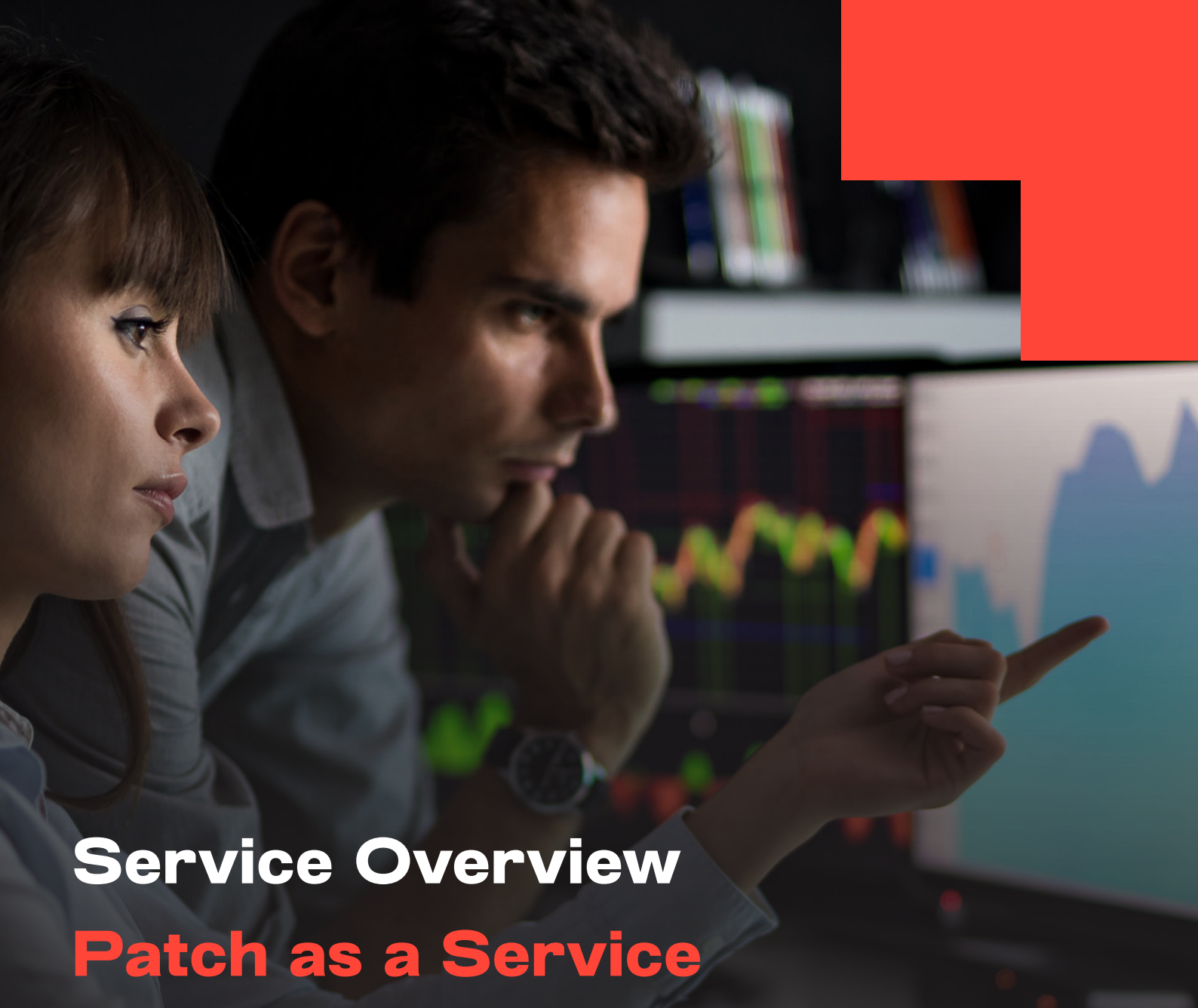

Service Overview

Patch as a Service

It only takes a crack in your defences to be exploited, before a catastrophic breach can irrevocably damage your business and its reputation. Furthermore, by not keeping your applications and operating systems up to date, stability, performance and on-going supportability can be adversely affected. Our patch management service overcomes the limitations of patch Tuesday and the challenges presented by diverse IT environments.

- Three tiers of service, aimed at providing flexibility over what you want patched
- We keep servers, applications and endpoints patched, using a phased approach to reduce risk
- Reduce the threat footprint facing your organisation and help you meet compliance obligations
- We take on responsibility for discovery, setup, patching and status reporting
- Automated and auditable for reduced strain on your IT and compliance teams

Ultima

Overview

The ever-evolving cyber-security landscape - ranging from zero-day malware and security breaches, to code exploits and threats from malicious actors, means that IT teams need to remain vigilant, in order to close vulnerabilities as soon as a fix is published. Couple that with the need to remain up to date with non-critical OS and application updates, means the need for a comprehensive and automated patching approach is critical.

Modern businesses can no longer rely on manual patching, especailly as they grow in complexity, and become dependant on multi and hybrid-cloud environments. With threats coming from multiple directions, including attacks on your endpoints and data centres, which can remain undetected for extended periods, its important to have a robust strategy, backed by tools that can provide heterogeneous coverage.

We provide a simple way of protecting your business, helping reduce the threat footprint and support compliance. Through our long-standing partnership with Ivanti, we negate the challenges traditionally associated with patching, thanks to a low-cost, per-device model, which benefits from three different service tiers, allowing you to select the coverage you need.

From critical updates to security hot fixes, we are able to keep your servers, applications and endpoints patched in accordance with a pre-defined schedule and rule-set; allowing you to focus on innovation. Each of our service offerings is aimed at helping you meet a different set of needs, from entry-level Microsoft OS patching, with daily PowerBI reports, through to health checks, third-party apps and emergency patching, which provides a deeper level of compliance for greater peace of mind.

So Why Patch?

Given that a significant proportion of external breaches are due to un-patched vulnerabilities, a poor patching regime can have catastrophic consequences on systems, personally identifiable information and intellectual property. These breaches erode consumer trust and can lead to significant legal implications. From corporate espionage to financial motivation, criminals are constantly on the look out for organisations who are behind on their security mitigation activities, so they can exploit them.

$4.24M

Average Cost

In 2021, an increase of 10% over 2020, with an average of 287 days to identify and contain a breach- IBM

71%

Found Patching

Complex and time consuming, with 61% being asked to postpone maintenance windows once a quarter - Ivanti

57%

Of Respondents

Believe the global transition towards a decentralised workplace made patch management more complex - Ivanti

57%

Of Cyber Crime Victims

Disclosed that their breach was directly attributed to an unpatched vulnerability in their IT systems- Ponemon Research

34%

Of Companies

Breached knew that they had unpatched vulnerabilities, but did nothing about them - Ponemon

$10.5T

Cybercrime by 2025

If a measured as a country, cybercrime would be the world's third largest economy - Cybersecurity Ventures

Key Benefits

Often de-prioritised in favour of more pressing activities, patch management as a discipline plays a crucial role in an organisation's ability to fend off threats, while improving stability and functionality. Our service overcomes these challenges, leveraging automated tools with actionable insights.

Adam Brown - Cyber Security Team Lead - Ultima

Fully Automated = Risk Mitigated
Remove the problem of having to continually monitor and manage the patch process, with a phased, automated deployment schedule

Managed Release Cadence
We continuously monitor patch sources, including those from known ISVs, automatically adding new releases as they become available

Powered By Ivanti
Identify and patch vulnerabilities across servers, endpoints, operating systems, and over 100 application vendors

Maintain Patch Goals
We can provide regular patching health checks, allowing you to satisfy internal audits and gain insights over your threat footprint

Automated Inventory
An automated discovery routine interrogates the farthest reaches of your environment to establish the asset and application scope

Failed Patch Reporting and Roll Back
Roll back for supported platforms, where the package fails to install correctly or leads to conflicts or stability issues post-deployment

Deep Analytics with Actionable Insights
We use PowerBI to provide near real-time patch reports that help to illuminate every corner of your IT estate

Emergency Patching Supported
Includes out of band patches designed to plug critical vulnerabilities and emerging cyber threats, outside of normal patching cycles

Service Plans

Simply choose the service tier and let us know the number of servers, applications and endpoints required, to establish the per-device / month costs. A one off set up cost applies during customer on-boarding, based on the number of devices in scope for patching. During setup, we will need access, and may need you to conduct a discovery exercise to locate the assets. Just contact your Ultima Account Manager or email our team at **presalesmanagedservices@ultima.com**, and we will advise which is the best service for you.

	Essentials	Advanced	Ultimate
Service Setup and On-Boarding [1]	From £1,000	From £2,500	£POA
Service Dependency	None	None	IRIS [2]
Patch Schedule Configuration Changes & Updates	24h SLA	8h SLA	4h SLA
On-boarding of New Devices into PMaaS [3]	✓	✓	✓
Report - Installed vs Outstanding Patches	✓	-	-
Report - Failed Patches by Device and ID	✓	-	-
Report - Power BI Dashboard	-	✓	✓
Report - Client Count of Patched vs Unpatched	-	✓	✓
Report - Breakdown of Patch Levels by OS	-	✓	✓
Report - Interactive View on Patch Status	-	✓	✓
Report - Agent Status (If Available)	-	✓	✓
Report - View Status by Patch vs Device	-	✓	✓
Create and Maintain CIs in ServiceNow CMDB	✓	✓	✓
Create and Maintain Customer Knowledge Articles	✓	✓	✓
Ivanti Platform Resilience and Backup	✓	✓	✓
Monthly License Usage / Billing Report	✓	✓	✓
Proactive Problem Trending and Investigation	✓	✓	✓
Roadmap - Patch Strategy and Future Direction	Annual	Biannual	Biannual
Roadmap - Review Patch Schedule & Optimisations	Annual	Biannual	Biannual

Service Plans

	Essentials	Advanced	Ultimate
Roadmap - Tech Review, Issues & Improvements	Annual	Biannual	Biannual
Routine Windows Client / Server - Feature Release	-	-	-
Routine Windows Client / Server - Quality Release	✓	✓	✓
Routine Linux - Quality Release	✓	✓	✓
3rd Party Application Patching	Microsoft Only	25 Vendors	Unlimited
Patch Pre-Loading for Manual Patching	✓	✓	✓
Guaranteed response and resolution SLA's	✓	✓	✓
Out of Band Patch Management	-	✓	✓
Agent Management	✓	✓	✓
Patch Deployment Windows - Endpoints	3	10	20
Patch Deployment Windows - Servers	13	26	26
Manual Patching - Per Configuration Item / Month	-	£65.00	£50.00
Additional 3rd Party Apps - Per App /Month	£0.75	£0.50	-
Issue Remediation - % of Device Count Tickets	-	5%	✓[4]
More Deployment Windows - Per Window / Month	-	£5.00	£5.00
Custom / Bespoke Reports - PowerBI	-	£POA	£POA

[1] Ultima will conduct a remediation scan during on-boarding, which may result in a professional services engagement being required, in order to bring the environment up to a supported state

[2] IRIS - Intelligent Remote Infrastructure Support is Ultima's Managed Service

[3] A Fair Usage Policy will apply.

[4] This is a Level 2 ticket Per Device only and not Per Patch. A Fair Usage Policy will apply.

Frequently Asked Questions

Q. What is Ivanti Security Control?

A. It is an enterprise-class patch management solution for endpoints and servers, which helps form part of an organisations' multi-layered security strategy. In addition to Microsoft patching, it is able to provide support for over 100 different third-party vendors.

Q. Is the minumum number of devices you will support?

A. While many aspects of this service are automated, there are some activities which require manual intervention, including initial setup and ad hoc tasks. In order to provide a consistent service, there is minimum commit of 100 devices, even if you have less than 100 to support.

Q. What happens if a patch results in an issue?

A. Where the package fails to install correctly or leads to conflicts or stability issues post-deployment, we will look to roll back to the previous version. It should be noted that this is dependant on the severity of the issue and if the patch or application permits roll-back. In all cases, you should ensure that backups or snapshots are taken.

Q. How are patches tested before they are deployed?

A. Patches are rigorously tested by the vendor and via early adopters and insider programmes, long before they are released to the wider community. By the time they have been picked up by tools like Ivanti, they are considered to be stable and ready for wide-spread release.

Q. Do you manage the application or device?

A. Yes at Ultimate tier only. PMaaS does not absolve you from your responsibilities for managing the device or application in question. You will need to provide the appropriate due diligence, including configuration, maintenance, troubleshooting and end user support.

Q. How can you help with our compliance requirements?

A. A comprehensive patching regime forms an essential part of an organisation's IT security strategy, whether that be to maintain Cyber Essentials or a particular ISO standard. We provide automated reports and compliance health checks, allowing you to demonstrate to your CISO or compliance team, how you are defending against vulnerabilities.

Q. What is the difference between Standard and Premium levels of reporting?

A. We use Ivanti native reporting (Standard) or Power BI (Premium) to provide business intelligence for our patch service. The main difference is the granularity of reports that are available to you as part of this service.

Q. What is Pre-Loading?

A. The installer is copied to the endpoint in advance. The main benefit of this technique is to reduce the load on the network during peak times, by staggering the delivery.

Q. What is Out of Band patching and why is it important?

A. Out of Band refers to newly discovered software vulnerabilities, which until mitigated, can be exploited to adversely affect programmes, data, computers and networks. Our Advanced and Ultimate service promises to patch this as soon as the remedy is released by the vendor, as opposed to waiting until the next scheduled cycle.

Q. Why are there limits on some of your plans?

A. These are to account for reasonable changes (e.g. to the configuration, devices and applications) over the course of any given month. By enforcing a limit, it allows us to ensure we have the necessary resources in place to support all of our clients, in accordance with our SLAs.

Q. Why is there a difference in per-device cost between Endpoints and Servers?

A. Back-end servers and the applications and workloads that run on them are typically business critical, meaning we have additional due diligence activities to consider when it comes to providing patching support, e.g. pre and post-patch checks and additional reporting requirements.

Q. How do you remotely access our site and how can we be sure that your service is secure?

A. We deturmine the best approach for your environment, with each case being agreed at the on-boarding workshop. This may include placing a dedicated server within your environment, or the use of an agent-based approach with remote connectivity from our Technical Service Centre.

About Ultima

Formed in 1990, Ultima has developed into one of the UK's leading intelligent infrastructure, cloud and automation companies, focused on the provision of tailored IT solutions and services, including the design, delivery and support of industry-leading technologies, backed by the very best in 24x7 support from our purpose-built UK Technical Service Centre.

No matter where you are on your IT journey, we can make technology a positive asset, aligned with the goals of your organisation. Whether that be mitigating the risks associated with changes in regulatory compliance, optimising infrastructure to improve efficiency, modernising legacy systems in order to take advantages of the cloud, or automating complex processes, we can help deliver better business outcomes at a commercial, strategic, operational and technical level.

As an end-to-end provider of IT services, we take a holistic approach to delivery, providing multiple entry points to clients who are looking to who are looking to manage their IT more effectively provide more effective technical solutions to their users, customers and partners. Solutions are delivered by Ultima's extensive team of highly skilled technical Solutions Architects, Consultants, Engineers and Project Managers.

We maintain long-standing relationships with a wide range of strategic and disruptive vendors, which alongside our internal pre and post-sales specialists, allow us to provide a wide range of services including;

- Hardware and Software Lifecycle Services
- Technology Steering and Strategic Development
- Business and IT Alignment
- Enterprise Change and Business Risk Management
- Technology Transformation and Automation Services
- IT Integrations - Mergers and Acquisitions
- Optimisation - Standardise, Rationalise and Consolidate
- 24x7 Managed Services

In 2021, Ultima acquired automation and cloud services provider- Just After Midnight, bolstering our skills in Microsoft Azure by adding capabilities around AWS, GCP, Alibaba Cloud and Full Stack, alongside Sitecore, Kentico, Drupal, Umbraco, and AEM. For a full announcement, visit here.

Ultima are proud to have been recognised by industry and channel partners for our expertise in a range of solution and service areas. For more information, visit here.

Head Office - Gainsborough House,
Manor Park, Basingstoke Road,
Reading, Berkshire, RG2 0NA

0333 015 8000
enquiries@ultima.com
ultima.com