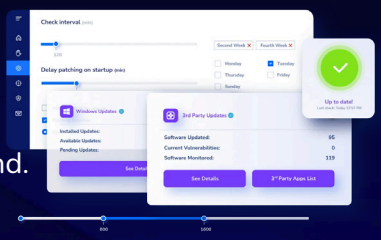
# DNS Security Endpoint

Heimdal®

## 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 DNS Security Endpoint solves

Malicious domains are a constant threat to all organisations. In 2020, nearly 4 out of 5 organisations experienced a DNS attack, and across all industries research suggests that organisations experience on average 9.5 domain attacks every year. Criminals can easily avoid behaviour and code scanners like antivirus and firewalls, resulting in devastating ransomware attacks or data breaches that can ruin your organisation. Heimdal's DNS Security Endpoint addresses these challenges. Working together, DarkLayer Guard and VectorN Detection use proactive, code-autonomous tools designed to layer on top of any existing security solutions. Their intelligence provides a unique level of protection that maps out critical security points in your network. It comes complete with predictive DNS that can predict if a domain is malicious before it even hosts malicious content.

## Benefits of Heimdal's DNS Security Endpoint

**100% compatibility** with existing security solutions and other Heimdal security modules.

A unique level of protection where **malicious domains are predicted** before hosting any content.

Visibility of security-critical points through the **Enhanced Threat To Process Correlation (TTPC)**, this maps out critical points in your environment.

**Malware is blocked at traffic level**, preventing communication with criminal infrastructure and reducing the risk of a successful attack.

**Flexible, easily scalable** and perfectly suited for remote and onsite teams.

BLACK SWAN
CYBER SECURITY SOLUTIONS

blackswancyber.co.uk
hello@blackswancyber.co.uk
01246 927142