



Service Catalogue

October 2026



Implementation Service

Discovery

- Initial discovery and scope confirmation.
- Kick off call discussing objectives, timelines and scope of project.



Planning

- Define phases of the deployment.
- Defining workshops for modules.



Delivery

- Delivery of pre-planned workshops.
- Tool instance pre-configuration.
- Module configuration and guidance.



Handover

- Tool module sign-off.
- Proof of execution document sent to customer.



Managed Services

*Packages & sensors

Service	Basic	Assist	Hands On (bolt on)
Service Desk	X	X	X
Best practice advice		X	X
Knowledge base		X	X
Technical service reviews		X	X
Technical configuration assistance			X
Custom content creation*			X
Security Engineering Resources			X
Capability integration			X
System management and tuning			X
Strategic planning assistance			X



Additional Services





Additional Services

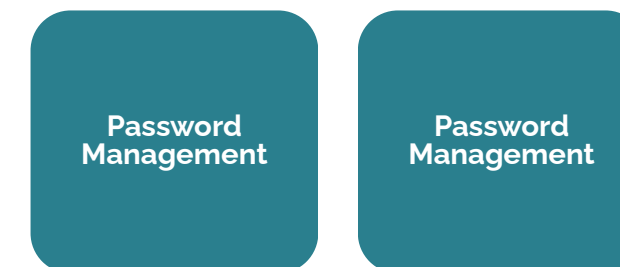
Start- up Business Services Pack



SMB Services Pack +



Enterprise Service Pack +





OS Patch Management

Keep devices secure with reliable patch management

Regular updates fix known vulnerabilities and help protect your systems from attack. While many devices update automatically, some still need oversight and manual intervention.

PointWire delivers a streamlined patch management service that reduces the burden on your IT team. Working with our trusted supplier ecosystem, we implement and configure automated tooling to deploy updates reliably, with minimal user interaction.

The result is a simpler patching process, a stronger security posture and more time for your team to focus on strategic work.

Service Scope

- In-Scope:
- Windows endpoints (Windows 10 and above, Windows Server 2012 and above).
 - Supported devices with internet connectivity.
 - Security and feature updates for operating systems.

- Out-of-Scope:
- Devices with no internet connection.
 - Unsupported operating systems. Devices without the client tools installed.
 - Devices not meeting the minimum requirements for the tooling.

Dependencies

Multi-Tenancy subscription to Tanium

Business Outcomes

Provide the latest OS Patching to include latest features, security patches and bug fixes. Ensures compliance with regulatory requirements. Enhances system stability and performance.

Service Level Agreements (SLAs)

Chose a patch window dependant on your risk tolerance for deploying patches and we will ensure they are patched in the following timeframes.

Metric	Target Days
Patch Window 1	8
Patch Window 2	14
Patch Window 3	21
Patch Success Rate	> 95% of devices without issue



Software Management

Keep your software up to date

Regular software and application updates fix known vulnerabilities and help protect your systems. While many updates happen automatically, some still need oversight or manual intervention.

PointWire delivers a streamlined software update service that reduces the burden on your IT team. Working with our trusted supplier ecosystem, we implement and configure automated tooling to deploy updates reliably, with minimal user interaction.

The result is a simpler update process, a stronger security posture and more time for your team to focus on strategic work.

Service Scope

- In-Scope:
- Windows endpoints (Windows 10 and above, Windows Server 2012 and above).
 - Supported devices with internet connectivity.
 - Applications within Tanium/PointWire's supported application list(s) for Tier 1.

- Out-of-Scope:
- Devices not meeting the minimum requirements for the tooling.
 - Devices not meeting the specification requirements of the application.
 - Applications outside PointWire's application list(s). Tier 3.

Dependencies

Multi-Tenancy subscription to Tanium

Business Outcomes

Provide the latest software packages to have new features, security patches and bug fixes. Ensures compliance with regulatory requirements. Enhances system stability and performance. Enhances the end user experience with new and updated applications.

Level of Service

Tier 1 Software updates on Tanium approved software and an ever-growing PointWire software list. Tier 2 Customer requested Applications that are customer specific and require customisation-Customer list. Additional cost dependant on quantity and complexity.

Service Level Agreements (SLAs)

Rolling deployment window to capture failed updates to keep impact to customer low. 10% Deployment 1, 30% Deployment 2 70% Deployment 3 for all applications.

Deployment	Earliest	Success Criteria	SLA
Deployment 1	Release +1		
Deployment 2	Release +2	90%	
Deployment 3	Release +3	90%	5 days



Vulnerability Reporting & Management

Take control of vulnerability management

PointWire, in strategic partnership with Tanium, helps you identify, prioritise and remediate vulnerabilities before they become a problem.

We assess and categorise each vulnerability by risk, so your team can focus on the issues that matter most. This targeted approach makes better use of your resources and supports a more secure, compliant environment.

Service Scope

In-Scope:

- Windows endpoints (Windows 7 and later, Windows Server 2008R2 and later). MVP.

Out-of-Scope:

- Devices without the client tools installed.
- Devices not meeting the minimum requirements for the tooling.
- Devices without the ability to run Java version 8.

Dependencies

Multi-Tenancy subscription to Tanium

Business Outcomes

Understand your vulnerability landscape based on risk to your organisation. Have the ability to triage and fix your vulnerabilities Allow PointWire to remediate your vulnerabilities either through our other services (OS and Software patching) or through bespoke remediation.

Level of Service

Tier 1 Vulnerability status represented on a dashboard/report that categorises by risk(CVE, CVSS, KEV, Threat Intel) Tier 2 Triage and remediate via OS patch and Software update services. Patch and Software services are a prerequisite. And bespoke remediation utilising Tanium.

Service Level Agreements (SLAs)

Tier 1

Metric	Target
Provide weekly vulnerability reports via email or SIEM tooling	Within 7 days
Scan endpoints for vulnerabilities	Every 24 hours (7 days for high resource CVEs)
Scan success rate across all assets	%

Tier 2

Metric	Target
Triage new critical vulnerability findings	Within 1 day of being found
High	Within 2 days of being found
Medium	Within 7 days of being found
Low	Within 15 days of being found



OS Hygiene

Move to Windows 11 with confidence

PointWire's Windows 10 to Windows 11 Migration Service helps you transition securely and efficiently, with minimal disruption to your users.

Using our multi tenant Tanium platform, we provide endpoint discovery, compliance validation, automated deployment and continuous assurance. Delivered as a managed service, we support the full migration lifecycle, from readiness assessment to post migration validation.

The result is less manual effort, greater operational continuity and confidence that migrated endpoints meet Microsoft's Windows 11 requirements and your internal security baselines.

Service Scope

In-Scope:

- Discovery & Readiness Assessment
- Pre-Migration Remediation
- Deployment Planning
- Migration Execution
- Post-Migration Validation
- Reporting & Handover

Out-of-Scope:

- Application Compatibility Assessment
- Software Remediation
- User Communication and Training
- End-User Device Re-Imaging
- Third-Party Tool Integration

Business Outcomes

- Complete Estate Discovery: Instantly identify every endpoint in your organisation and assess readiness for Windows 11, ensuring no device is left behind.
- Pre-Migration Assurance: Validate that each device meets Microsoft's hardware and security requirements before any upgrade begins.
- Smart, Phased Deployment: Orchestrate secure, automated upgrades through Tanium Deploy with zero manual intervention from the end user.
- Minimal Disruption: Maintain productivity with silent deployment scheduling, bandwidth-optimised delivery, and remediation of failed upgrades.

Service Level Agreements (SLAs)

SLA	Target / Measure	Purpose
Readiness Assessment Coverage	100% of in-scope devices assessed	Confirms Tanium discovery and asset visibility.
Successful Migration	≥ 95% of devices upgraded on first attempt	Demonstrates effectiveness of deployment process.
Security Baseline Compliance	≥ 98% of migrated endpoints meet Windows 11 security baseline	Ensures compliance objectives are achieved.
Average Upgrade Duration	< 30 minutes per endpoint	Validates efficiency and minimal user disruption.
Remediation Time for Failed Migrations	≤ 2 hours mean time to recover	Shows operational responsiveness and stability.
Reporting Cadence	Daily technical (if needed); weekly executive summary	Reinforces governance and transparency.
End-User Disruption	< 2 hours downtime average per device	Quantifies the business impact of migration activities



Confidentiality Notice

This document is confidential and intended solely for **[Customer Name]**'s authorised representatives. It must not be copied, shared, or reused beyond your organisation's internal business needs without PointWire's written permission.

PointWire Limited owns the copyright of this document and reserves all rights. While we take care to ensure accuracy, PointWire is not liable for errors in this document, and excludes liability for any loss connected with its use, to the extent permitted by the law.