Heimdal™ Security Product Sheet

Heimdal™
E-PDR & Microsoft E5

Licensing Board Compatibility Technical Sheet

www.heimdalsecurity.com

E: sales.inquiries@heimdalsecurity.com

P: +45 7199 9177

Heimdal ™ E-PDR – Microsoft E5 Licensing Board Compatibility Technical Sheet

Microsoft's E5 Licensing for Microsoft 365 merges productivity with advanced security features, covering cloud security, information protection & access governance, Insider Risk Management & Mitigation, Azure AD, advanced eDiscovery and auditing, and business analytics. The present technical sheet will assess the compatibility rating of Heimdal™ Security's E-PDR suite with E5 Licensing for Office 356 and underline the various available additions and the manner in which these components enrich the suite's functionality.

Complementary Approach for Enhancing Productivity and Security

Heimdal™ Security's E-PDR suite provides a complementary approach to Microsoft's E5 Licensing & Security tiers, further underpropping security & user accessibility areas such as Remote Access Support, email fraud prevention, advanced email security, ACL, APT mitigation, AV protection, active ransomware monitoring and malicious encryption prevention, access governance, and malicious user containment.

Aggression response is tier-based, allowing Heimdal's E-PDR suite to fully interact with Microsoft's security features, actively augmenting their capabilities. While offering decent protection against spamming and email-delivered threats, E5's ESEC tier has severe limitations especially in the area where mods are employed to circumvent spamming rules, definitions, and exclusion lists. Furthermore, E5 offers limited to no support in the area of electronic mail fraud prevention, a shortcoming that can potentially become a liability, uncovered by an institution's or corporation's risk assessment & mitigation plan.

With ransomware aggression on the rise, the need for efficient, defender-side, countermeasures is warranted. Ransomware Encryption Protection by Heimdal™ and documented proofs-of-concept demonstrate that endpoint-based solution coupled with cloud-native protection is the most efficient defense against malicious encryption attempts, upholding information confidentiality and data integrity.

Heimdal™ Security E-PDR – E5 Licensing Harmonization

Ransomware Encryption Protection

Ransomware Encryption Protection (REP) by Heimdal™ has been designed to address malicious encryption attempts and hinder the process. Leveraging machine-learning-modeled threat Intelligence, Ransomware Encryption Protection is to identify and resolve file-based and fileless ransomware droppers.

Heimdal™ Security's anti-encryption methodology is premised on severing the bridge between the fifth and sixth links of Lockheed Martin's Cyber Kill Chain. Ransomware Encryption Protection interposes between deployment and C2 actions, actively disrupting the attack, preserving the integrity of the client's data-at-rest. The solution has been designed to work in conjunction with any Anti-Virus product including Heimdal Next-Gen Endpoint Antivirus.

Ransomware Encryption factors in I/O Reads, I/O writes directory & file enumerations, and file executions. Relevant information is fed to the Heimdal Threat Intelligence Cloud each time Insight detects anomalous activity that could point to an encryption attempt. The information collected and transmitted for in-depth analysis is the process ID, name of the process, process owner, signature, session ID, full path, command line, thread count, number of READ-type operations, number of WRITE-type operations, and the generated MD5 checksum.

In the case of Heimdal's Ransomware Encryption Protection, the Insight engine – the user-side component that actively monitors systems for malicious encryption attempts - will detect the non-system-specific file-encryption attempts and disrupt the encryption cycle at IPC level. With the attack chain disrupted, Heimdal Next-gen Endpoint Antivirus will force-scan the sector where the malicious encryption occurred, identify the malicious executable, and dispose of it. Ransomware Encryption Protection offers junk files as 'encryption bait'; this serves two purposes: to uphold important data integrity and to aid the defender in deriving a decryption key by reverse-engineering the code.

Privileged Access Management

Heimdal™ Security's Privileged Access Management gives leeway to true access governance automation by providing the administrato with advanced whitelisting and blacklisting features beyond Azure's IAM profiling and user-interaction management. The major advantage of Heimdal™ P.A.M. is the ability to automatically subvert the non-admin users' rights, a feature that facilitates the rights curation process, preventing creepers and adding an extra protective layer against Insider Threats. Elevated admin sessions are fully logged, further enforcing the user accountability factor.

Privileged Access Management by Heimdal™ Security is the only IAM\PAM that is the only de-escalation on threat detection proof-of-concept to day. Logged elevated sessions are automatically revoked and processes killed if the antiviral engine detects file-based of file-less malware on the user's machine, if the user attempts to maliciously elevate kernel-type processes or run software that abnormally encrypts files located on the machine.

The automatic de-escalation features only function if Heimdal's Next-Gen Antivirus is detected on the machine. Infinity Management dashboard adds more granular controls and elevated session rules– user rights curator can enforce an anti-system file elevation rule that prohibits the user from requesting SYSTEM-type file elevation.

Application Control

Application Control, Privileged Access Management's add-on increases the administrator's control over user-requested elevated sessions via live application whitelisting and blacklisting. App Control can block in-session apps by software name, certificate, publisher, MD5 path, or file path and is capable of curating individual rights per Active Directory Group.

Monitoring is done in passive mode by active inspection of the system's index. Every action is cataloged, with a 90-day retention rate for all elevated session approved or denied requests. Historical approval or denials can be refurbished through Application Control to automatically enforce Allow or Block administrative decisions for similar user-requested elevated sessions.

Next-Gen Antivirus

Next-Gen Antivirus by Heimdal™ Security is the baseline product that annexes Windows Defender's functionality further enhancing file-based and file-less malware detection. Local file, signature & registry objects scanning methodologies are available, as are sandboxing, backdoor inspection, process behavior-based scanning.

As a next-generation antivirus, Heimdal's product has been designed to operate in tandem with ingress\egress inspection tools, being capable of detecting and mitigation brute-force attacks.

Additionally, the Next-Gen Antivirus can also be coupled with Ransomware Encryption Protection to detect, mitigate, and resolve malicious encryption attempts.

Fully integrable with AD, Next-Gen Antivirus can be augmented with MDM capabilities for Android devices.

Being modular by design, Heimdal™'s AV and MDM can communicate with the Threat Prevention engine, actively securing & covering AV 'blindspots' – user compromise detection, identify malware that employs advanced obfuscation features, and actively detect and prevent process exploitation.

Threat Prevention

Multi-dimensional and pluri-vectorial traffic-filtering and APT mitigation solution, Heimdal™ Security's Threat Prevention Endpoint and Network ensure complete protection over zero- and n-day threats. Machine-Learning and Bloom Filter-facilitated scanning, reduce false positives, curbs latency, and minimize system footprint.

Compatible with any antiviral, anti-malware, or anti-ransomware encryption tool. Traffic-filtering functions regardless of communication protocol used for C2 or data exfiltration.

Patch & Asset Management

Handles Microsoft, proprietary, and 3rd party app patching and updating. Additional configuration required by admin for WSUS integration. No integrative components are available for Intune or SCCM. Admin scripting can further streamline the updating or patching process. Capable of correctly deliver updates and patches regarding time-zone or user availability.

Patch and updates for Microsoft, 3rd party, or proprietary are distributed via HTTPS and local P2P. All software uploaded is automatically AES encrypted by Heimdal™ Security's proprietary tool.

Email Security & Fraud Prevention

Heimdal™ Security's Email Security and Fraud Prevention modules are designed to fill in the detection and mitigation gaps left by the E5 tier. Email Security adds MX Record-based setup, threat tracing, logging, along with DKIM\SPF & DMARC sender check.

Email Security by Heimdal™ has an error margin of 0.05%, a feat offered by the combination of phase scanning, Bayesian modeling, and Pattern & hashed value filtering. Logged data can be downloaded directly from the dashboard for forensic purposes.

Added ability to deep-scan attachments and optionally block or sandbox password-protected attachments. Email Fraud Prevention factors in more than 120 attack vectors to protect users from post-infection action-on-target.

Real-time monitoring is ensured by Heimdal's fraud prevention engine. On threat detection, email is quarantined and relayed to the human team for further inspection. Additionally, the administrator can force-scan ATP on user-requested quarantine release of a suspicious object.