Heimdal

Support | Website | Dashboard

C-Level Report

Demo Customer Sales

02.02.2026 - 09.02.2026

Hello Demo Customer Sales,

Wondering how Heimdal has been protecting your IT estate in the background? Here is an overview of the relevant cybersecurity information during the report timeframe.

Return on Investment

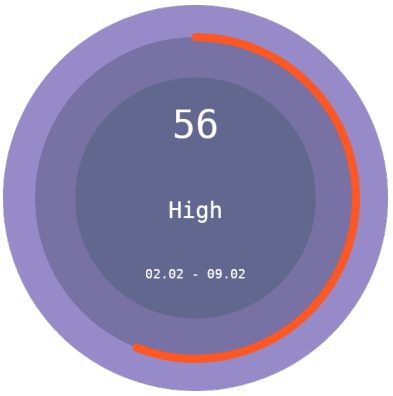
The return on investment figure represents the total savings that your organization made during the selected timeframe, in which Heimdal provided a secure and clean environment for your enterprise.

€1,649.16

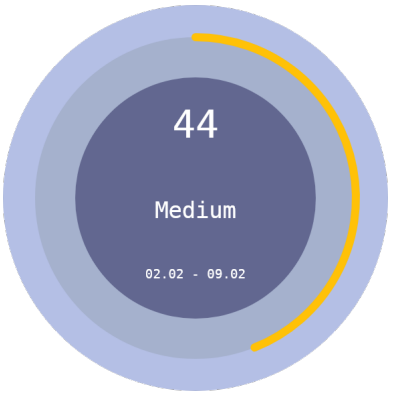
Total cost saved

Risk Score Overview

Device Risk Score



M365 Risk Score



1. Device Info Status

During the selected time frame, we have recorded the following information related to devices (machines) from your estate:

7	0	0
Unique Endpoints	Maximum in one day	Revoked

2. Device Info Notifications

During the selected time frame, the overall health of your IT estate is good.

3. Group Policy Status

In your present Group Policy configuration, it seems that some of your modules are either disabled or in reporting mode, Here is a snapshot of the most important product modules, cyber-security wise:

Network:

Login Anomaly Detection

Endpoint:

Group Policy	DarkLayer Guard	VectorN Detection	3rd Party Patch Management	Operating System Updates	Ransomware Encryption Protection	Next-Gen Antivirus	XTP
AV Server	✓	✓	✓	✓	!	✓	✓
Finance	✓	✓	✓	✓	R	✓	✓
Ingen windows update	✓	✓	✓	✓	R	✓	✓
Inter IT test	✓	✓	✓	✓	R	✓	✓
MAIN POLICY	✓	✓	✓	✓	R	✓	✓
(Master GP) Master of Master GP	✓	✓	!	R	!	!	!
REmote desktop test Finnce	✓	✓	✓	✓	R	✓	✓
Rep_Only_GP	!	✓	!	!	✓	!	!
(Master GP) Reseller Master GP	✓	✓	✓	R	R	!	!
ring 2	✓	✓	✓	!	R	✓	✓
SErver Baseline	✓	✓	✓	!	R	✓	✓
Standard	✓	✓	✓	✓	R	✓	!
(Master GP) TEST	✓	✓	!	R	!	!	!
TESt veals	✓	✓	✓	✓	R	✓	✓
test1	✓	✓	!	✓	!	!	!
(Master GP) test1234	✓	✓	!	R	!	!	!
TKO-GP	✓	✓	✓	R	!	!	!
TKO-GP2	✓	✓	!	R	!	!	!
UK Location - end points	✓	✓	✓	✓	R	✓	✓

For a full view of the Product modules overview, please access the Heimdal dashboard here.

4. DNS Security - DLG Network

During the report time frame, DNS Security - DLG Network analyzed 0 traffic requests and prevented 0 attacks.

0	0	0
Analyzed traffic requests	Prevented attacks	Manual Blocklists

5. DNS Security - DLG Endpoint

During the report time frame, DNS Security - DLG Endpoint analyzed 27 requests, out of which 18 proved to be malicious and have been blocked.
In the Stats area, you can also see an overview of the TOP 5 most blocked domains, TOP 5 processes associated with DNS blocks (TTPC), and TOP 5 targeted hostnames.

27	18	0
Analyzed requests	Prevented attacks	Manual Blocklists

6. TTPC View

Detections	Numbers of matches
chrome.exe	**14**

By looking at your TTPC view, it seems that the most targeted hostnames were the following:

- **Hostname03**
- **Hostname04**
- **Hostname01**

7. DNS Security - VectorN Detection

When it comes to VectorN detections malware strains and/or info related to AI-driven patterns and malicious scripts that could infect hostnames through DNS, the TOP 4 malware patterns are listed below.

7
Dangerous traffic patterns

Malicious strains	Count
APT strain	**5**
Attack blocked	**1**
Botnet strain	**1**

TOP 4 Malware patterns

8. Patch and Asset Management – 3rd Party Patch Management

During the selected time frame, Heimdal's Patch & Assets product module successfully deployed 2 3rd party patches, updating 0 applications;

2	0	0
Applied 3rd party patches	Updated applications	High/ Important & Critical vulnerable applications

9. Patch and Asset Management – Operating System Updates

During the selected time frame, Heimdal's Patch & Assets product module successfully deployed 195 OS updates; however, there are still 8 high and critical vulnerabilities (Severity: Important and Critical) present in your environment that we recommend addressing immediately.

195

Applied OS updates

Severity

Critical and Important OS Updates

- **6 Critical**
- **2 High**

10. Endpoint Detection – Next-Gen Antivirus

During the selected time frame, the Next-Gen Antivirus module quarantined 3 files, greatly enhancing your enterprise's endpoint security. The TOP 5 most infected files from your estate were: psinject.ps1, maverickransomware.exe, maverick.zip, funny_meme.scr, setup_flash.exe , while the most encountered infection types were riskware and virus.

3

Quarantined files

Files	Number of hits
psinject.ps1	**3**
maverickransomware.exe	**3**
maverick.zip	**2**
funny_meme.scr	**2**
setup_flash.exe	**2**

TOP 5 most infected files

11. Endpoint Detection – Zero-Trust Execution Protection

During the selected time frame, Zero - Trust Execution Protection blocked 30 interceptions, securing your apps and data from zero-day vulnerabilities. The TOP 5 process names triggering the blocks were: dymo.officehelper.exe, dymo.webapi.win.host.exe, dymo.officehelper, installpepper_26_0_0_151.exe, qemu-ga.exe.

30

Blocked interceptions

Files/Processes	Number of hits
dymo.officehelper.exe	**13**
dymo.webapi.win.host.exe	**3**
dymo.officehelper	**2**
installpepper_26_0_0_151.exe	**2**
qemu-ga.exe	**2**

TOP 5 blocked process names

12. Endpoint Detection – Firewall

During the selected time range, the Firewall module has protected 3 devices and prevented 4 Brute Force Attacks.

4

Brute Force Attacks

Hostnames	BFA
Hostname04	**2**
Hostname01	**1**
Hostname05	**1**

TOP 5 hostnames with BFAs

13. Endpoint Detection – Ransomware Encryption Protection

In the selected interval of this report, REP stopped 6 ransomware attacks. The TOP 5 most encountered process names were: 7zg,vboxsvc,7z,encryptionenginetest,encryptionenginetest1.

6

Endpoint Detections

Associated processes names	Number of hits
7zg	**7**
vboxsvc	**3**
7z	**2**
encryptionenginetest	**1**
encryptionenginetest1	**1**

TOP 5 Associated process

14. Endpoint Detection – Ransomware Encryption Protection Cloud

REP for Cloud also stopped 28 ransomware attacks. Here's an overview of the top 5 affected users based on the number of affected files:

28

Cloud Detections

Email	Number of affected files
emily.jones@example.com	**8**
michael.brown@example.com	**8**
john.smith@example.com	**6**
sarah.lee@example.com	**6**
david.wilson@example.com	**6**

TOP 5 affected users

15. Endpoint Detection – Extended Threat Protection (XTP)

During the selected time frame, our Extended Threat Protection (XTP) module, which provides evidence-based information about cybersecurity risks and offers a holistic view of weaknesses, categorized on Mitre Attack tactics and techniques, flagged 15 Critical and High severity detections , corresponding to the following processes TOP 5: cmd.exe, schtasks.exe, powershell.exe, AtBroker.exe, SystemSettingsAdminFlows.exe and pertaining to the following TOP 5 categories: Persistence, Execution, Exploit Public-Facing Application, Defense Evasion, Privilege Escalation.

15

XTP Detections

Files/Processes	Number of hits
cmd.exe	**4**
schtasks.exe	**4**
powershell.exe	**2**
AtBroker.exe	**1**
SystemSettingsAdminFlows.exe	**1**

TOP 5 process names

Categories	Number of hits
Persistence	**5**
Execution	**4**
Exploit Public-Facing Application	**4**
Defense Evasion	**4**
Privilege Escalation	**4**

TOP 5 categories

16. Privileges & App Control – Privilege Elevation and Delegation Management

In the report's interval, 11 elevations had been performed using Heimdal's PEDM module, out of which 5 had been session elevations and 6 file elevations The TOP 5 most escalating hostnames were: Hostname01,Hostname02,Hostname-Ubuntu-20.04,Hostname-Ubuntu-24.04 , while the TOP 5 most executed processes were: reportgen.exe,cameraapp.exe,backupsvc.exe,scanner.exe,filesync.exe.

11	5	6
Elevations	Session elevations	File elevations

Hostnames	Number of elevations
Hostname01	**4**
Hostname02	**4**
Hostname-Ubuntu-20.04	**2**
Hostname-Ubuntu-24.04	**1**

TOP 5 most escalating hostnames

Files/Processes	Number of executions
reportgen.exe	**1**
cameraapp.exe	**1**
backupsvc.exe	**1**
scanner.exe	**1**
filesync.exe	**1**

TOP 5 most executed processes

17. Privileges & App Control – Application Control

During the selected time frame, Application Control allowed 0 processes and blocked 0 processes.

0	0
Executions Allowed by Rules	Executions Blocked by Rules

18. Email Protection – Email Security

In the time frame selected for this report, our Email Security product scanned 0 emails, quarantining/rejecting 0 emails. In your IT estate, ESEC is enabled on 6 domains.

0	0	6
Scanned emails	Quarantined/ rejected emails	Domains protected by ESEC

Domain	Status	SPF	DMARC
demo.heimdalsecurity.com (MX)	🟢	🟢	🔴
test1234.com (MX)	🔴	🟢	🔴
test2.com (MX)	🔴	🟢	🔴
testeewewr.com (MX)	🔴	🟢	🔴
testheimdalsecurity.com (MX)	🔴	🟢	🔴
testtest.com (MX)	🔴	🟡	🔴

19. Remote Desktop

During the selected time frame, an overall of 0 Remote Desktop sessions have been performed, out of which 0 have been Heimdal agent sessions and 0 have been Invite / non-Heimdal agent sessions. Throughout this period, there were 0 concurrent sessions accounted for your organization.

0	0	0	0
Remote Desktop sessions	Heimdal agent connections	Non-Heimdal agent connections	Concurrent sessions

20. M365 User Security

During the selected time frame, the top 5 M365 user based on risk score are:

User	M365 Risk Score
user04@demo.com	50
user08@demo.com	50
user01@demo.com	42
user02@demo.com	42
user03@demo.com	42

Should you need to get in touch with us or require technical assistance, please email us at corpsupport@heimdalsecurity.com and we'll get back to you as soon as possible!

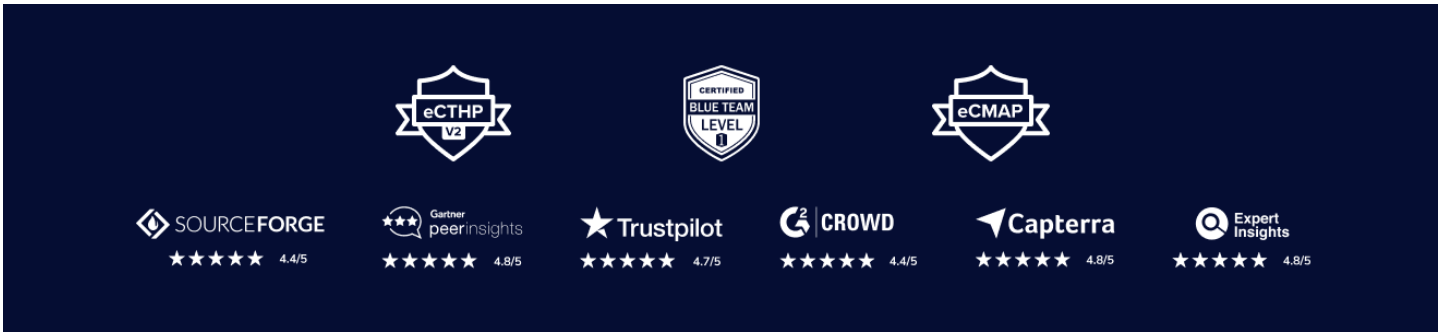
Need Assistance?

If you require any help, please don't hesitate to reach out to us at the appropriate contact:

1. Corporate Customers: **b2bsupport@heimdalsecurity.com**
2. Partners: **partnersupport@heimdalsecurity.com**
3. MXDR Service: **mxdr@heimdalsecurity.com**

We're committed to providing you with the best possible experience and security.

Best regards,
The Heimdal Team



Heimdal