

Next-Generation Antivirus 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 – Next-Generation Antivirus

Heimdal's Next-Generation Antivirus identifies and mitigates new, sophisticated attacks. Here are the key features:

- Real time scanning and detection through machine learning
- Detects and remediates viruses, Advanced Persistent Threats (APT's), financial fraud, ransomware and data leaks
- Leverages built in Windows Defender signature base and complements it with heuristics (behaviour based scanning)
- Uses SIGMA rules from the MITRE ATT&CK framework to detect unknown threats - identifying and mitigating attacks that traditional methods can miss
- As files start running, it continues to monitor all processes on your computer using investigative behaviour-based analysis

Benefits

- Faultless detection and mitigation - detecting new, sophisticated threats that traditional methods miss
- Strong security - Heimdal identifies grey threats that fall into an area between malicious and non-threatening activity
- Thorough threat detection processes - using sandbox and backdoor inspection capability, files not identifying as malware enter the sandbox to see how they function
- Multi-dimension detection enhances protection - all unknown files are scanned in real time via the cloud

| |  Heimdal® Next-Generation Antivirus | SentinelOne | Sophos Intercept X | ESET |
|------------------------------|--|-------------|--------------------|-----------|
| Overall rating | 4.8 ★★★★★ | 4.7 ★★★★★ | 4.7 ★★★★★ | 4.3 ★★★★★ |
| Uses MITRE ATT&CK framework | ✓ | ✓ | ✗ | ✗ |
| Integration with DNS filters | ✓ | ✗ | ✗ | ✗ |
| Overview | <p>Heimdal Next-Generation Antivirus stands out because of its use of the MITRE ATT&CK framework, which focuses on detecting the behaviours and techniques of attackers, allowing for the identification of a broader range of threats, including those that are emerging or previously unseen.</p> <p>No other Next-Generation Antivirus can integrate with Heimdal's other products.</p> | | | |

Objection handling

We already have antivirus, why do I need this?

Heimdal's Next-Generation Antivirus adds more behaviour-based characteristics and MITRE ATT&CK is the main differentiator and benefit.

I think our Windows Defender already does this

Heimdal wraps around and uses the built in intelligence from Windows Defender, complementing it with heuristics and indicators of threats from the MITRE ATT&CK framework.