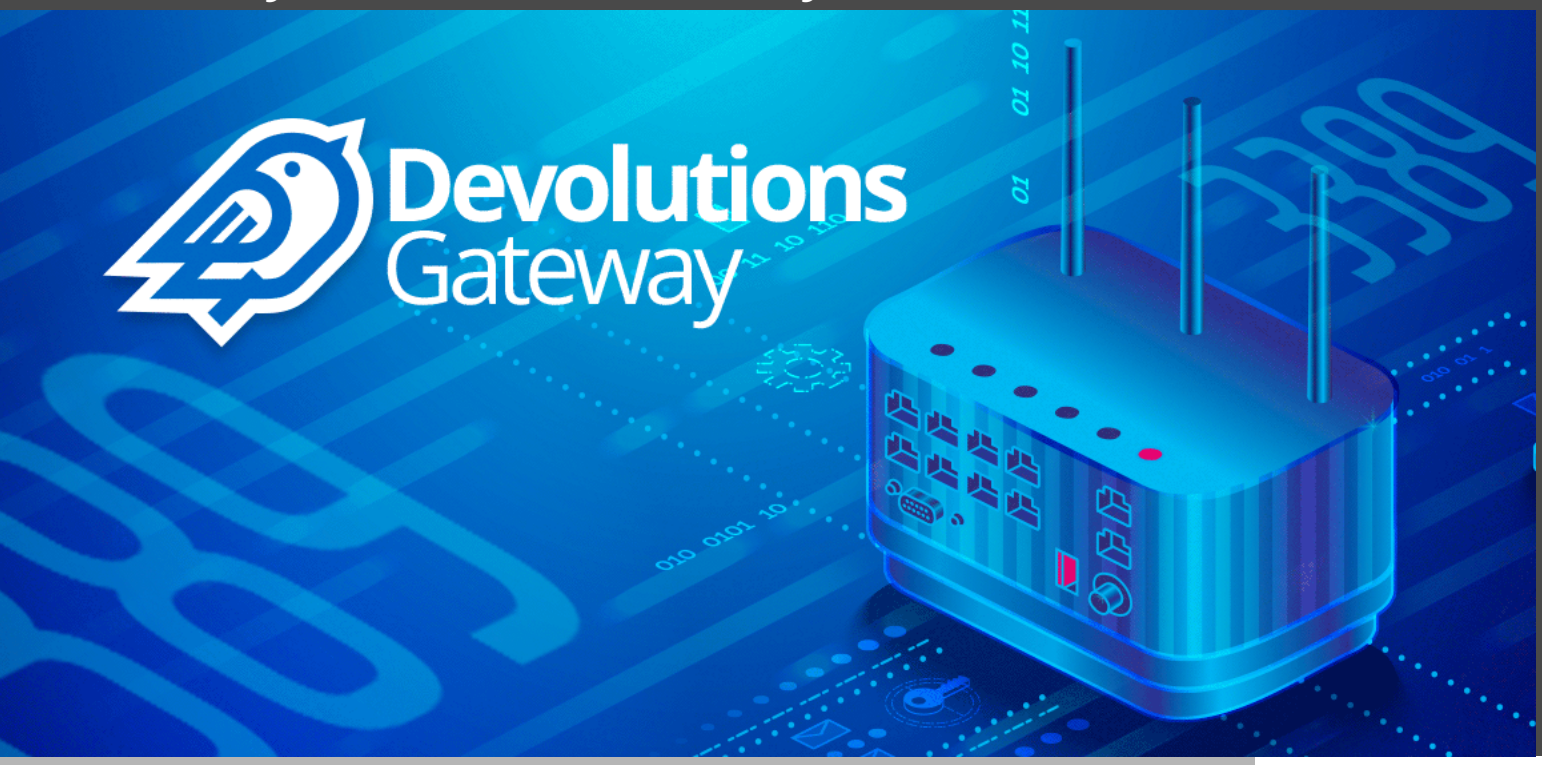
Devolutions

[NEW] Use Case: How Organizations That Use RDP Can Improve Security, Performance & Functionality by Switching from RD Gateway to Devolutions Gateway



THE MICROSOFT REMOTE DESKTOP PROTOCOL (RDP) SHOULD NEVER BE EXPOSED DIRECTLY ON THE INTERNET

The Microsoft Remote Desktop Protocol (RDP) should never be exposed directly on the Internet (port 3389). As such, Microsoft advises deploying the Remote Desktop Gateway (RD Gateway) for secure access.

However, there are some key problems with this approach:

- **Since the RD Gateway protocol uses Windows authentication (NTLM/Kerberos) over HTTP, external malicious actors can exploit this vector to launch brute force and password spraying attacks against Active Directory.**
- **The RD Gateway degrades network performance by tunneling RDP TLS over HTTPS (TLS in TLS connections).**
- **Enforcing multi-factor authentication (MFA) on the RD Gateway connections is known to be particularly difficult.**

The good news is that there is an effective and affordable solution: Use **Devolutions Gateway** in conjunction with **Devolutions Server** and **Remote Desktop Manager**.

In our new case study (which includes how-to steps), you will discover how this approach:

- **Enhances security** by enforcing MFA via Devolutions Server authentication on all Devolutions Gateway RDP connections.
- **Reduces exposure** by tunneling external RDP connections, but without exposing Active Directory accounts to brute force attacks.
- **Improves network performance** through efficient RDP connection tunneling that, unlike the RD gateway, does not use TLS in TLS connections.
- **Expands visibility** for just-in-time (JIT) RDP connections, and supports detailed centralized session tracking and auditing.

Click here to instantly download the Use Case [PDF].

Click here for a full list of Use Cases that are also available for download.