Heimdal

Support | Website | Dashboard

Detailed Report

Demo Customer Sales

28.12.2025 - 27.01.2026

Hello Demo Customer Sales,

This report provides a detailed analysis of your environment during the report timeframe.

Return on Investment : €339.59

View ROI Data

DNS Security Endpoint

Risk Level: Low

27	18	36
Analyzed traffic requests	Prevented attacks	Category blocks

Latest DNS Endpoint Threats

Hostname	URL	Threat Type
• Hostname01	givemereddit.stream	
• Hostname01	givemereddit.stream	
• Hostname01	givemereddit.stream	
• Hostname01	givemereddit.stream	
• Hostname01	givemereddit.stream	

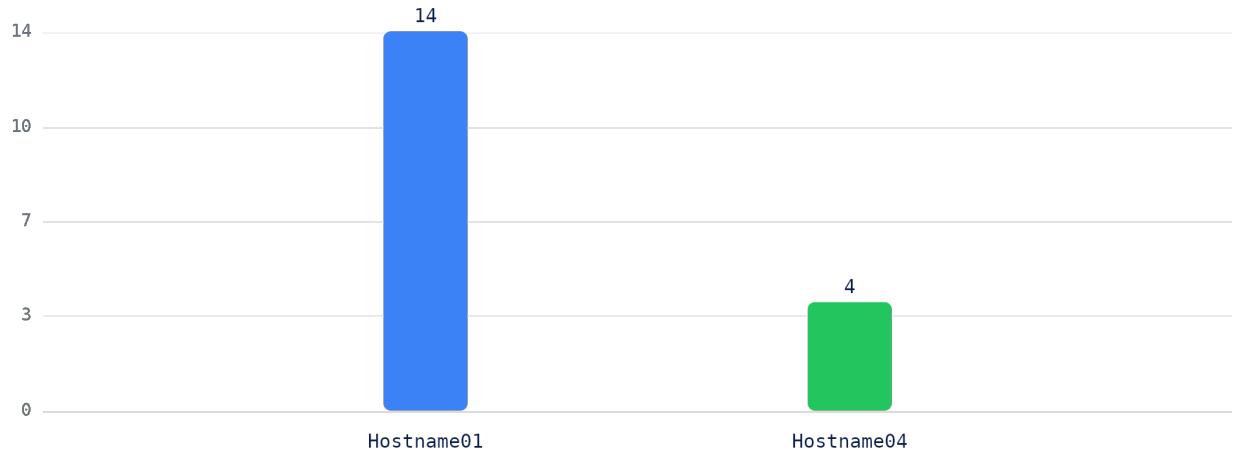
Most used malicious domains

Domain	Number of detections
• givemereddit.stream	14
• scarabresearch.com	4

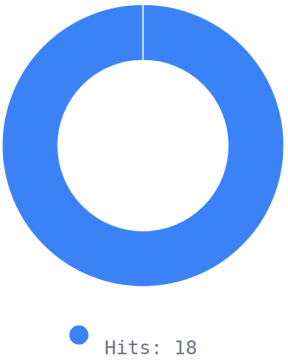
Most installed CASB apps

Application	Installed endpoints
• OneNote	1
• Microsoft Outlook	1

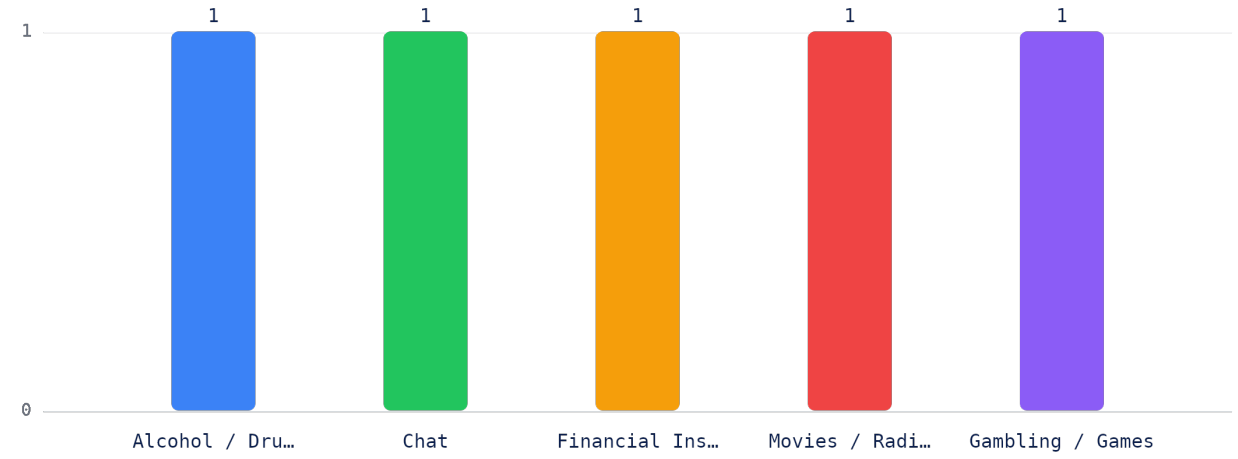
Top 5 Blocked DNS Clients



Threat Type Distribution



Top 5 Categories Blocked



View DNS Endpoint Data

VectorN Endpoint

Latest VecotrN Detections

Hostname	Malware Pattern	TTPC	Probability of Infection

No Data Available

View VectorN Endpoint Data

DNS Security Network

Risk Level: Low

0	0	0
Analyzed traffic requests	Prevented attacks	Category blocks

Latest DNS Network Threats

Hostname	URL	Threat Type

No Data Available

Most used malicious domains

Domain	Number of detections

No Data Available

Most installed CASB apps

Application	Installed endpoints

No Data Available

View DNS Network Data

VectorN Network

Latest VectorN Detections

Hostname	Malware Pattern	Probability of Infection
No Data Available		

View VectorN Network Data

3rd Party Patch Management

0	3	1	1
Vulnerable applications	Patches applied	Updated applications	Applications monitored

Most critical vulnerabilities

Windows

Hostname	Software	Version	CVE	CVSS
No Data Available				

MacOS

Hostname	Software	Version
No Data Available		

Linux

Hostname	Software	Version	CVE	CVSS
No Data Available				

Click here to see all 3rd Party Assets installed in your estate. To see all currently outdated patches, click here.

Here is an overview of your group policies where 3rd Party Patching is disabled:

Windows Group Policy
(Master GP) test1234
(Master GP) TEST
Rep_Only_GP
(Master GP) Master of Master GP
test1

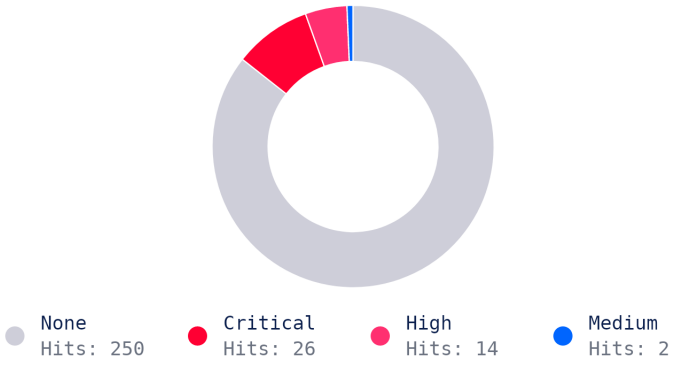
For a full view of the Product modules overview, please access the Heimdal dashboard here.

View 3rd Party Patching Data

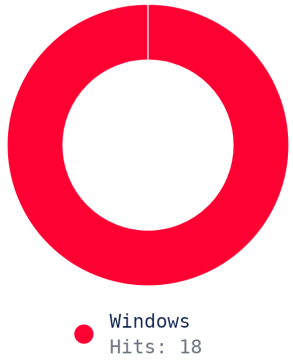
Operating System Updates

436	323	74
Updated applications	Vulnerable applications	Patches applied

Available OS Updates Breakdown



Vulnerabilities by OS Breakdown



Click here to see a severity breakdown of all your OS Updates.

Critical available updates

Windows

Title	Severity	CVE	Devices
• 2021-02 Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB4601319)	None	CVE-2020-1472	1
• 2021-01 Cumulative Update for Windows 10 Version 1909 for x64-based Systems (KB4598229)	None	CVE-2021-1694	1
• 2021-04 Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5001330)	None	CVE-2021-27092	2
• 2020-10 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 2004 for x64 (KB4578968)	Important	CVE-2020-1147	1

MacOS

Title	Version	Devices

No Data Available

Linux

Title	Package	Version	CVE	Devices

No Data Available

Click here to see all OS Updates Assets installed in your estate. To see all failed OS Updates deployments, click here.

Here is an overview of your group policies where OS Updates module disabled or in Reporting Mode:

Windows Group Policy	Disabled or in Reporting Mode
(Master GP) test1234	R
(Master GP) Reseller Master GP	R
SErver Baseline	!
(Master GP) TEST	R
Rep_Only_GP	!

Linux Group Policy	Disabled or in Reporting Mode
Custom	!

Mac Group Policy	Disabled or in Reporting Mode
Custom	!

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

View OS Updates Data

Next-Gen Antivirus

Risk Level: High

We highly recommend you take immediate action to run a full-system scan on the endpoints singled out in the Most Affected Endpoints section of this report.

93	19	0	riskware
Infections found	Quarantined files	Functionality issues	Most frequent type of malware detected

Latest Infections

Hostname	File name	Threat category
• Hostname01	invoke-masstokens.ps1	riskware
• Hostname01	reflectivepick_x86.dll.enc	riskware
• Hostname01	psinject.ps1	trojan
• Hostname02	lnemf.dll	trojan
• Hostname01	invoke-masscommand.ps1	riskware

Latest Quarantined Threats

Hostname	File name	Threat category
• Hostname03	maverickransomware.exe	APC/MALWARE
• Hostname03	invoice_malware_01.exe	virus
• Hostname03	cv_final_virus.doc	virus
• Hostname03	track_player.exe	virus
• Hostname03	funny_meme.scr	virus

Latest functionality issues

Hostname	Issue

No Data Available

Most Affected Endpoints

Hostname	Number of detections
• Hostname01	40
• Hostname01	12
• Hostname05	7
• Hostname04	6
• Hostname02	5

View NGAV Data

XTP

25

Total detections

Latest Detections

Hostname	Rule name	Severity
• Hostname01	Suspicious Typical Malware Back Connect Ports - D29C773B	Medium
• Hostname04	Suspicious Rundll32 Without Any CommandLine Params - E6BA02A6	High
• Hostname02	Suspicious Subsystem for Linux Bash Execution - 7EE83BA1	Medium
• Hostname04	Execution in Webserver Root Folder - AF740BEC	Medium
• Hostname03	Execution in Webserver Root Folder - AF740BEC	Medium

Top 5 Rule Detections

Rule name	Number of detections	Severity
• Shells Spawned by Web Servers - 4937DE71	4	High
• Suspicius Add Task From User AppData Temp - C874B97B	4	High
• Execution in Webserver Root Folder - AF740BEC	3	Medium
• Powershell launch regsvr32	2	Critical
• Suspicious Typical Malware Back Connect Ports - D29C773B	2	Medium

View XTP Data

Firewall

15	5
Firewall Rules	BFA Detections

Latest Brute Force Attacks By Risk Level

Hostname	Attempts	Detection Type	Remote IP	Risk Level
• Hostname05	50	Brute Force Attack	34.218.62.116	
• Hostname04	32	Brute Force Attack	45.11.202.13	
• Hostname04	1	Brute Force Attack	178.59.170.155	
• Hostname01	89	Brute Force Attack	103.187.242.27	
• Hostname02	1	Brute Force Attack Private	10.55.55.2	

Most targeted hostnames

Hostname	Local IP	External IP & No. of attempts	Country of origin
• Hostname01	10.201.201.9	103.187.242.27 (89)	Greece
• Hostname05	10.201.201.33	34.218.62.116 (50)	United States
• Hostname04	10.201.201.22	45.11.202.13 (32)	Turkey
• Hostname02	10.201.201.7	10.55.55.2 (1)	

View Firewall Data

Zero-Trust detections

30	0	0	30
Total detections	Interceptions allowed	Interceptions blocked	Interceptions blocked by default

Latest Zero-trust Detections

Hostname	Process name	Status
• Hostname01	DYMO.OfficeHelper.exe	Unknown
• Hostname01	InstallPepper_26_0_0_151.exe	Unknown
• Hostname01	DYMO.OfficeHelper.exe	Unknown
• Hostname01	DYMO.OfficeHelper.exe	Unknown
• Hostname01	DYMO.WebApi.Win.Host.exe	Unknown

View Zero-Trust Data

Privilege Elevation and Delegation Management

4	5
File elevations	Session elevations

Most elevated processes

Process name	Elevations
• audiohost.exe	1
• backupsvc.exe	1
• dbmonitor.exe	1
• scanner.exe	1
• systemcheck.exe	1

Most elevated users

Username	Elevations
• Hostname02	5
• Hostname01	4

Additional stats

2	0	9	0
Users with admin rights	Users de-elevated due to risk	Blocked elevations due to CVS risk	AI approved elevations

View PEDM Data

Application Control

0	0
Executions Allowed by Rules	Executions Blocked by Rules

Most executed processes

Process name	Number of executions
No Data Available	

Here is an overview of your group policies where Application Control module is disabled:

Group Policy
(Master GP) test1234
(Master GP) TEST
AV Server
Rep_Only_GP
TKO-GP

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

View AppControl Data

Email Protection

Domain Status

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

Email Security

Last 90 days summary

Overall stats		Status breakdown		
Emails actioned	5	Delivered	100%	5
Total Malicious	0	Quarantined		0
Total Inbound	5	Rejected		0
Total Outbound	0	Undelivered		0
		Queued		0

0	0	0	0
Scanned Emails	Spam Emails	Virus	Advanced Threats

View ESEC Data

Email Fraud Prevention

Last 90 days summary

Overall stats		Status breakdown		
Emails actioned	5	Delivered	100%	5
Total Malicious	0	Quarantined		0
Total Inbound	5	Rejected		0
Total Outbound	0	Undelivered		0
		Queued		0

0	0	0
Scanned Emails	Outliers	Fraud

View EFP Data

Remote Desktop

0	0	0	0
Attended Sessions	Unattended Sessions	Invite Sessions	Concurrent Connections

Devices with most connections

Hostname	Username	Sessions
No Data Available		

View Remote Desktop Data

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