Heimdal®

Ransomware Encryption Protection

Heimdal®'s Ransomware Encryption Protection at a glance

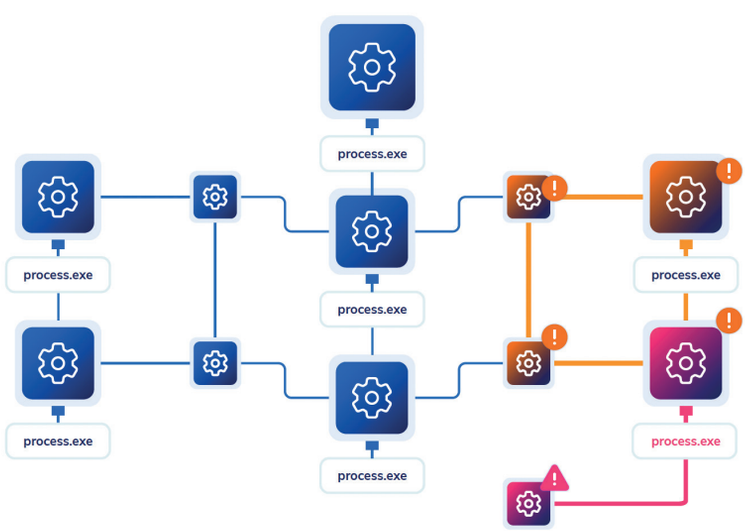
Ransomware Encryption Protection is a revolutionary % signature-free module, ensuring market-leading detection and remediation of any ransomware strain, whether file-less or file-based. This module was engineered to be universally compatible with any antivirus. Ransomware Encryption Protection extends the functionality of your antivirus instead of displacing it.

Ransomware Encryption Protection Full Technical Description

Take full control of every process running on your endpoint – the encryption protection is the only security solution on the market that can map out a previously unknown malicious activity and prevent it from DoS-ing your sensitive files.

The stunning graphic helps you understand where the ransomware originated and what it was trying to achieve. Heimdal Security's anti-ransomware software has the lowest false-positive rate in the market on account of our Intelligence, which allows us to study malicious behaviour in a safe environment.

Reporting made easy – from the dashboard, you will be able to view the full details of a malicious encryption incident; this includes time states, tree diagrams with process callbacks, PowerShell scrips, computed MD5 hash, enumeration of read\write operation performed during encryption attempts, command-line arguments, the signature of malicious process, owner, and many more.



Ransomware Encryption Protection will display an easy to follow process tree diagram after each detection of a positive malicious encryption attempt.

Ransomware has become increasingly sophisticated

Each day, over 200,000 new ransomware strain are detected, meaning that every minute brings us 140 new ransomware strains capable of evading detection and inflicting irreparable damage. Ransomware operators will never stop, not even after the victim pays the demanded ransom.

The threat actor could withhold the data, plant spyware on the victim's network or endpoints, and conduct similar attacks. Machines afflicted by ransomware can experience debilitating side-effects such as critical errors and performance issues.

SMBs and corporations bear the brunt of ransomware attacks. With kits readily available for purchase on the dark web, even a non-technical person can shut down a small or medium-sized business with subpar cybersecurity protection.

184 MILLION RANSOMWARE
attacks per year*

$20 BILLION LOST
to ransomware every year*

$115 THOUSAND AVERAGE COST
of ransomware attack*

85% OF SMBs ATTACKED
In 2020, 85% of SMBs reported a ransomware attack*

67% DEPLOYED VIS PHISHING
67% of ransomware are deployed via phishing emails*

30% OF BUSINESSES
Attacked by ransomware could regain access in less than a week*

30% OF BUSINESSES
Attacked by ransomware managed to get their data back*

Contact Brigantia

Suite 2.1, Hurstwood Business Centre, York Road, Thirsk, YO7 3BX

Tel: 020 3358 0090 | Email: partnersupport@brigantia.com | Web: www.brigantia.com

* ENISA Report for Insider Threat in 2020

Ransomware Encryption Protection

Ransomware Encryption Protection supports advanced event logging. Each encryption attempt is classified according to MD5 hash, PID, process callback, machine ID, and much more.

REP (Ransomware Encryption Protection) severs the attack chain. REP's can adapt in order to eliminate both zero-day threats and altered malicious code.

Powerful set-and-forget function – REP is universally compatible with any antivirus, offering your network powerful HIPS\HIDS capabilities, detecting and resolving any APTs that may linger on your network. Once you set up your Ransomware Encryption Protection, you don't need to worry about ransomware ever again, as any encryption attempts will be blocked by default.

REP's Insight Engine continuously analyses system processes, searching for subtle signs associated with ransomware activity –unauthorised usage of encryption functions and deletion* of Volume Shadow Copies. With passive and active scanning features, Ransomware Encryption Protection is capable of accurately filtering out grey noise (i.e. normal system operations).

*Not to be conflated with disk corruption, a typical sign of ransomware activity. REP will register VSC removal as ransomware-specific, but not the corruption of the VSC volume blocks.

Ransomware Encryption Protection: Specs & Features

Features	REP Heimdal's Ransomware Encryption Protection
Detect ransomware regardless of signature	✓
Identify Attack Origin and System Path	✓
Detect attempted kernel-level I\O, read\write operations, directory executions and file enumerations	✓
Advanced event logging (MD5, PID, read events, write events, threats, process callbacks, digital signature, machine ID, username, owner, and CVE classification)	✓
HIPS\HIDS capabilities	✓
Whitelisting and blacklisting features	✓
Graphical representation of remediations	✓
Signature-less protection	✓
Eliminates APTs	✓
Universal compatibility with any cybersecurity solution (like Antivirus or other EDR components)	✓
Comprehensive graphics and tree diagrams available after every incursion	✓

Antivirus is not enough

Countering ransomware means stopping the file encryption process.

Ransomware Encryption Protection by Heimdal is the only anti-ransomware technology capable of arresting ANY malicious encryption as it unfolds. Owing to Heimdal Security's advanced Intelligence, Ransomware Encryption Protection can distinguish between normal operating system encryption processes and malicious attempts.

Fully compatible with any antivirus, anti-malware or EDR software on the market, Ransomware Encryption Protection offers a full audit trail with stunning graphics that help you visualise the attack as it's unfolding.

Ransomware Encryption Protection empowers you to:

- Prevent data leaks.
- Secure your networks and endpoints against malicious encryption attempts.
- Eliminate downtimes associated with ransomware attacks.
- Attenuate and remove post-ransomware effects.
- Extend the detection capabilities of your existing cybersecurity software.
- Achieve higher compliance.
- Gain complete protection against zero-day threats.
- Perk up your ROI.
- Combine with any SIEM for improved policy violation detection.

Contact Brigantia

Suite 2.1, Hurstwood Business Centre, York Road, Thirsk, YO7 3BX

Tel: 020 3358 0090 | Email: partnersupport@brigantia.com | Web: www.brigantia.com