HEIMDAL™ SECURITY

Run either or combine Privilege Access Management and Application Control

Heimdal Privileged Access Management and Application Control

The Privileged Access Management and Application Control modules secures three major areas of the IT access infrastructure, ensuring everything works smoothly and threats are kept away: Management of privileges, App control and Auditing.

Importantly the Auditing function is granular and enables Data Protection compliance. The modules support a full audit trail of Allowed Executions, Blocked Executions and Passive Mode monitored executions, with 90-day retention for all logs.

Features of the Heimdal Privileged Access Management module:

- Allow or block requests for escalations with one click (mobile approval supported) with full control of the escalation process (auto-approval flow can be defined)
- Only fully automated de-escalation upon identification of a threat solution
- Easy to control and define rules on a per administrator basis
- Individual rights can be defined per Active Directory group (NIST AC-5 compliance)
- Option to remove existing Admin rights (NIST AC-1,6 compliance)

Features of the Heimdal Application Control module:

- Allow or Block execution of apps based on File Path, MD5, Publisher, Certificate or Software Name criteria
- Default approval for system applications
- Ability to use historical executions history for future Allow or Block decisions
- Ability to see what users have executed with full audit trail
- Comprehensive filtering functionality with 90 day retention of all logs
- Option to remove existing rights and give access to application execution (NIST AC-6 compliance)

Heimdal offers the world's only option to run either or combine Privilege Access Management and Application Control.

Contact Brigantia

Unit 7, College Business Park, Kearsley Road, Ripon, North Yorkshire, HG4 2RN

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

Upon enabling both modules, they will further enhance each other:

- Define lists of apps which can be accessed only during elevated rights sessions
- Allow access to restricted applications during elevated sessions
- Restrict access to some applications even when user rights are elevated
- Allow access to running certain apps without full elevation necessary

Benefits:

- Significant increase overall security
- Boost productivity and free of resources
- Protect revenue and intellectual property by minimising the risk of insider threat
- Save money

Available on:

65% of the damages caused by insider threat to an organisation are both financial and reputational

- ENISA Report for Insider Threat 2020

88% of organisations surveyed say that insider threat is a cause for alarm

- ENISA Report for Insider Threat 2020

40% of organisations surveyed feel vulnerable to having confidential business information exposed through insider threat

- ENISA Report for Insider Threat 2020

Contact Brigantia

Unit 7, College Business Park, Kearsley Road, Ripon, North Yorkshire, HG4 2RN

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