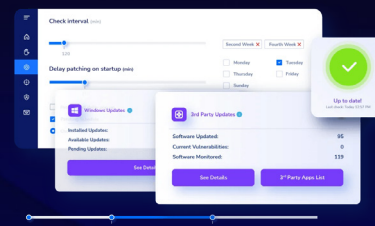


Why Heimdal?

Heimdal offers an end-to-end, proactive, unified cybersecurity suite built to defend against next-gen threats.

The unique, multi-layered approach provides comprehensive protection across all areas. Through Heimdal, you can experience advanced protection across your organisation, from endpoints and networks to emails and beyond.



The challenges Heimdal's Ransomware Encryption Protection solves

Ransomware is one of the biggest cybersecurity threats and organisations must have robust measures in place to keep machines secure and prevent data loss. Heimdal's Ransomware Encryption Protection solution delivers market-leading detection and remediation of any ransomware strain, securing endpoints and networks against the most advanced ransomware encryption attempts.

The solution is universally compatible with any antivirus, extending the functionality of your existing antivirus instead of replacing it. Taking a zero-trust approach, this solution is designed to be a final layer and insurance against encryptions and is the most efficient line of defence against total data loss and exfiltration.

From the very start, Heimdal's solution builds up a picture of day-to-day encryptions that are authorised, creating an 'allow' list. This method allows you to see what's been blocked and only allows what's on the list to be on the machine, blocking everything else.

Benefits of Heimdal's Ransomware Encryption Protection

Heimdal's Ransomware Encryption Protection solution offers the following benefits:



Detects ransomware regardless of signature, identifies origin of attack and system path.



The lowest detection gap on the market, increasing the accuracy of your defences and reporting.



Universal compatibility with any cybersecurity solution such as antivirus or other extended detection and response components.



Safeguard cloud operations including Microsoft, Amazon and Citrix cloud, and integrate with OneDrive, SharePoint, and Teams.



Superior threat intelligence with no file dependency which means the solution quickly works out if something is a threat and eliminates it before it can encrypt your files.



Advanced event logging (MD5, PID, read events, write events, threats, process dial backs, digital signature, machine ID, username, owner, and CVE classification).