

Cloud Security Tips to Ease the Transition from GroupWise to the Cloud



Reports of the state of [cloud security](#) in 2019 show a good news/bad news scenario. The good news for GroupWise users contemplating a move to the cloud? Security offerings have improved. And most cloud service providers stay on top of infrastructure security. In fact, none of the high-profile breaches of 2018 resulted from cloud service provider negligence.

The bad news? Organizations have largely failed to keep pace with emerging security technologies. Misconfiguration ranks a close second to credential hijacking as the most common cause of security breaches. Less than half of organizations with data in the cloud encrypt that data. And only one third of organizations use single sign-on to protect access.



**Novell.
GroupWise.**



Take Responsibility for Cloud Security

Too many organizations move data to the cloud and breathe a sigh of relief, mistakenly thinking that the cloud service provider will now take over the security reins. All too often, a wakeup call comes in the form of a security breach, compromised data and loss of trust. The organization realizes abruptly that it should have paid more attention to configuration details.

For example, consider the case of an organization moving from [GroupWise to Office 365](#). Microsoft ensures the integrity of the infrastructure. They manage the servers and storage and keep the operating system and application software up-to-date. The customer organization, on the other hand, handles security at the data level.

That is, the customer must ensure effective system configuration. This includes determining strict access controls and backup policies, enabling data encryption and properly implementing available security controls.



Harness the Power of Microsoft's Security Tools

Many former GroupWise users choose to [migrate to Office 365](#). Fortunately, Microsoft offers a number of sophisticated cloud security tools to help ensure data safety and regulatory compliance. Some of these include:

- **Microsoft Secure Score** – The Security Center rates your organization's security posture, giving points for performing recommended tasks and configuring security features. It then provides recommendations for further actions to take to improve security.

- **Office 365 Security Center** – This dashboard allows you to view reports and perform many essential security tasks from a single location. For instance, you can enable multi-factor authentication and role-based access control. You can also define policies for device management and threat protection, and you can define alerts for certain actions.
- **Microsoft Cloud App Security** – Cloud App Security allows you to discover and monitor cloud apps in use at your organization, including shadow IT. You can block risky apps and even monitor managed devices outside the corporate firewall. In an age of multi-cloud environments, these capabilities can prove crucial.
- **Microsoft Office 365 Advanced Threat Protection** – This service provides email filtering to protect against zero-day threats. It protects against unsafe attachments, keeps users from clicking on malicious links, detects email spoofing and provides anti-phishing controls.
- **Microsoft Defender ATP** – This platform focuses on endpoints and uses big data and machine learning to detect anomalies quickly and automatically respond to threats.
- **Compliance Manager** – Designed to help organizations achieve and maintain regulatory compliance, this risk-assessment tool includes customer-managed controls for common regulations such as GDPR and HIPAA. Continuous monitoring and recommended actions help organizations improve their compliance score.

Tap into Proven Expertise

Balancing the benefits of the cloud with the risk of cyber-attack requires a comprehensive approach to [cloud security](#). Fortunately, emerging technologies provide a cloud-native approach to the unique challenges in this new environment.

The consultants at Messaging Architects will guide you through your safe transition to the cloud. From pre-migration consultations through defining security controls and conducting ongoing risk assessments, we will help you securely navigate the cloud.