Windows gaming overlay and widget.	1520	BLOATWARE
Microsoft Solitaire Collection	A collection of classic card games pre-installed with Windows.	948	DISTRACTION

ANALYSIS

Over 2,700 instances of consumer-grade software were found. Gaming platforms like Steam and Epic are not only a distraction but a significant security risk, as they allow users to download and execute unvetted code. Utilities like Caffeine can be used to bypass security policies.

RECOMMENDATIONS

- Immediately uninstall all gaming platforms and non-essential consumer applications.
- Use endpoint management policies to block the executables for these applications.
- Implement a "Debloat" script during OS deployment to remove built-in Windows games and bloatware.

SECTION 2: LIFECYCLE & TECHNICAL DEBT

Critical Infrastructure (Servers & Databases)

PRODUCT NAME	VERSION	INSTALL COUNT	SUPPORT STATUS	RISK LEVEL
Windows Server 2012 R2	6.3	42	EXPIRED OCT 2023	Critical
SQL Server 2008 R2	10.50	18	EXPIRED 2019	Critical
SQL Server 2014	12.0	24	EXPIRED 2024	Critical
Oracle Database	11g R2	7	EXPIRED 2020	Critical
Ubuntu LTS	18.04	31	EXPIRED 2023	Critical
IIS Express	7.5 / 8.0	14	EXPIRED	Critical

ANALYSIS

136 critical server assets were detected operating completely outside of vendor support. The most widespread risk is the Windows Server 2012 R2 estate (42 servers) which stopped receiving updates in October 2023. Additionally, 18 instances of SQL Server 2008 R2 represent a severe compliance failure and security vulnerability.

RECOMMENDATIONS

- Immediate in-place upgrade or migration for all Windows Server 2012 R2 instances to 2019 or 2022.
- Prioritize the decommissioning or upgrading of SQL Server 2008/2014 instances to prevent data breaches.
- Remove IIS Express instances from production environments.

Workstation & Desktop Risk ("Red List")

PRODUCT NAME	VERSION(S)	INSTALL COUNT	RISK CONTEXT
Internet Explorer	10 / 11	1250	SECURITY / OBSOLETE
Microsoft Silverlight	5	324	EXPIRED 2021 / EXPLOITABLE
Windows 10	Multiple	591	EXPIRED OCT 2025
Microsoft Office 2013	Professional Plus	25	EXPIRED 2023 / UNPATCHED
Java SE Development Kit	1.6 / 6	11	CRITICAL SECURITY VULNERABILITY
Adobe Acrobat DC	2015 / 2017	12	EXPIRED / UNPATCHED
VLC Media Player	2.2.4	21	VULNERABLE VERSION
Google Chrome	69 / 91	15	SECURITY / OBSOLETE

ANALYSIS

The environment has a massive footprint of End-of-Life technology. Over 1,200 machines with Internet Explorer and 300+ with Silverlight represent a critical failure in lifecycle management, exposing the network to well-known, unpatchable exploits. Furthermore, nearly 600 machines running Windows 10 are nearing their support cutoff, creating an urgent migration requirement.

RECOMMENDATIONS

- Initiate an emergency project to remove Internet Explorer and Silverlight from all endpoints. Use Edge IE Mode for legacy app compatibility.
- Expedite the Windows 11 migration project for the remaining 591 Windows 10 assets immediately.

- Deploy a patch management script to update or remove vulnerable versions of common utilities like VLC and Chrome.

SECTION 3: FINANCIAL & COMPLIANCE RISKS

⚠️ **AUDIT WARNING:** Oracle Java usage detected. Oracle now licenses Java on an "Employee Metric" basis for newer versions, meaning the license cost is calculated based on your total employee count, not just the number of users.

Oracle Java Risk

PRODUCT NAME	VERSION	INSTALL COUNT	RISK CONTEXT
Oracle Java SE Development Kit	1.6 / 6	11	LEGACY COMMERCIAL (SECURITY CRITICAL)
Oracle Java SE Development Kit	22	2	MODERN "EMPLOYEE METRIC" LIABILITY
Oracle Java Runtime Environment	8 Update 202+	9	MODERN "EMPLOYEE METRIC" LIABILITY

ANALYSIS

We detected 11 instances of the ancient and insecure Java 1.6, and 11 more instances of modern Java versions that fall under Oracle's new, strict licensing terms. Any one of these modern installs could trigger a compliance event costing the entire employee headcount of [Sample Client] if discovered during an audit.

RECOMMENDATIONS

- Urgently locate the users of modern Oracle Java (v22, v8u202+) and uninstall immediately. Replace with an OpenJDK distribution (e.g., Temurin or Corretto) if Java is required.
- Isolate the machines running the insecure Java 1.6 from the internet and prioritize migrating the application that depends on it.

Developer Tool Compliance

PRODUCT NAME	DESCRIPTION	INSTALL COUNT	RISK CONTEXT
Visual Studio Community	A full-featured IDE for students and open-source contributors.	13	LICENSE VIOLATION

ANALYSIS

13 installations of Visual Studio Community were detected. Its license explicitly prohibits use in enterprise organizations (above a certain size/revenue). This represents a direct violation of Microsoft's license terms and is a high-risk finding in an audit.

RECOMMENDATIONS

- Immediately uninstall all instances of Visual Studio Community.
- Provide users with a compliant alternative, such as Visual Studio Code (which is free for commercial use) or a properly licensed Visual Studio Professional subscription.

SECTION 4: SHADOW AI & DATA LEAKAGE

PRODUCT NAME	DESCRIPTION	INSTALL COUNT	DATA PRIVACY RISK
OpenAI ChatGPT (Desktop App)	A large language model-based chatbot.	50	HIGH (DATA RETENTION)
Dropbox	A cloud-based file hosting service.	6	HIGH (DATA EXFILTRATION)
DeepL	An AI-powered neural machine translation service.	2	HIGH (DOCUMENT UPLOADS)
Perplexity	An AI-powered conversational search engine.	2	MEDIUM (SEARCH HISTORY)
Cursor	An AI-first code editor.	1	HIGH (CODE LEAKAGE)

ANALYSIS

The use of consumer AI and cloud storage tools presents a severe data leakage risk. Any corporate data, code, or confidential documents entered into these public services can be used to train their models or stored outside of corporate governance, creating a permanent, unretractable data breach.

RECOMMENDATIONS

- Block consumer AI and storage domains (e.g., chat.openai.com, dropbox.com) at the network level.
- Redirect users to a sanctioned, enterprise-governed alternative (e.g., Copilot for Microsoft 365, OneDrive) where data privacy is contractually guaranteed.

Disclaimer: This report was generated by the NEO AI Model. While every effort is made to ensure accuracy, AI models can make mistakes. These insights are intended for guidance purposes only. Please verify all findings against the raw data available in Licenseware.