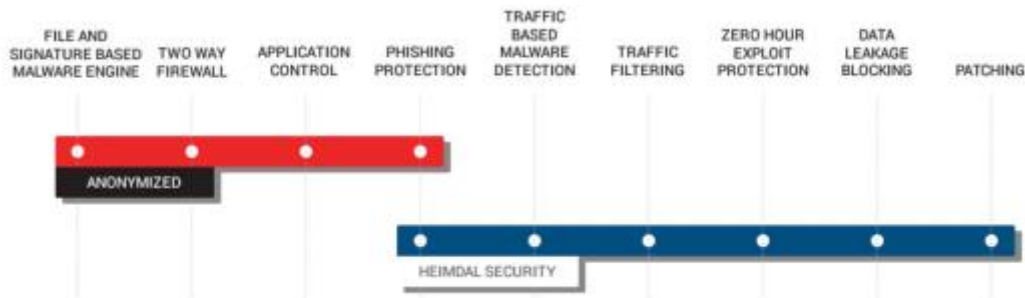


Heimdal Security

Unique traffic based PC protection, combined with an Enterprise scale patching system

Antivirus looks for files and actions, whereas Heimdal looks at traffic. Therefore, Heimdal and Antivirus work independently but in tandem. Heimdal prevents hackers from taking data from your PC and moving it out of your network.



Part of the best in the Cyber Threat space

Heimdal Security is part of Gartner’s selected 25 on Cyber Threat intelligence and is part of the best in E-crime. Heimdal delivers market leading threat intelligence to organisations across the world such as the FBI, the Metropolitan Police and Lloyds Banking Group.

Developed by world champions

The Heimdal Security software was developed in 2011 by the 19th and 20th Team Defcon CTF World Champions in hacking. Heimdal is now used to protect organisations across Europe against advanced attacks, wherever their users may go.

Even adds to leading protection

Antivirus products and Heimdal are a great security compliment to each other, because they address different Endpoint security aspects. Today’s leading antivirus products offer great signature and file based scanning, with firewall and phishing protection, but they are still different from Heimdal.

What is the difference

The key difference in Heimdal to Antivirus products is that Heimdal focuses on the communication from and to the PC to combat and detect incoming 2nd generation malware, combined with patching to close security gaps used by hackers.

Works with any antivirus

Heimdal works with any antivirus engine on the market. The combined protection you receive will vary between the engines used, but Heimdal will always add traffic based protection against new 2nd generation attacks, where no antivirus product is able to intercept these attacks.

Cyberthreat Security Suite with 3 key layers



2-way traffic scanning engine

Heimdal has a unique, client-based 2-Way Traffic Scanning Engine which protects you against Zero Hour exploits, dangerous web locations, malicious content from legitimate websites, cybercriminal attacks and data leakage. Heimdal is the traffic scanning alternative for any business.



Unique TPA Engine

The unique, traffic-pattern Malware Engine is a perfect layer of extra protection for any Antivirus product. It enables you to detect and block new and advanced malware strains. Heimdal's state-of-the-art technology is accredited by the US Department of Justice, the FBI and Europol. Heimdal uses traffic-based detection, while antivirus uses file and signature scanning.



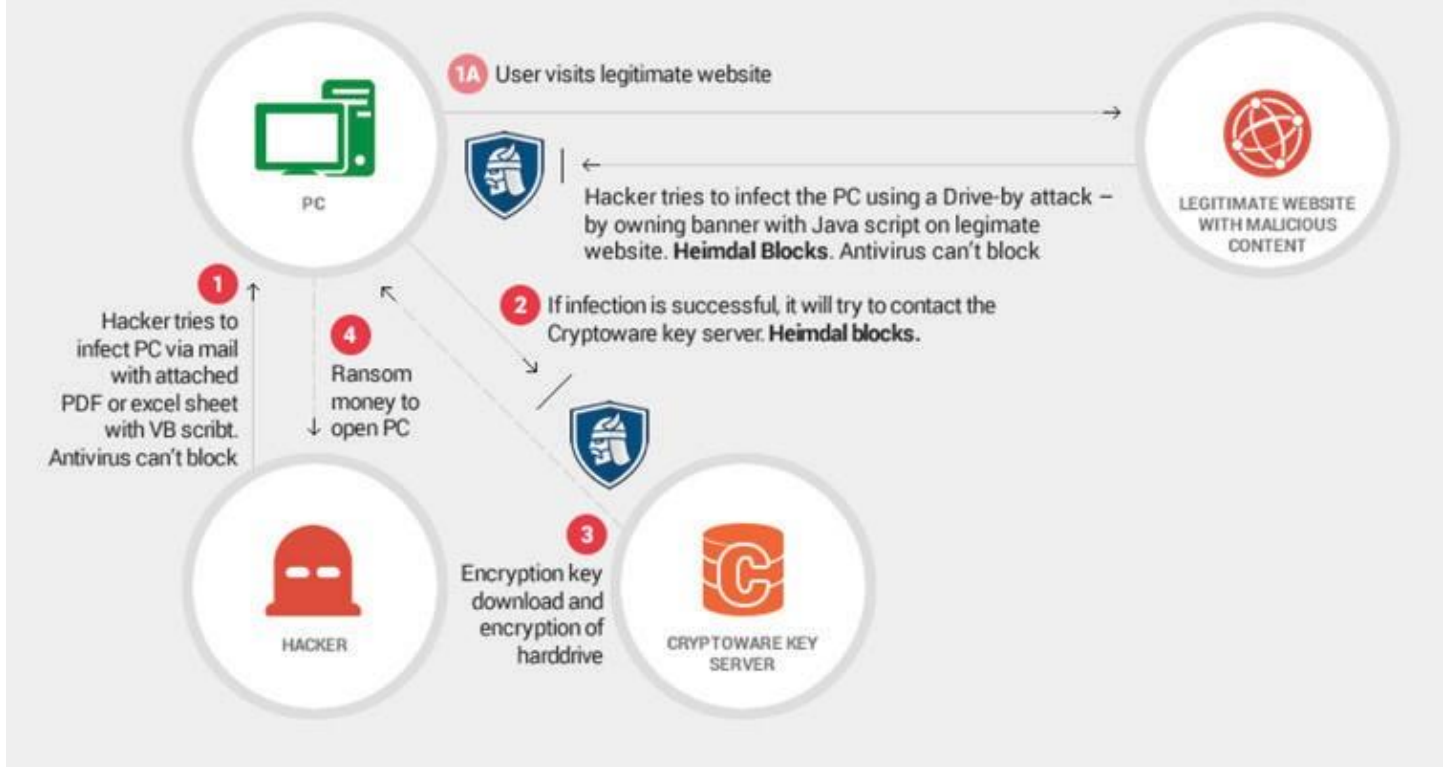
Software installer and patching

Looking for vulnerability intelligence? Heimdal provides you with essential intelligence about your vulnerabilities. It can also install and patch critical applications automatically, silently, with zero setup and without user interruption, while offering the flexibility you need. Patching is a key component in any IT security environment, as exploits are used in 65% of all attacks.

Heimdal Security

PROTECTS YOUR DATA

CRYPTOLOCKER

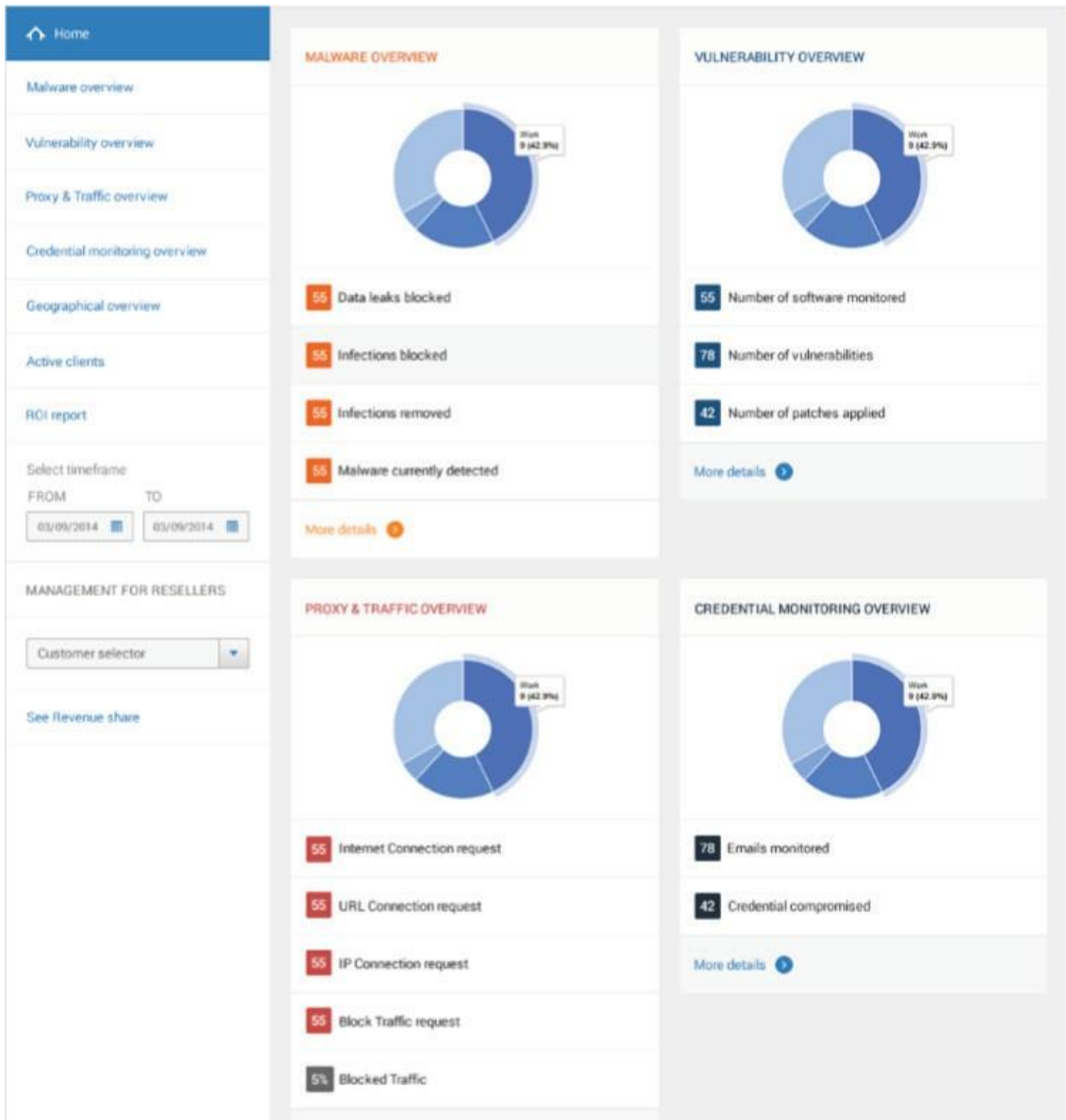


Cryptoware Protection

CTB-Locker, Cryptolocker, Cryptodefence or Cryptowall is likely the most advanced malware in the world.

Heimdal offers protection where antivirus products give up - offering Patching, Exploit blocking, Dropper protection or key delivery filtering.

Infections can happen either via vulnerabilities or exploits delivered from legitimate website banners and cannot be detected by antivirus products. Once the exploits are used, Malware droppers deliver the payload which can avoid your antivirus. This means that hackers are often successful in bypassing defenses. Heimdal uses it 4-layers to stop Ransomware attacks at different levels.



Heimdal Unified Threat Platform

The Heimdal Unified Threat Platform is an integrated SIEM platform which gives you a clear overview of key security aspects in your client and user environment. Heimdal Corporate provides SIEM (Security information and event management) and IDP/HIPS and DLP protection.

Heimdal helps you monitor: -Malware -Data leaks -Vulnerabilities -Traffic usage - Malicious traffic.

Giving you 360 degree control of the risks in your organization.

GROUP ⓘ

Group name:

Ad Group:

Priority:

Language:

TRAFFIC & PROXY ENGINE ⓘ

Traffic engine

Proxy engine

IP Filtering

URL Filtering

MALWARE DETECTION ⓘ

Enable signature detection

Enable detection based on network traffic

SOFTWARE MANAGEMENT ⓘ

Enable automatic install/updates

INSTALL	UPDATE	APPLICATIONS
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Adobe Acrobat Reader
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Mozilla Firefox
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Adobe Flash Plugin
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Adobe Shockwave Player
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Skype
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Opera Browser
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Adobe Acrobat Reader
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Mozilla Firefox
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Adobe Flash Plugin
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Adobe Shockwave Player
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Skype
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Opera Browser
<input type="checkbox"/>	<input type="checkbox"/>	Adobe Shockwave Player
<input type="checkbox"/>	<input type="checkbox"/>	Skype
<input type="checkbox"/>	<input type="checkbox"/>	Opera Browser

Enable automatic scanning

PROXY ⓘ

Host:

Port:

Username:

Password:

Domain:

MISCHELANEOUS SETTINGS ⓘ

Update error retry interval

Ping forwarding interval

Ping reschedule interval

Show ballon tips in the client

Enable logging of matcher information in the client

Group Policies and Active Directory Integration

Allows you to define policies for Traffic scanning, malware detection, patching and installation for different segments of your Heimdal Corporate environment.

This gives you the option to segment your entire IT environment and create policies which apply to your exact needs across the Active Directory groups of your organisations. Heimdal policies can be made both one to one and one too many.