Heimdal®

C-Level Report

20.02.2025 - 21.03.2025

Hello HEIMDAL Support Team,

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

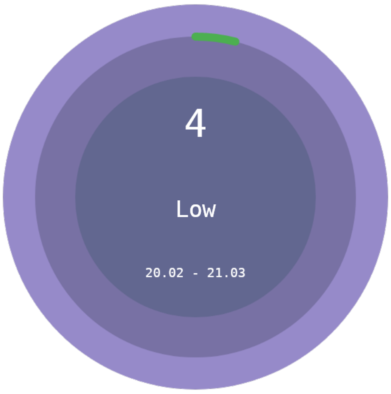
The return on investment figure represents the total savings that your organization made during the selected timeframe, in which we provided a secure and clean environment for your enterprise.

€611.90

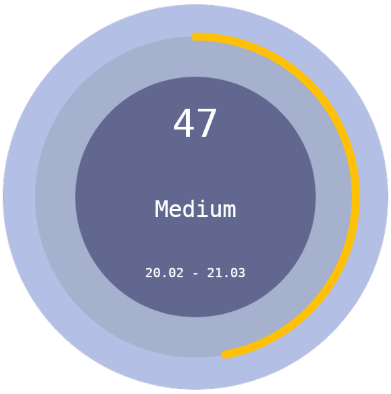
Total cost saved

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:

21	**20**	**2**
Unique Endpoints	Maximum in one day (March)	Revoked

2. Device Info Notifications

During the selected time frame, the overall health of your IT estate is good. However, there are some devices (machines) having operational issues and we strongly recommend addressing those issues.

Hostname	Operational Issues
AZURE2	**1**

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:

Endpoint:

Group Policy	DarkLayer Guard	VectorN Detection	3rd Party Patch Management	Operating System Updates	Ransomware Encryption Protection	Next-Gen Antivirus	XTP
3rd Party Patch Management	!	!	✓	!	!	!	!
Application Control	!	!	✓	!	!	!	!
Azure AD Group 1	!	✓	!	!	!	!	!
Azure AD Group 2	!	✓	!	!	!	!	!
Azure AD Group 3	!	✓	!	!	!	!	!
BitLocker	!	!	!	!	!	!	!
DarkLayer Guard	✓	✓	!	!	!	!	!
Email Fraud Prevention	!	!	!	!	!	!	!
Firewall Management	!	!	!	!	!	!	!
Main (catch-new-endpoints)	!	✓	!	!	!	✓	!
Next-Gen Antivirus (Avira)	!	✓	!	!	!	✓	!
Next-Gen Antivirus with XTP (WD)	!	✓	!	!	✓	✓	✓
OS Updates	!	!	!	!	!	!	!
Privilege Elevation and Delegation Management	!	!	!	!	!	!	!
Ransomware Encryption Protection	!	!	!	!	✓	!	!
Remote Desktop	!	!	!	!	!	!	!
ROMY's devices (DON'T TOUCH)	✓	✓	✓	✓	!	✓	!
Scripting	!	✓	!	!	!	!	!
Testing AD Computer Group	✓	✓	!	!	!	!	!
Testing AD User Group	!	!	!	!	!	!	!
USB Management	!	✓	!	!	!	!	!

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
Analyzed Traffic Requests	Prevented attacks

5. DNS Security - DLG Endpoint

During the report time frame, DNS Security - DLG Endpoint analyzed 49798 requests, out of which 3 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.

49798	3
Analyzed requests	Prevented attacks

6. TTPC View

Detections	Numbers of matches
chrome.exe	**1**

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

.SUPPORT9

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.

0

Dangerous traffic patterns

Malicious strains	Count
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 338 3rd party patches, updating 101 applications; however, there are still 1 high and critical vulnerabilities (CVSS ≥ 7) present in your environment that we recommend addressing immediately.

338

Applied 3rd party patches

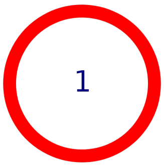
101

Updated applications

1

High/ Important & Critical vulnerable applications

CVSS



Critical and High 3rd party patches

● **1 Critical**

▲ **0 High**

From a Cyber Essentials scheme perspective, your environment contains 11 machines that fully meet the CE 3rd party patch management compliance criteria and 6 machines that are not CE compliant.

9. Patch and Asset Management - Operating System Updates

During the selected time frame, Heimdal's Patch & Assets product module successfully deployed 26 OS updates; however, there are still 0 high and critical vulnerabilities (Severity: Important and Critical) present in your environment that we recommend addressing immediately.

26

Applied OS updates

From a Cyber Essentials scheme perspective, your environment contains 13 machines that fully meet the OS Updates compliance criteria and 4 machines that are not CE compliant.

10. Endpoint Detection Next-Gen Antivirus

During the selected time frame, the Next-Gen Antivirus module quarantined 5 files, greatly enhancing your enterprise's endpoint security. The TOP 5 most infected files from your estate were: eicar_com.zip, couponprinter.exe, fileopenersetup.exe, 0.out, eicar.com , while the most encountered infection types were potentially unwanted software and trojan.

5

Quarantined files

Files	Number of hits
eicar_com.zip	**2**
couponprinter.exe	**2**
fileopenersetup.exe	**2**
0.out	**2**
eicar.com	**1**

TOP 5 most infected files

11. Endpoint Detection - Zero-Trust Execution Protection

During the selected time frame, Zero Trust Execution Protection blocked 0 interceptions, securing your apps and data from zero-day vulnerabilities.

0

Blocked interceptions

12. Endpoint Detection - Firewall

During the selected time range, the Firewall module has protected 0 devices and prevented 0 Brute Force Attacks.

0

Brute Force Attacks

13. Endpoint Detection - Ransomware Encryption Protection

In the selected interval of this report, REP stopped 0 ransomware attacks.

0

Endpoint Detections

14. Endpoint Detection - Ransomware Encryption Protection Cloud

REP for Cloud also stopped 0 ransomware attacks.

0

Cloud Detections

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 0 Critical and High severity detections

0

XTP Detections

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

In the report's interval, 27 elevations had been performed using Heimdal's PEDM module, out of which 2 had been session elevations and 25 file elevations. The TOP 5 most escalating hostnames were: SUPPORT8,SUPPORT9, while the TOP 5 most executed processes were: dllhost,cmd,powershell,consent,Autodesk_Revit_2025_4_ML_setup_webinstall.

27

Elevations

2

Session elevations

25

File elevations

Hostnames	Number of elevations
SUPPORT8	**17**
SUPPORT9	**10**

TOP 5 most escalating hostnames

Files/Processes	Number of executions
dllhost	**9**
cmd	**7**
powershell	**4**
consent	**3**
Autodesk_Revit_2025_4_ML_setup_webinstall	**3**

TOP 5 most executed processes

17. Privileges & App Control - Application Control

During the selected time frame, Application Control allowed 419 processes and blocked 7 processes.

419

Allowed

7

Blocked

18. Privileges & App Control - Privileged Account and Session Management

During the selected time frame, 1419 sessions have been completed using Heimdal's Privileged Account & Session Management module, while 2 users had PA&SM user accounts created.

1419

Completed sessions

2

Created user accounts

19. Email Protection - Email Security

In the time frame selected for this report, our Email Security product scanned 117 emails, quarantining/rejecting 11 emails. In your IT estate, ESEC is enabled on 2 domains.

117

Scanned emails

11

Quarantined/ rejected emails

2

Domains protected by ESEC

Domain	MX	SPF	DMARC
centiumtest.co.uk	🔴	🟡	🔴
centiumtest.com	🟢	🟢	🟢

20. Remote Desktop

During the selected time frame, an overall of 2 Remote Desktop sessions have been performed, out of which 2 have been Heimdal agent sessions and 0 have been Invite / non-Heimdal agent sessions. Throughout this period, there were 1 concurrent sessions accounted for your organization.

2	2	0	1
Remote Desktop sessions	Heimdal agent connections	Non-Heimdal agent connections	Concurrent sessions

21. M365 User Security

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

User	M365 Risk Score
test2@centiumtest.com	**100**
test1@centiumtest.com	**100**
test3@centiumtest.co.uk	**100**
sync_dc_773f4bcca90a@centiumtesting.onmicrosoft.com	**30**
aadsupport@centiumtest.com	**0**

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!

Heimdal®

One Platform. Total Security.

©2024 Heimdal®
Vat No. 35802495, Vester
Farimagsgade 1, 2 Sal, 1606
København V

heimdalsecurity.com