RDS | ADVANCED SECURITY

9 powerful security features to shield RDS infrastructure and control access to corporate remote servers. RDS-Advanced Security is the intelligent solution that any good administrator needs to protect their RDS servers from external attacks.

The Most Powerful Cybersecurity Tool to Shield RDS Servers.

Download and install RDS-Advanced Security on remote servers or machines, set up the security features that you need, and be protected instantly.

600+M
Hackers IPs Blocked

9 FEATURES
To Shield RDS Servers

GLOBAL IP MANAGEMENT

Easily manage IP addresses from one place with a single list for both blocked and whitelisted IP addresses. This means that all IPs detected by Homeland and BruteForce protections are centralized here to check, edit, add or remove at convenience. IP address lists are searchable, with the possibility to make bulk actions.

INSTANT REMOTE DESKTOP SECURITY

As soon as RDS-Advanced Security is activated, RDS servers will already be shielded from 600+ million known Hacker IP addresses. A learning period enables the software to understand the standard behavior of the RDS infrastructure and adapt to it. Advanced settings allow deep customization of the level of security of each feature.

HOMELAND PROTECTION

Easily block unwanted countries and allow access from specific countries by whitelisting or blocking IP addresses. Restrict access to from the Internet and add or remove specific processes to the list.

BRUTE FORCE DEFENDER

Protect publicly accessible RDS servers from hackers, network scanners and brute-force robots guessing Administrator logins and passwords. Monitor Windows failed login attempts and automatically block offending IP addresses after a specific number of failures.

WORKING HOURS RESTRICTION

Limit RDS access during business hours. Authorize users or groups to connect during chosen days and timeslots, and enable automatic session disconnection. Specify time zones depending on user's office location. Scheduled warning messages to notify users.
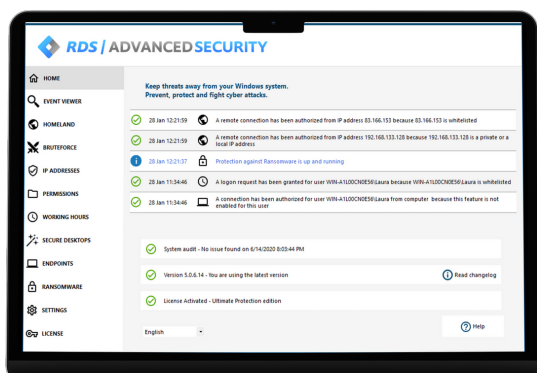
RANSOMWARE PROTECTION

RDS-Advanced Security uses behavioral detection techniques to catch ransomware unknown to antivirus and antimalware software. For a greater level of protection, it creates bait files in key folders where ransomware attacks often originate. Including a learning period to exclude standard business patterns, it reacts instantly:

- **Detects** ransowmare attacks and send real-time email alerts
- **Blocks** attacks and quarantines affected programs and files
- **Reports** the list of running processes with snapshots and recovery

RDS TOOLS

RDS | ADVANCED SECURITY

ALL-IN-ONE DASHBOARD ⌄

Easily manage and configure all security features. The user-friendly dashboard includes an event log and features status. Event interaction is possible thanks to a search bar and right click. An automatic system audit monitors the operations and security. A Lite Mode is available.

ENDPOINT PROTECTION ⌄

Decide whether a user can connect to RDS servers from any device or only specific device names. RDS-Advanced Security automatically creates a list of devices that attempt to connect, facilitating the administrator's task of accepting or denying access. By pairing devices to user accounts, Endpoint Protection prevents compromised credentials from being used to access networks.

HACKER IP PROTECTION ⌄

Instantly protect Microsoft RDS infrastructures against known on-line attacks, on-line service abuse, malware, botnets and other cybercrimes. Block 368 million malicious IP addresses from day 1.

PERMISSIONS ⌄

Manage RDS access permission for users, groups, files, folders and printers. Easily inspect and edit permissions in the side-by-side dashboard. Choose from four permissions: Deny, Read, Modify or Ownership, and three views inspection.

SECURE DESKTOP ⌄

Configure the RDS security level for each user or group. Select between three standardized RDS security levels:

- Windows Mode: access to default Windows session
- Secured Desktop Mode: access to documents, printers, Windows key and session disconnection
- Kiosk Mode: prevent a connected user from running prohibited actions.

PRE-REQUISITES ⌄

1   **HARDWARE**
RDS-Advanced Security supports 32-bit and 64-bit architectures.

2   **OPERATING SYSTEM**
RDS-Advanced Security is compatible with Microsoft Windows version 7, Service Pack 1 (build 6.1.7601) or Windows 2008 R2, Service Pack 1 (build 6.1.7601) or higher.

2   **SOFTWARE**
- Runtime: .NET Framework 4.5.3 or higher
- Microsoft Windows 7 SP1 and Windows 2008 R2 SP1 require an additonal update to support SHA2 Cross Signing (KB4474419). This update allows RDS- Advanced Security built-in firewall and ransomware protection to run properly.

🏢   RDS-Tools Software

🌐   www.rds-tools.com

📍   63 Rue André Bollier, 69307 Lyon, France

RDS TOOLS