Remote Access Protection (RAP)

The End of Remote Breaches

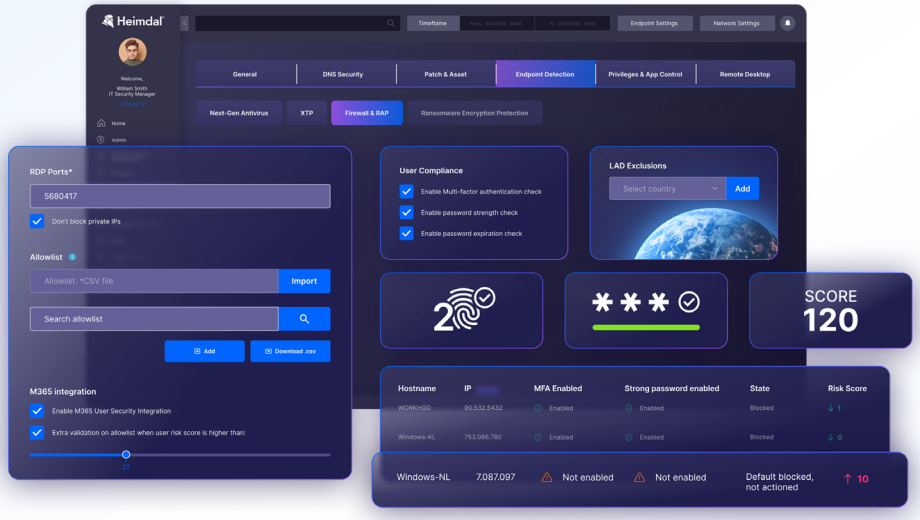
Data Sheet - Part of the Heimdal® NGAV & Firewall Suite

WHY RAP MATTERS

Attackers no longer need to break in. They log in.

Remote access abuse is one of the most common initial access methods in cyberattacks today. Whether through RDP, remote admin tools, or misused applications, attackers exploit these entry points to launch ransomware, steal data, and compromise entire environments.

Remote Access Protection (RAP) is Heimdal's answer. Sitting at the intersection of endpoint security and identity protection, RAP enforces strict access control for RDP and other remote services. It blocks all external remote access by default, only allowing connections from explicitly allowlisted IPs and ports when used with the Heimdal Firewall module. RAP also adds adaptive user risk scoring when combined with Heimdal User Security and TAC.



HOW RAP WORKS

Function	Description
Default-deny remote access (incl. RDP)	All RDP connections are blocked unless IPs are explicitly allowlisted by the admin.
Brute-Force Protection	Intelligent throttling and blocking of repeated login attempts from unknown IPs.
IP Allowlisting with Expiration	Granular control over approved IPs with optional expiration and session management.
User Validation (with TAC)	Checks MFA status, password complexity, and login anomaly history before allowing access.
Session Awareness	Tracks IP, location, login time, tool used, and user identity to evaluate the risk of each remote session.

KEY BENEFITS

Prevents RDP-based Breaches

Blocks remote desktop access by default. Only trusted, admin-approved sources get through.

Adaptive Risk-Aware Controls

Enforces access based on Microsoft 365 login telemetry, MFA status, password strength, and user risk score.

Unified Deployment

Included with Heimdal NGAV and Firewall. No extra agents or consoles required.

Integrates with Threat-hunting & Action Center (TAC)

Feeds telemetry and login patterns into TAC for broader threat hunting, response, and risk scoring.

IDEAL FOR

MSPs and MSSPs looking to secure customer environments and limit support risk from misused remote tools.

Mid-size and enterprise IT teams who need stronger access control without network complexity.

Regulated industries that require tighter controls over RDP, VPN, and session-based access.

WHAT MAKES RAP DIFFERENT

Heimdal RAP	Traditional Firewall	MFA / Identity Tools	EDR Solutions
Host-level blocking of remote access sessions	Network-level only	User authentication only	Reactive response
Context-aware RDP control	Static IP rules	Limited session context	Post-intrusion detection
Ties into user risk scoring from Heimdal TAC	No integration	No endpoint context	No pre-login enforcement

RAP supports IP and port-level allowlisting when used with the Heimdal Firewall module, offering granular access control.

INCLUDED WITH:

- **Heimdal Next-Gen Antivirus (NGAV) + Firewall**
- **Enhanced functionality when used with:**

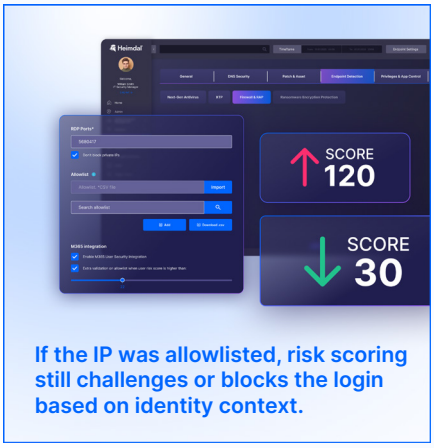
  Heimdal Threat-hunting and Action Center (TAC)

  Heimdal ITDR / User Security & Microsoft 365 Integration

RAP IN ACTION: A BREACH PREVENTED

Scenario: A threat actor obtains valid credentials from a phishing campaign and attempts to connect using a remote access tool from an unfamiliar IP.

With RAP enabled:



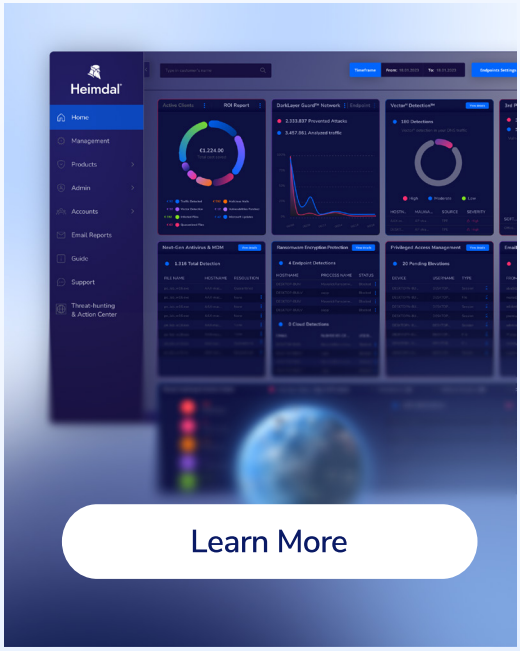
START CLOSING THE MOST ABUSED ENTRY POINT

RDP isn't going away. But it doesn't have to stay exposed.

Remote Access Protection gives you hard-stop controls at the point of login — turning one of the weakest links into a sealed entry point.

Remote Access Protection is now available as part of Heimdal's Next-Gen Antivirus and Firewall module.

Contact your Heimdal Success Manager or request a demo to see how it stops remote abuse in real time.



Capterra ★★★★★ 4.8/5 | Expert Insights ★★★★★ 4.8/5 | Gartner peerinsights ★★★★★ 4.8/5 | SOURCEFORGE ★★★★★ 4.4/5