

Cloud-based Security Solutions Deliver Powerful, Scalable Protection for SMBs



The average small to medium business (SMB) has most likely migrated at least some essential data and operations to the cloud. At the same time, SMBs face increasingly strict privacy regulations, as well as a growing number of cyber attacks. And with a mobile, often remote, workforce, the environment demands reliable, cloud-based security solutions.

As the security landscape grows more complex, many SMBs find that they lack the in-house expertise needed to keep data safe. And as they move more sensitive information to the cloud, protecting that data requires proactive solutions. Businesses need the ability to predict data breaches rather than simply providing damage control after the fact.

Cloud-based security solutions offer significant advantages over traditional approaches, from budget impact to ease of use. Consider these benefits then learn the features to look for in a solution that will keep your data safe from attack.

Benefits of Cloud-based Security Solutions

While the resources available to SMBs differ significantly from those available to large enterprises, organizations of all sizes face similar cyber threats. In fact, cyber criminals have increasingly turned their attention to smaller businesses. Fortunately, one prominent benefit of cloud-based security lies in the scalability of the solutions. You pay for what you use.

Additionally, traditional security solutions require significant expense and expertise to purchase and maintain equipment and software. [Cloud-based security](#), on the other hand, requires little to no capital expense. It is relatively easy to configure and manage, and the cloud environment ensures access to up-to-date protection.

For example, using a cloud security provider, a small business can feasibly set up a solution in a matter of hours. The solution works behind the scenes, with no impact on performance, blocking attacks and providing alerts to unusual activity. Regular reports and a comprehensive dashboard provide visibility into data and access.



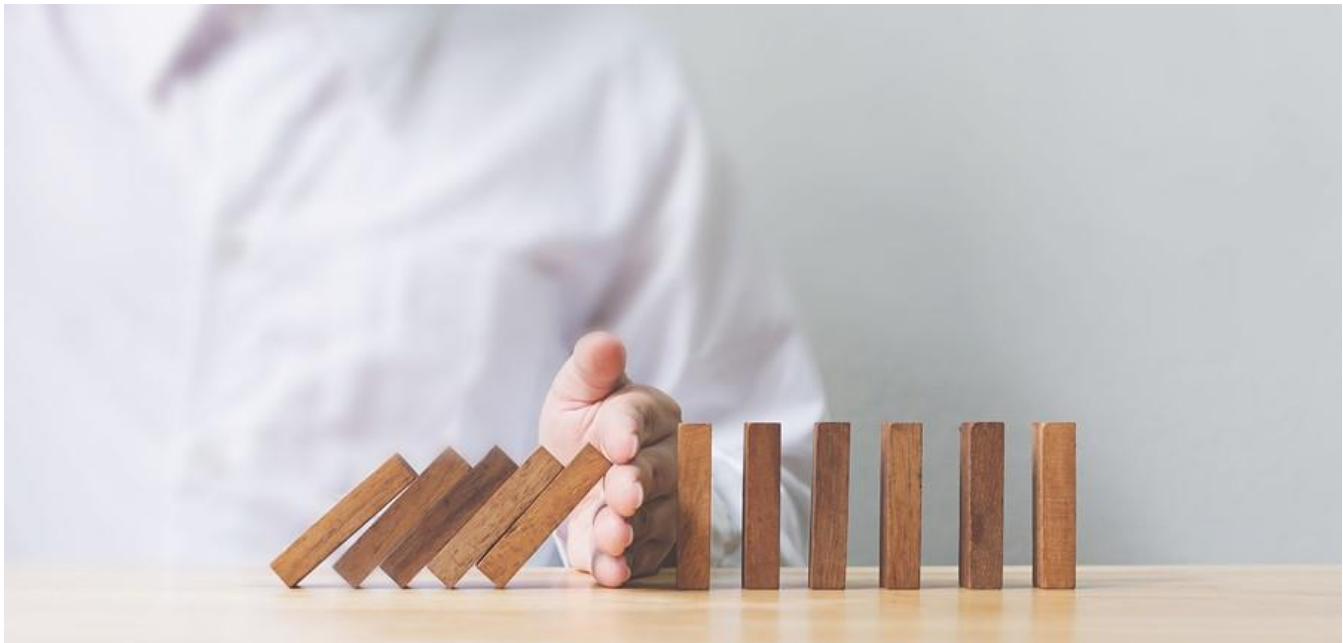
Features to Look for in Cloud-based Security

When choosing cloud-based security solutions, businesses should first identify the data and workflows they need to protect. Armed with that information, they can choose a solution that provides protection for that workload. For example, does the business use multiple clouds or virtual machines? Will the cloud security solution need to integrate with on-premises directory systems?

Some key features to look for include the following:

- **Cloud-native** – Traditional security measures fall short in cloud environments, where the perimeter has expanded exponentially. Choose cloud-first security solutions built to meet the challenges unique to the cloud.
- **Automation** – Security threats evolve at lightning speed. Manual security practices that rely on human monitoring and legacy software cannot keep up. Look for automation and AI-driven solutions that provide real-time protection from most threats. Additionally, look for the ability to automate enforcement of acceptable use policies.

- **Encryption** – Typically, cloud vendors and businesses share responsibility for encryption. Ensure full encryption at the file level, protecting data both in transit and at rest. Look for vendors that stay abreast of [advancements in data encryption](#).
- **Access management** – Choose solutions that provide comprehensive access management at a granular level, including role-based and risk-based access. Additionally, look for multi-factor authentication and access monitoring.
- **Data loss prevention** – Data loss prevention (DLP) includes tools to classify regulated data and enforce the protection of that data with encryption and detailed monitoring. Reporting capabilities within DLP systems enable regulatory compliance.
- **Superior service** – Choose security providers with a reputation for excellent service. This should cover initial implementation, as well as ongoing, remote maintenance. Look for extensive monitoring and reporting capabilities.
- **Ability to work in a multi-cloud environment** – Most organizations use a mix of public and private clouds. Your provider should work seamlessly across multiple clouds.



Proactive Protection with eCare Secure Route

eMazzanti Technologies has been providing critical security for businesses of all sizes for nearly 20 years. With [eCare Secure Route](#), we deliver scalable, enterprise-grade security built for the cloud. IT managers deploy quickly and manage security easily through a web-based dashboard.

In addition to providing ease of use, eCare Secure Route uses machine learning to protect against emerging threats before an attack occurs. In fact, the solution stops up to 98 percent more attacks than traditional security solutions. Call eMazzanti today to learn more about [protecting vital information assets](#) in the cloud.

2015 | 2013 | 2012 Microsoft
Partner of the Year



Inc. 500 || **5000**
2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010



ShoreTel Sky
Partner of the Year