

Patch and compliance



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 managed patch service IRIS, overcomes the limitations of patch Tuesday and the challenges presented by diverse IT environments.



Fully automated

Remove the problem of having to continually monitor and manage the patch process, with a phased, automated deployment schedule



Powered by Ivanti

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



Automated inventory

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



Managed release cadence

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



Maintain patch goals

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



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

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.

\$3.62M

average data breach cost

With a **27.7% likelihood of a recurring material data breach** within the next two years

- Ponemon Institute

5.1B

breaches in 2021

1,243 security incidents were discovered in 2021, which accounted for 5,126,930,507 breached records

- ITGovernance

57%

of cyber attack victims

Disclosed that their breach was **directly attributed to an unpatched vulnerability** in their IT systems

- Ponemon Institute

34%

of companies breached

Knew that they had un-patched vulnerabilities, but did nothing about them

- Ponemon Institute



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

Ultima

Patch and compliance

IRIS provides 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 other, more strategic areas of your business.

Each of our service offerings is aimed at helping you meet a different set of needs, from entry-level Microsoft OS patching, with automated reporting, through to health checks, third-party applications and emergency patching, which provides a deeper level of compliance and greater peace of mind.

How to buy

With a minimum entry point of 250 devices (made up of a combination of servers and endpoints), simply choose the service and number of devices 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.

Prices start from just £2.39 per device.

As part of the set up process, we will need secure VPN access to your network, and may need to conduct an initial discovery exercise in order to locate the assets in scope. Just contact your Account Manager or email enquiries@ultima.com and our team will be able to advise which is the best service for you.

Contact us
for more info

0333 015 8000
enquiries@ultima.com
www.ultima.com