

Heimdal - DNS Security Endpoint battlecard

Company overview




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.

Product – DNS Security Endpoint

- Two-way DNS level traffic filter
- Hunt, prevent, detect and respond to traffic based threats
- DarkLayer Guard and VectorN Detection use proactive, code-autonomous tools designed to layer on top of any existing security solutions
- DNS Security Endpoint intelligence provides a unique level of protection that maps out critical security points in your network
- Comes complete with predictive DNS that predicts if a domain is malicious before it even hosts malicious content

Benefit

- Compatibility - 100% compatibility with existing security solutions and other Heimdal security modules
- Advanced protection - malicious domains are predicted before hosting any content
- Visibility of security-critical points - Enhanced Threat To Process Correlation (TTPC) maps out critical security points in your environment
- Reduce risk - malware is blocked at traffic level, preventing communication with criminal infrastructure
- Flexibility - easily scalable and perfectly suited for remote and onsite teams

	 Heimdal DNS Security Endpoint	Cisco Umbrella	DNS Filter	Webroot DNS
Overall capability score	5 ★★★★★	4.4 ★★★★★	4.6 ★★★★★	4.5 ★★★★★
Integrates with antivirus	✓	✗	✗	✗
Content filtering	✓	✓	✓	✗

Objection handling

Doesn't my antivirus cover this?

No, antivirus is about reactive security whereas Heimdal's DNS Security Endpoint is a suite with 3 key layers of protection that filter cyber threats before they reach your system, as well as during and after cyberattacks. DNS Security Endpoint complements antivirus.

I have a remote team, does it work for them?

Heimdal's DNS Security Endpoint works well with a remote working environment and can be implemented on the endpoint- no matter where your staff go they're protected.