RDS-Knight

The right weapon against cyber-criminals

Cyber Criminals Know You Use Remote Desktop systems

At the risk of stating the obvious, cyber security – protecting business, supplier and customer data from nasty and damaging digital intruders, should now be a high priority for every organization. Working in a top discipline like delivering products and services, it's probably fair to say that most of us should be doing more in terms of cyber security. The risks and consequences cannot be underestimated and clearly, the problem is not going to go away anytime soon.

No longer an 'if' question, cyber-crime is undoubtedly a 'when'. Following a recent survey, a chamber of commerce reported that around 55% of firms in a single county have been hit in the past two years. **In terms of business risks and associated consequences, Remote Desktops must be shielded and protected.**

Most organizations assume that the hackers who threaten them will be motivated by the value of the information the company uses to provide its services. The truth is that cyber criminals don't necessarily care about the value of corporate, personal and/or financial data. Many attacks are perpetrated on systems because there's value in the processing power of the systems themselves.

As Windows infrastructures grow and evolve, it gets more and more difficult for security experts to see all the endpoints in their architecture. And you need to know your Remote Desktop vulnerabilities to mitigate your risk. **RDS-Knight** consists of a robust and integrated set of security features to protect against these Remote Desktop attacks.

This software approach combines advanced technology as well as the latest lessons and insights our elite team of Remote Desktop cyber security specialists brings back from real-world missions. **RDS-Knight is available in two editions:**

RDS-Knight *Security Essentials* is **the best package to keep your Remote Desktop connection safe**, with powerful protection features. It is the low-cost security solution you can even apply to all W7/W10 Pro RDP accesses.

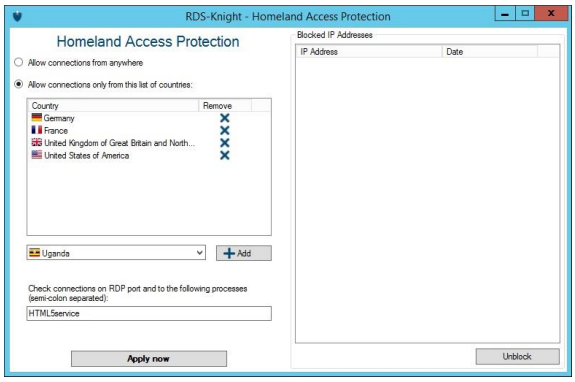
RDS-Knight *Ultimate Protection* is the security tool every Windows Server administrator "Must Have": it provides all that you need to effectively protect your users' environments and prohibit malicious actions.

RDS-Knight provides 6 major protections

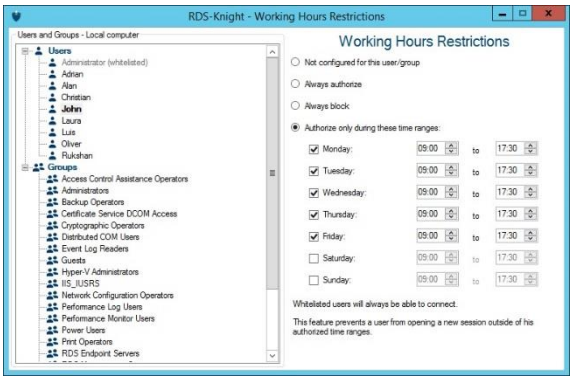
➢ Prevent foreigners to open a session.

Your users are located in Germany, France, Italy and the USA. Why would you allow any user to connect from other countries?

This feature is included in RDS-Knight Security Essentials.



➢ Prevent users to connect at night.



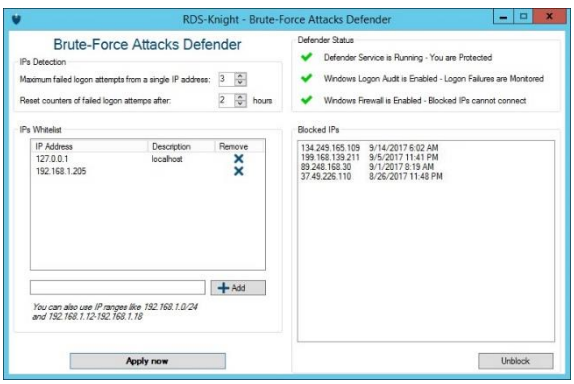
Users are working during daytime and they are not allowed to connect out of their working hours. It is as simple as that! Any user connecting at night will be automatically logged out of the system.

This feature is included in RDS-Knight Security Essentials.

➢ Avoid brute-force attacks.

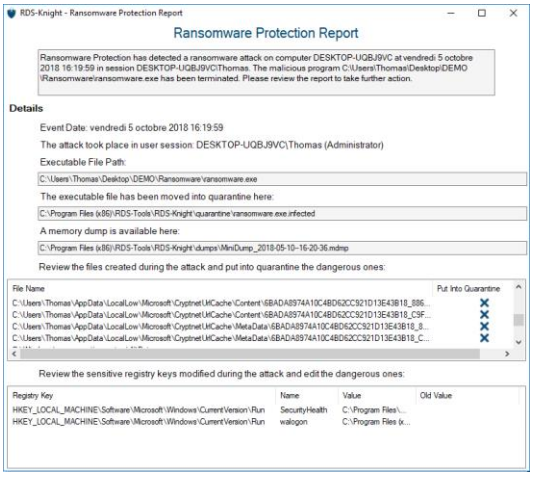
Stop the constant attacks right now with **RDS-Knight** brute-force attacks defender. It **will instantly protect your server** by monitoring Windows failed login attempts and automatically blacklist the offending IP addresses after several failures.
Moreover, you can configure it to match your needs.

This feature is included in RDS-Knight Security Essentials.

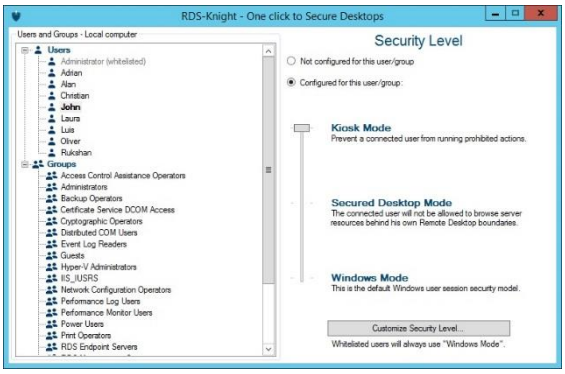


➢ Detect and Stop Ransomware.

Ransomware are the most significant of today's cyber threats. Their actions on your systems will either completely lock your access or encrypt the majority of your files until you pay the ransom cyber criminals request. **RDS-Knight Anti-Ransomware protection** will efficiently detect, block and prevent ransomware attacks. It will prevent your business from catastrophic consequences by removing the ransomware at an early stage.



Learn how to anticipate these threats with reports showing the source of the attack



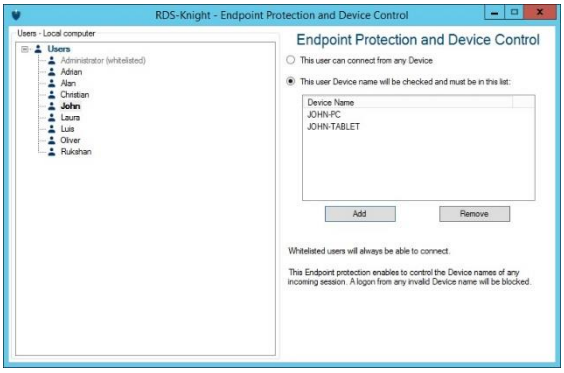
A logon from any invalid device will be blocked.

➢ Protect users' profiles.

Windows systems are providing too many features and only few experts can properly manage this kind of complexity. Most of us are not skilled enough to set up security rules and to hide Windows features from users' Remote Desktops. Like a dream, **RDS-Knight will enforce for you the security level you want** to secure your RDS server. And the best is that you can do it **"user per user", or per group**.

➢ Prohibit connection from non-authorized devices.

With the rise of BYOD and remote working, where technology allow users to connect and work from everywhere with their own device, you need to be sure that every device can be controlled and kept safe. Thanks to **RDS-Knight,** you can either allow your user to use any device, or just **allow him/her an access with a specific device** by entering its name, which will be checked by the endpoint protection.

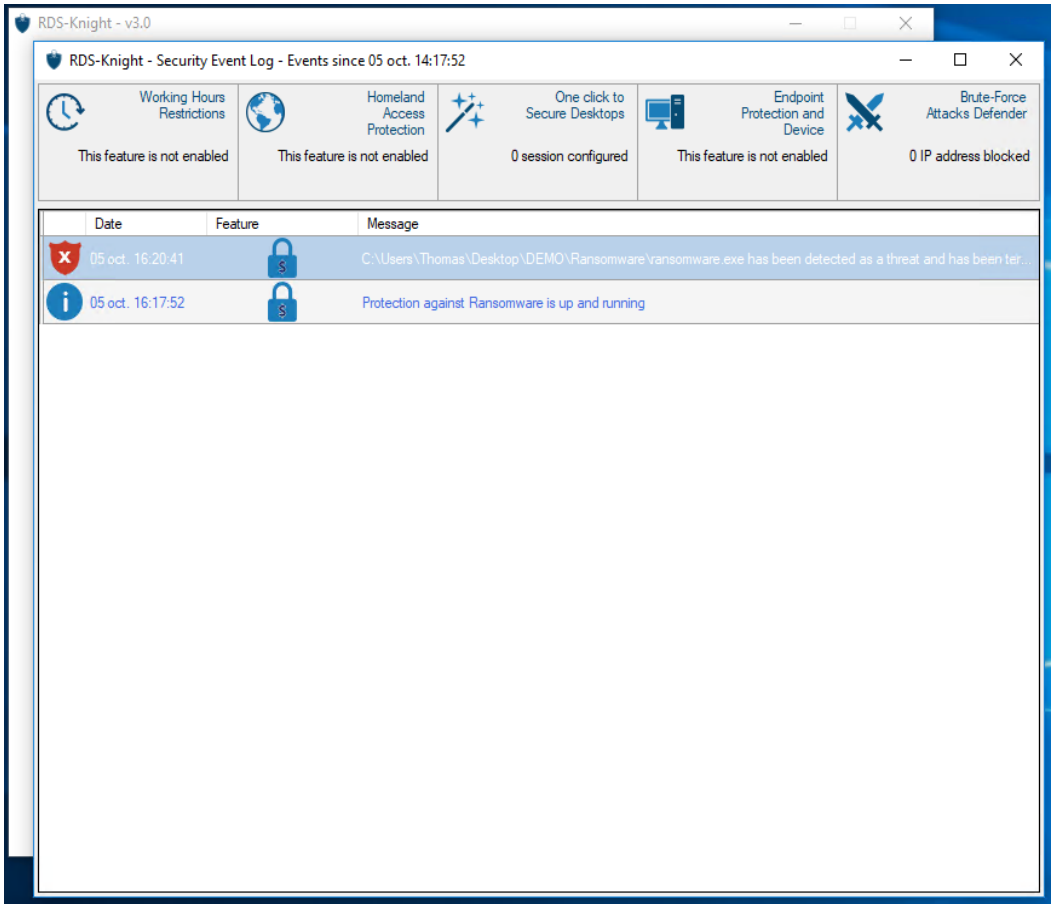


As soon as you apply it, users will benefit from a protected environment.

➢ Check RDS-Knight defensive job in Real-time.

With the **Security Event Log,** you can display all detailed information regarding events, and keep track of any logon request and configuration in real time, such as:

- Blocked, Failed or Granted connections.
- Stopped Attacks and Quarantined files.
- Configured User Sessions.



Keep threats out of your Windows system.
RDS-Knight will protect you against Remote Desktop attacks.

Pre-requisites

RDS-Knight is compatible with the following 32 and 64-bit OSs:

- Windows 7 to Windows 10
- Windows Server 2008 R2 to Windows Server 2016

Download a 15-days free trial