



RDS-Knight

The right weapon against cyber-criminals

Cyber Criminals Know You Use Remote Desktop systems

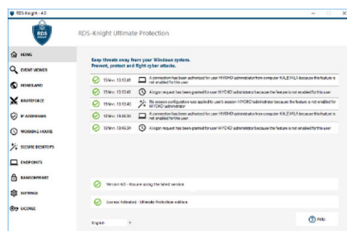
At the risk of stating the obvious, cyber security – protecting business, supplier and customer data from nasty and damaging digital intruders, should now be a high priority for every organization. Working in a top discipline like delivering products and services, it's probably fair to say that most 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.

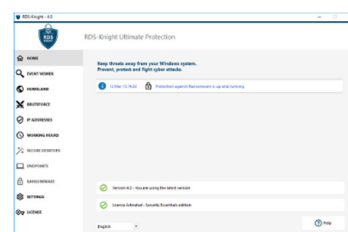
As Windows infrastructures grow and evolve, it gets more and more difficult for security experts to see all the endpoints in their architecture. And you need to know your Remote Desktop vulnerabilities to mitigate your risk. **RDS-Knight** consists of a robust and integrated set of security features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

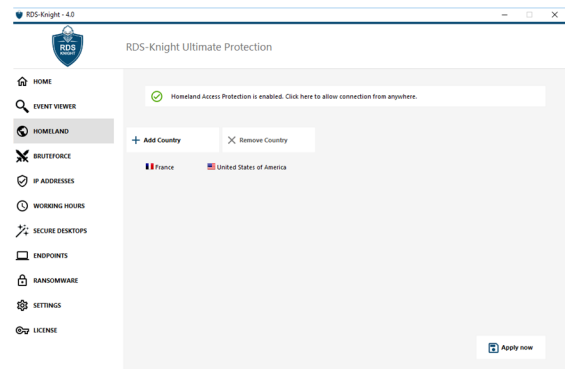


RDS-Knight provides 6 major protections

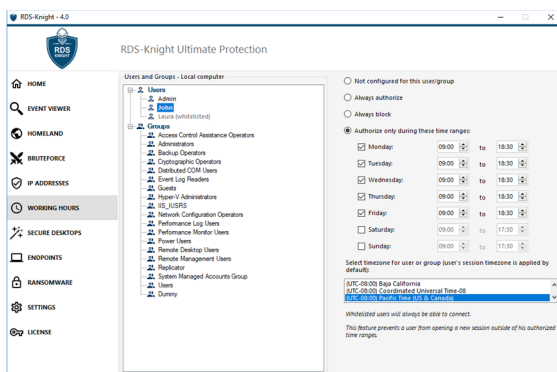
➤ Prevent foreigners to open a session.

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

In a snap with **RDS-Knight**, protect your TSplus servers from hackers trying to open a session from foreign countries. This is extremely simple and so powerful. Just do it!



This feature is included in RDS-Knight Security Essentials.



This feature is included in RDS-Knight Security Essentials.

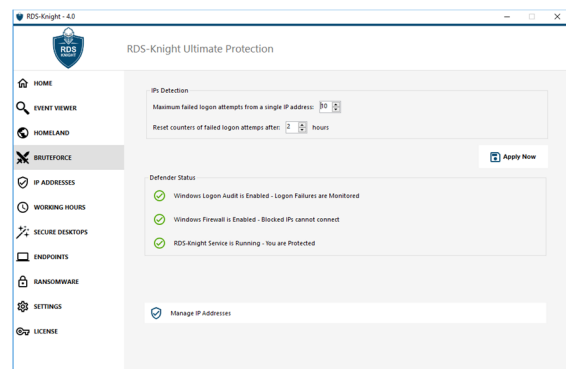
➤ Prevent users to connect at night.

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.

➤ 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.

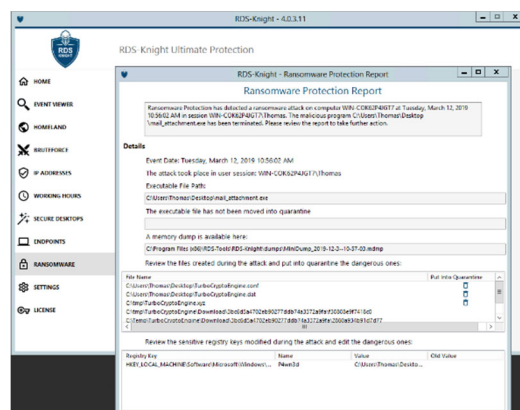
Moreover, you can configure it to match your needs.



This feature is included in RDS-Knight Security Essentials.

➤ Detect and Stop Ransomware.

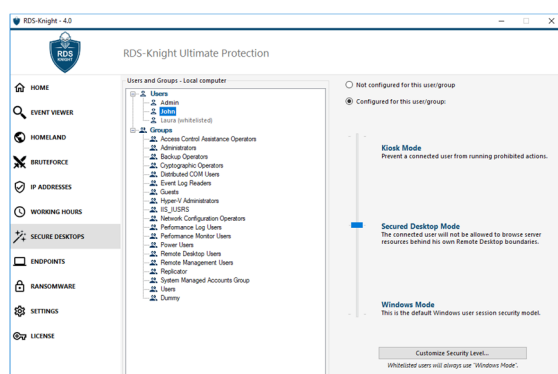
Ransomware are the most significant of today's cyber threats. Their actions on your systems will either completely lock your access or encrypt most of your files until you pay the ransom cyber criminals request. **RDS-Knight Anti-Ransomware protection** will efficiently detect, block and prevent ransomware 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

➤ Protect users' profiles.

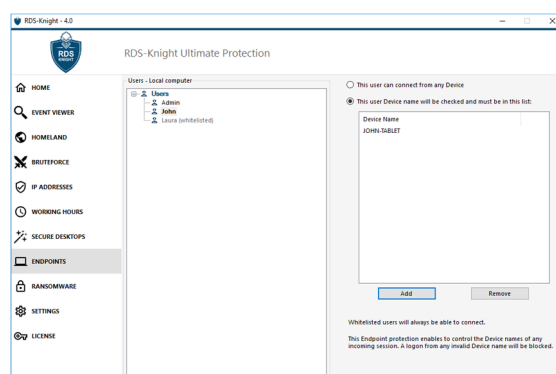
Windows systems are providing too many features and only few experts can properly manage this kind of complexity. Most of us are not skilled enough to set up security rules and to hide Windows features from users' Remote Desktops. Like a dream, **RDS-Knight will enforce for you the security level you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



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

➤ 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.



A logon from any invalid device will be blocked.

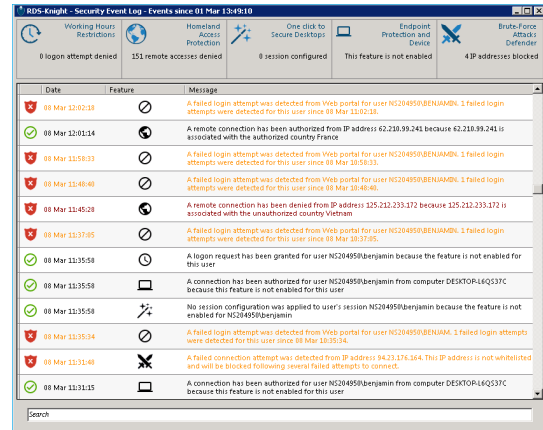
Easy to Manage

Check RDS-Knight defensive job in Real-time.

With the **Security Event Log**, display all detailed information regarding the last 2500 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.

This offers a more relevant alternative than a full audit solution. Plus, a deep global search is also available in order to find specific events quickly.

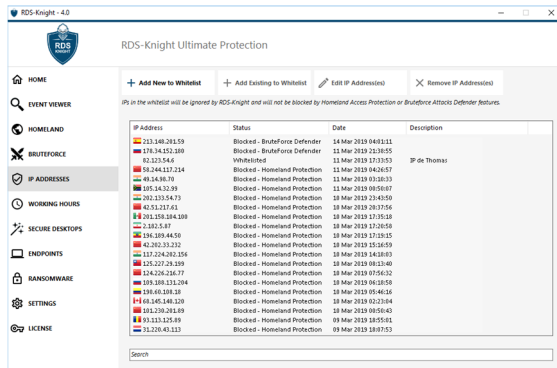


Date	Feature	Message
08 Mar 12:02:18	⊗	A failed login attempt was detected from Web portal for user NS204950BENJAMIN. 1 failed login attempt was detected for this user since 08 Mar 11:02:18.
08 Mar 12:01:14	⊗	A remote connection has been authorized from IP address 62.218.99.243 because 62.218.99.243 is associated with the authorized country France.
08 Mar 11:58:33	⊗	A failed login attempt was detected from Web portal for user NS204950BENJAMIN. 1 failed login attempt was detected for this user since 08 Mar 11:58:33.
08 Mar 11:49:48	⊗	A failed login attempt was detected from Web portal for user NS204950BENJAMIN. 1 failed login attempt was detected for this user since 08 Mar 11:49:48.
08 Mar 11:45:28	⊗	A remote connection has been denied from IP address 125.212.235.172 because 125.212.235.172 is associated with the unauthorized country Vietnam.
08 Mar 11:37:05	⊗	A failed login attempt was detected from Web portal for user NS204950BENJAMIN. 1 failed login attempt was detected for this user since 08 Mar 11:37:05.
08 Mar 11:35:58	⊗	A login request has been granted for user NS204950BENJAMIN because the feature is not enabled for this user.
08 Mar 11:35:58	⊗	A connection has been authorized for user NS204950BENJAMIN from computer DESKTOP-UQ537C because this feature is not enabled for this user.
08 Mar 11:35:58	⊗	No session configuration was applied to user's session NS204950BENJAMIN because the feature is not enabled for NS204950BENJAMIN.
08 Mar 11:35:34	⊗	A failed login attempt was detected from Web portal for user NS204950BENJAMIN. 1 failed login attempt was detected for this user since 08 Mar 11:35:34.
08 Mar 11:31:48	⊗	A failed connection attempt was detected from IP address 94.23.176.164. This IP address is not whitelisted and will be blocked following several failed attempts to connect.
08 Mar 11:31:15	⊗	A connection has been authorized for user NS204950BENJAMIN from computer DESKTOP-UQ537C because this feature is not enabled for this user.

See and search amongst the 2500 last events on the Security Event Log

Unified and Efficient IP Addresses Management

IP addresses management is made easy with a single list to manage both blocked and whitelisted IP addresses. A convenient search bar provides search capabilities based on all information provided. Further, administrators can perform actions on several selected IP addresses with a single click, such as unblocking and adding to whitelist multiple blocked IP addresses. It's also possible to provide meaningful descriptions to any IP addresses.



IP Address	Status	Date	Description
211.148.281.59	Blocked - BruteForce Defender	14 Mar 2019 04:03:11	
176.34.552.180	Blocked - BruteForce Defender	15 Mar 2019 21:38:55	
42.215.54.6	Whitelisted	12 Mar 2019 12:35:53	IP de Thomas
58.244.117.214	Blocked - Homeland Protection	15 Mar 2019 04:26:57	
49.14.186.70	Blocked - Homeland Protection	15 Mar 2019 03:10:33	
105.16.52.39	Blocked - Homeland Protection	15 Mar 2019 06:06:07	
202.135.54.73	Blocked - Homeland Protection	15 Mar 2019 23:43:50	
42.137.171.61	Blocked - Homeland Protection	15 Mar 2019 20:17:54	
201.158.124.4309	Blocked - Homeland Protection	15 Mar 2019 17:35:58	
2.126.5.87	Blocked - Homeland Protection	15 Mar 2019 17:28:56	
194.189.44.50	Blocked - Homeland Protection	15 Mar 2019 15:15:15	
42.202.33.232	Blocked - Homeland Protection	15 Mar 2019 15:16:55	
112.124.262.154	Blocked - Homeland Protection	15 Mar 2019 14:03:03	
125.227.28.109	Blocked - Homeland Protection	15 Mar 2019 08:13:40	
124.206.236.77	Blocked - Homeland Protection	15 Mar 2019 07:56:12	
105.189.121.204	Blocked - Homeland Protection	15 Mar 2019 06:18:59	
181.46.108.38	Blocked - Homeland Protection	15 Mar 2019 05:41:24	
146.245.545.120	Blocked - Homeland Protection	15 Mar 2019 02:33:04	
101.230.281.89	Blocked - Homeland Protection	15 Mar 2019 00:50:42	
93.233.125.89	Blocked - Homeland Protection	09 Mar 2019 18:55:01	
71.226.43.113	Blocked - Homeland Protection	09 Mar 2019 18:07:53	

Add/Edit or Remove IP Addresses from the whitelist

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 2019

Download a 15-days free trial