aws small and medium business

AMAZON WEB SERVICES

Three Essential Considerations for Securing Your Business

AWS SMB | MAY 2022

Security Impacts Every Part of Your Business.

The digital transformation of small and medium-sized businesses has created efficiencies, new business models and opportunities for growth. As companies take advantage of digital strategies to better run their businesses and improve engagement with customers, strengthening data security is front and center. It's estimated that 43 percent of cyber issues now target small or medium-sized businesses.[1]

Securing your organization impacts everything from capex budgets, operations, profitability, and even your brand's reputation. Limited IT resources can mean more unprotected points of entry. In addition, your industry or government might require you to comply with security and privacy regulations. Trying to manage a rapidly evolving security environment can get in the way of your ability to scale your digital footprint as you grow.

1. Fundera, **"Surprising Small Business Cyber Security Statistics,"** 2021.

Why Should You Consider the Cloud?

The cloud gives small and medium-sized businesses an opportunity that they've not had previously–to achieve their security, risk, and compliance requirements with a level of automation and visibility that would not be possible if they were relying solely on internal resources. The cloud can immediately improve your security posture in three essential ways: physical security, compliance, and flexibility.

When comparing cloud security with investing in your own infrastructure, resources, and tools, there are three essential security considerations: physical security, compliance, and flexibility. For small and medium-sized businesses, which often face staffing and budget constraints, the cloud usually delivers the greatest return.

1 **Physical security**

Housing servers, storage devices, and networks in a safe and secure location is a fundamental requirement for protecting against theft and tampering. It's also imperative to keep IT infrastructure updated with application and security releases to prevent vulnerability.

In the cloud model, a trusted cloud provider manages the security of the foundational IT infrastructure and controls physical access to it. Auditors validate the design and operational effectiveness of the cloud providers' security controls by walking through processes and evaluating evidence, relieving customers of the requirement to perform certain validation work themselves for their IT environment. With managed services, you can get automatic patching to make sure the managed service software powering your deployment stays up-to-date with the latest patches.

2 Compliance

Collecting and storing sensitive customer and business data usually requires that you understand and comply with certain regulations specific to your geographic region, industry, or both. These mandates place a necessary but heavy burden on smaller businesses. Keeping up with the often-changing requirements can be challenging enough; from there, you must execute the necessary steps to achieve compliance, manage audits, and provide compliance reporting. Compliance can be expensive, but usually costs less than paying a fine for noncompliance.

Cloud providers can automate compliance, integrating checks, audits, and updates into your infrastructure services. When considering a cloud provider, be sure to understand the third-party regulation and frameworks they support, as well as the certifications they've achieved. It's important to know what tools are available to help you manage compliance and prove adherence during audits.

3 Flexibility

A broad set of capabilities and services work together to determine a company's security posture. Many organizations have already invested in tools that manage some or all of the cybersecurity spectrum, including access control, threat detection and mitigation, compliance, and network and application protection. Still other businesses may be at a loss as to where to start when it comes to cybersecurity.

Wherever you may be in your security journey, make sure your strategy affords your business the flexibility to meet your company's specific needs for protecting its data and applications. If you move some of your IT infrastructure to a cloud environment, for example, you may want to integrate security solutions you're already using with your cloud account for ease of use and to get a greater return on your existing investment, so it's important to make sure your cloud provider offers that option.

aws small and medium business

Summary

Moving to the cloud simplifies how you secure your data while lowering costs. You gain access to the cloud provider's vast cybersecurity expertise, as well as that of its partners, programs, and training, to round out the skills of your technical staff to better mitigate risk, avoid downtime, and meet compliance requirements.

Learn more

Download our eBook, ***Secure Your Business With the Cloud*** or **contact AWS Sales**.