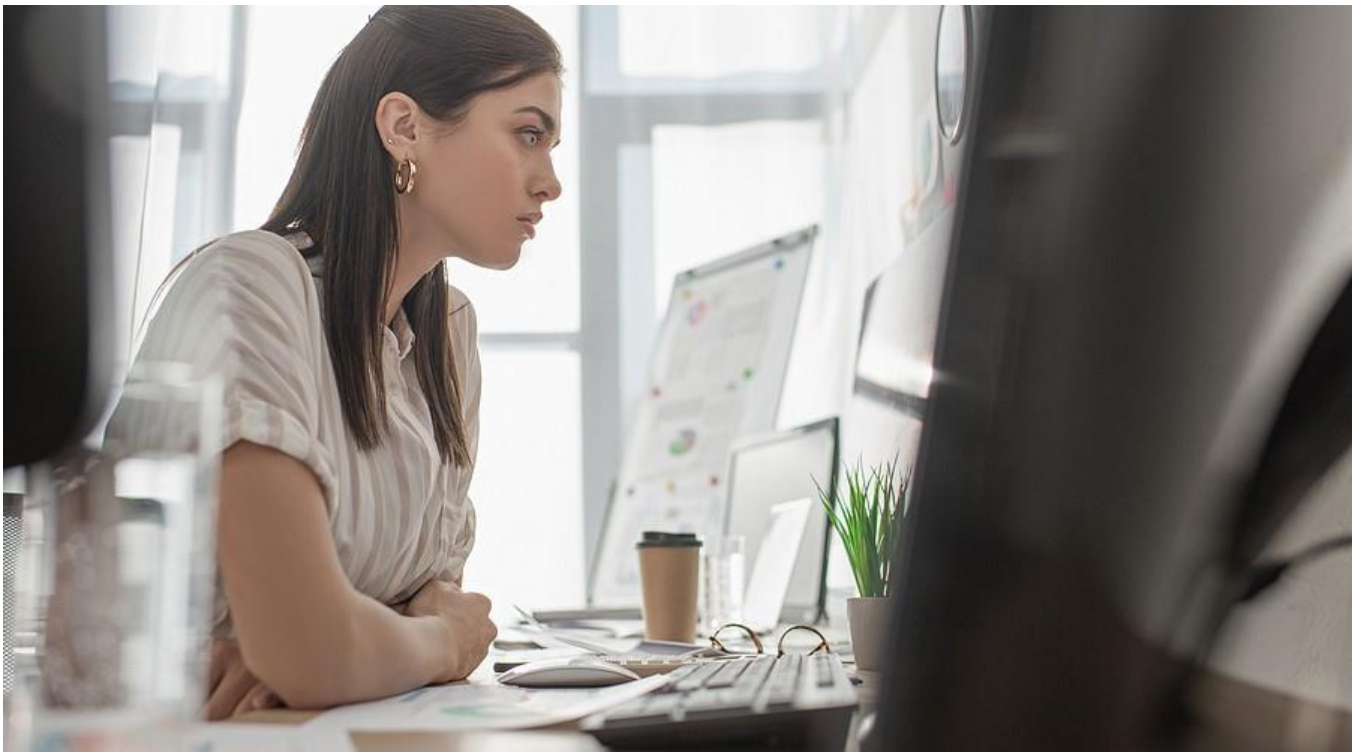
Default Cloud Security Tools May Not Provide Enough Protection



In the past decade, most businesses have moved at least some of their workloads to the cloud. This allows SMBs to use enterprise-class tools, and it delivers business agility to companies of all sizes. However, these benefits come with increased security risks. Cloud providers offer default cloud security tools, but these free tools can leave companies vulnerable.

Opportunity Comes with Risk

Moving to the cloud makes good business sense and may, in fact, prove a necessity for companies to remain competitive. It facilitates remote work and collaboration, and scalability means that businesses can easily expand storage and tools to match growth.

At the same time, the new landscape brings new risks. For instance, in a public cloud, one server may store data from multiple companies. And, while cloud providers generally place a priority on security, no system can promise complete protection. A single successful breach of a cloud provider could have disastrous effects for dozens, even hundreds, of companies.

Additionally, operating in the cloud complicates regulatory compliance. Many regulations require companies to document exactly who has access to the data and how sensitive data is secured. Using a cloud provider means introducing the possibility for additional insider threats and surrendering a substantial amount of control and visibility.

Default Cloud Security Tools Leave Businesses Vulnerable

To help customers keep data secure, cloud providers offer built-in security tools, often for free. While these default tools may satisfy compliance checkboxes, they can give organizations a false sense of security. All too often, customers misconfigure the security controls, leaving data vulnerable. And in many cases, the default tools provide inadequate protection.

For instance, Microsoft Windows Defender provides antivirus protection. It does a decent job at delivering the basics, such as detecting malware. But it falls far short of the competition in blocking phishing sites, and it does not offer additional tools like dark web monitoring or a password manager.

Whether or not the default security tools will suffice depends somewhat on the organization's environment. For example, a business that needs to secure data in multiple clouds will benefit from third-party security tools. Default security tools from one vendor typically do not work effectively with offerings from another vendor.

Likewise, businesses that use the cloud to process or store highly sensitive workloads and data need superior security strategies.

Choosing Effective Security Solutions

When determining the right cloud security strategy, organizations should look for several key features, including:

- Encryption – The cloud provider and the customer share responsibility for encrypting data in transit and at rest. Ensure full encryption at the file level using the appropriate type of encryption method for the security challenges involved.

- Automation – Hackers use sophisticated, automated tools to cripple their targets. Consequently, security solutions must use automation and artificial intelligence to deliver effective countermeasures.

- Access management – A competitive security solution will provide role-based and risk-based access management at a granular level. It should also provide for access monitoring and multi-factor authentication.
- Data loss prevention (DLP) – DLP software classifies and monitors critical data to reduce the risk that sensitive data will fall into the wrong hands. Additionally, it provides reporting capabilities necessary for compliance audits.
- Ability to work in a multi-cloud environment – Choose a security solution that works seamlessly across a mix of public and private clouds.

Comprehensive Cloud Security with eMazzanti

While default security tools provide checkbox security, eMazzanti aims higher. For example, with eCare Secure Route, businesses benefit from predictive intelligence to stop malware and phishing attempts over any protocol, port, or app. In fact, this solution halts 50 to 98 percent more attacks than antivirus and firewalls alone, with no added latency.

eMazzanti offers a comprehensive suite of security tools and services. Starting with a free cybersecurity assessment, we will tailor a solution to meet your business needs and protect valuable digital assets.