ENDPOINT SECURITY COMPETITIVE OVERVIEW

HEIMDAL SECURITY ADVANTAGES

Our E-PDR ecosystem is built upon an innovative technology that allows for continuous prevention using DNS-based attack protection and patching, combined with an immediate response along with ransomware encryption protection and rights management.

Key competitors and products

CrowdStrike (Falcon Prevent, Falcon Insight)

Weak at :

- Lacks ability to prevent threats from major sources like Websites, urls and Dns.
- Poor performance when it's in offline mode.
- The basic Anti-Virus itself is costly and anything on the top will be very expensive in general.
- Comes as a signatureless solution. That means, even the known malwares will stay in the machine for years.

Best at :

- CrowdStrike stands powerful in their EDR Forensic capabilities and Threat intelligence.

Heimdal vs. Crowdstrike

Heimdal offers a significantly wider lineup than Crowdstrike, with Threat Prevention, Patch and Asset Management, Privilege Access Management and Email Security as extras.

Heimdal Threat Prevention offers more prevention and differentiated detection, compared to any IOA/IOC competitor. Heimdal Threat Prevention offers IOC/IOA at the traffic layers, before attacks even hit machine processes, but offers the process layer detection, using the traffic layer. Crowdstrike is more traditionally and reactively focused using the file and memory layer for detection of attacks.

Both Heimdal and Crowdstrike offers XDR, but head to head the biggest customer benefit is a unified and wider Heimdal lineup, which allows them to have everything in one dashboard.

Microsoft (Defender Antivirus, Defender ATP)

Weak at :

- Multiple console to manage and less in feature for the customer.
- Always emphasize on the current version of windows.
- Windows platform oriented.
- It's still not robust enough and have to improve a lot in ransomware protection

Best at :

- Enterprise license from Microsoft covers the cost of Windows defender as well.

Heimdal vs. Microsoft

As Heimdal is one agent for everything, then the more you plug-in, the more it intelligent it becomes. Working side by side with your E5 on Patch Management, Application Whitelisting etc, you can also use Heimdal to run your security autonomously alongside E5.

Threat Prevention for example working hand in hand with Privilege Access Management, will ensure that users don't get privileges when they are at risk – and the patch management will ensure users are in a compliant state, silently.

Last but not least the Ransomware Encryption Detection is directly bolted onto Microsoft's Antivirus offering by scanning for encryptions via malware that the Defender would have missed.

Trend Micro (Apex One, Worry-Free)

Weak at :

- Multiple products are required to benefit from all features
- Limited cloud management and System heaviness was a big concern from many customers.
- Server protection (Deep Security) is an expensive uplift and customer have to rely on multiple agents.

Best at :

- Aggressive Pricing and Wide range of product including the introduction of XDR and Network security helped them stay stronger in the market.

Heimdal E-PDR vs. Trend Micro

Heimdal's wide offering delivers a far greater prevention (proactive) and detection (reactive) surface than what is offered by Trend Micro. Heimdal offers Threat Prevention, Patching for both MS and 3rd party, A Next-Gen AV, Ransomware Encryption Protection and Privilege and Application Control in one suite, where as Trend Micro is centric around the traditional reactive offering.

The Heimdal offering excels by having a much wider end-to-end view on the threatscape and will at the same time offer a comparable detection on Next-Gen Antivirus standalone.

SentinelOne (Endpoint Protection)

Weak at :

- No complimentary security products – does not offer encryption, mobile, email or firewall protection.
- Traditional reactive approach with zero visibility to web based threats.
- An expensive product with multiple costly add-ons.
- And finally, rollbacks won't work everytime.

Best at :

- Sentinel one Forensic Capability is very good and appealing along with their patented roll back feature.

Heimdal™ Next-Gen AV vs. Sentinel One

Sentinel one features advanced forensics of attack and a very well packaged security suite with very good detection, working on top of Windows Defender ATP.

Heimdal™ is a more straight forward, detection and remediation tool offering more advanced means of detection, with less means of analysis. The key difference between the two is the ease of use and detection.

Heimdal's Next-Gen AV is superior in ease to deploy, implement and use with excellent detection. Both products are reactive.

ESET (Endpoint Protection)

Weak at :

- Complex Management Console.
- Customer have to rely on multiple agents.
- Missing core features a vendor should have like Traffic filtering, Patch Management and Application whitelisting and blacklisting.
- On-premise EDR only and it's expensive as well.

Best at :

- CPU Utilization and their amazing performance in third part assessment tests.

Heimdal E-PDR vs. Eset EPP

Heimdal's wide offering delivers a far greater prevention (proactive) and detection (reactive) surface than what is offered by Eset.

Heimdal offers Threat Prevention, Patching for both MS and 3rd party, A Next-Gen AV, Ransomware Encryption Protection and Privilege and Application Control in one suite, where as Eset is centric around the traditional reactive offering.

The Heimdal offering excels by having a much wider end-to-end view on the threatscape and will at the same time offer a comparable detection on Next-Gen Antivirus standalone.

Kaspersky Endpoint Security

Weak at :

- High RAM & CPU consumption.
- A bit complex interface to work with.
- On-premise EDR only

Best at :

- Market demand for On-premise EDR solution.

Heimdal E-PDR vs. Kaspersky

Heimdal's wide offering delivers a far greater prevention (proactive) and detection (reactive) surface than what is offered by Kaspersky.

Heimdal offers Threat Prevention, A Next-Gen AV, Ransomware Encryption Protection and Privilege and Application Control in one suite, where as Kaspersky is centric around the traditional reactive offering and patching only.

The Heimdal offering excels by having a much wider end-to-end view on the threatscape and will at the same time offer a comparable detection on Next-Gen Antivirus standalone.

McAfee (Endpoint Security, MVISION Endpoint)

Weak at :

- Very Complex platform to manage.
- Features such as device control and application control are additional modules for the endpoint security.

Best at :

- Single console with advanced control features.

Heimdal E-PDR vs. Mcafee EPP

Heimdal's wide offering delivers a far greater prevention (proactive) and detection (reactive) surface than what is offered by Mcafee.

Heimdal offers Threat Prevention, Patching for both MS and 3rd party, A Next-Gen AV, Ransomware Encryption Protection and Privilege and Application Control in one suite, where as Mcafee is centric around the traditional reactive offering.

The Heimdal offering excels by having a much wider end-to-end view on the threatscape and will at the same time offer a comparable detection on Next-Gen Antivirus standalone.

ESET (Endpoint Protection)

Weak at :

- Complex Management Console.
- Customer have to rely on multiple agents.
- Missing core features a vendor should have like Traffic filtering, Patch Management and Application whitelisting and blacklisting.
- On-premise EDR only and it's expensive as well.

Best at :

- CPU Utilization and their amazing performance in third part assessment tests.

Heimdal E-PDR vs. Eset EPP

Heimdal's wide offering delivers a far greater prevention (proactive) and detection (reactive) surface than what is offered by Eset.

Heimdal offers Threat Prevention, Patching for both MS and 3rd party, A Next-Gen AV, Ransomware Encryption Protection and Privilege and Application Control in one suite, where as Eset is centric around the traditional reactive offering.

The Heimdal offering excels by having a much wider end-to-end view on the threatscape and will at the same time offer a comparable detection on Next-Gen Antivirus standalone.

Symantec (Symantec Endpoint Protection, SEP Cloud)

Weak at :

- Still relaying on the same old techniques in detecting threats.
- Limited exploit prevention capabilities and no specific anti-ransomware feature
- Market demand have gone down after Broadcom Acquisition

Best at :

- Symantec has wide range of technologies and they are still in leader in magic quadrant. A good combination of DLP, Endpoint Security and much more.

Heimdal E-PDR vs. Symantec ATD

Heimdal's wide offering delivers a far greater prevention (proactive) and detection (reactive) surface than what is offered by Symantec.

Heimdal offers Threat Prevention, Patching for both MS and 3rd party, A Next-Gen AV, Ransomware Encryption Protection and Privilege and Application Control in one suite, where as Symantec is centric around the traditional reactive offering.

The Heimdal offering excels by having a much wider end-to-end view on the threatscape and will at the same time offer a comparable detection on Next-Gen Antivirus standalone.

Why choose Heimdal™'s enhanced EDR?

We have merged EPP* with EDR* and developed the ultimate security model:

E-PDR (Endpoint Prevention, Detection, and Response)
*EPP (Endpoint Protection Platform) | *EDR (Endpoint Detection and Response)

Our E-PDR ecosystem is built upon an innovative technology that allows for continuous prevention using DNS-based attack protection and patching, combined with an immediate response to advanced cyber threats of all kinds.

- **Track Your Endpoints' Activity**

Now you can track your endpoints' activity using a comprehensive approach to data analysis and respond to recent security incidents by mapping your data against actionable threat intelligence sources.

- **Manage Desktop Rights**

Plus, you can add the option to manage desktop rights and cover not only Gartner's #3 security project recommendation (Detection and Response), but also #2 (Vulnerability Management) and #1(Privileged Access Management), all in one solution.

- **State-of-the-art Cybersecurity**

Get to know a state-of-the-art cybersecurity standard for your enterprise, especially in this day and age when legacy Antivirus solutions do not offer optimal protection against next-gen attacks.

What your EDR system should not be missing:

✓ Machine-learning Capabilities

✓ HIPS/HIDS and IOAs/IOCs

✓ Real-time Response

✓ Integration With Multiple Security Tools

✓ Automatic Vulnerability Patching

✓ Automatic Admin Rights Management