aws small and medium business

AMAZON WEB SERVICES

Secure your Business with Cloud-based Solutions

A Guide and Assessment for Small and Medium-sized Businesses

AWS SMB | MARCH 2022

Table of contents

Introduction

What you'll learn

This eBook is intended to help decision-makers in small and medium-sized organizations understand how cloud-based security can reduce risks efficiently and cost-effectively.

You'll learn:

- The security challenges and opportunities facing small and medium-sized businesses
- Best practices for a cybersecurity program framework
- Advantages of a cloud-based approach to cybersecurity
- How to assess if the time is right to deploy a cloud-based security approach
- How Amazon Web Services (AWS) can help you protect your business

CHAPTER 1:

Security challenges and opportunities facing small and medium-sized businesses

The digital transformation of small and medium-sized businesses is creating efficiencies, new business models, and opportunities for growth. It also introduces a greater need for security as potential vulnerabilities are introduced to software, hardware, and networks. For example, the shift to remote work, whether 100% or hybrid, is now a business reality that creates more points of entry into your computer systems and data—and each needs to be protected.

By developing a stronger security posture, business reduce the risk of downtime and disruption to operations, which can impact a customer experience, or ultimately revenue. But for businesses with limited IT resources, building an in-house security program can be complicated costly. Central to this is finding the right staff to manage security solutions. The demand for cyber expertise has become so high many businesses have difficulty sourcing sufficient talent to support their own program.

As a result, many small and medium-sized businesses find managing their own security is:

- **Resource intensive.** Any business that stores customer and/or payment data is also responsible for adhering to compliance standards and regulations based on their industry and customer location. Adherence requires legal and IT expertise that adds cost and complexity.
- **Complex.** Security solutions are complicated and required up-to-date expertise and dedicated personnel to deploy, install, configure and manage.
- **Expensive to monitor and maintain.** The cost of storing, managing and securing data, including the application of antivirus, malware software, and other security alerts can add up quickly.

This has the potential to create conflicting priorities, and force IT organizations to make choices between business objectives such as support for customer experience, supply chain management, revenue growth, or funding and supporting security efforts.

In order to effectively address this issue, business decision makers must a clear understanding of the basic security functions, how they work together to protect and improve the resiliency of your organization, and what opportunities and options exist to adopt them.

CHAPTER 2:

The building blocks of a cyber security program

Many technologies can be applied to identify potential threats and help prevent them from becoming security incidents, but how do they all fit together? Most security products and services reflect elements of industry standard security frameworks, most of which cover five core areas: identify, protect, detect, respond, and recover. Described below are the specific outcomes of each of these five functions in managing cybersecurity risk:

- **Identify.** A critical first step when developing an organizational understanding to help manage and prioritize cybersecurity is to identify the unique business context, resources, and risk specific to your organization.

- **Protect.** A key objective of any security program is to address security gaps. The technology and activities necessary to protect your systems range from identity management to awareness and training. Multifactor authentication and Single Sign On (SSO) are examples of technologies used to provide protection by providing remote employees with secure access to company systems.

- **Detect.** Detecting a cybersecurity event is a critical function of security monitoring tools including antivirus and malware software that collect and store large logs of system activity, often alerting a security analyst of unusual patterns or anomalies for investigation.

- **Respond.** A security program is only effective if there is a capability to respond to detected threats. Response outcomes include planning, communications, and mitigation to provide a timely and appropriate level of response.

- **Recover.** Recovery is the process of resuming normal operations as quickly as possible after an incident. Backup, restore, and business continuity are foundational elements of a recover function.

The best practices consider the requirements of each function and layer security throughout your architecture and organization to provide a comprehensive risk-based approach to developing your security strategy. Every small and medium-sized organization's security strategy should consider each function and then ensure that the mix of technologies and services meet your unique business needs.

For example, a business that stores customer and/or payment data is responsible for adhering to industry-specific compliance mandates, such as the Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR) in Europe. These regulations dictate processes for capturing, storing, and sharing data and specify required technologies for multilayered data protection, such as firewalls and data encryption. For companies in these industries, well defined protect functions are a critical component of the security framework.

CHAPTER 3:

How cloud solutions enhance security and control

Managing security in the cloud allows you to safeguard your operating environment and customer and corporate data without compromising performance, cost or optimal architecture. With cloud-based security, you inherit strong security and compliance controls and benefit from the ability to easily scale and enhance visibility and control. Automation enables efficiencies that help improve your protection and save time, and trusted security partners and solutions enable you to continuously improve with new and innovative security features.

For example, a cloud security solution designed for your specific requirements can support your business in the following ways:

- **Provide data protection.** Verify that data is properly protected and compliance standards are met without having to know the ins and outs of each regulation. Automated data detection and encryption continuously monitors and protects your data moving through and across workloads.
- **Help achieve compliance and data privacy.** Get a comprehensive view of your compliance status and continuously monitor your environment using automated compliance checks. Timely updates help you meet security and compliance standards for your specific industry.

- **Detect potential threats through continuous monitoring.** Use the latest technologies, including integrated threat intelligence, anomaly detection, and machine learning to detect and stop malicious or unauthorized traffic to prevent it from becoming a business-impacting event.
- **Manage user and device access.** Manage user identity, access policies, and entitlements as well as business governance including, user authentication, authorization, and single sign-on instead of dedicating your resources to these tasks. As your organization grows, the cloud easily scales your identity and access management capabilities.
- **Enforce network and application security.** Enforce fine-grained security policy at network control points across your organization. Cloud services can also scan for known software vulnerabilities, even those introduced unintentionally during development and deployment that can be exploited to access your network.

With cloud-based security, your data is continuously monitored, and issues can be detected early, without straining your own limited resources. And with cloud services, you only pay for what you use.

CHAPTER 4:

Assessment: Could your business benefit from cloud-based security?

Evaluating your current security posture is a straightforward way to determine how quickly you would benefit from a cloud security solution. Review the statements below and check those where you have the personnel or tools to address essential security activities:

- ☐ We install current antivirus and identity management on all devices.
- ☐ We have installed and configured a firewall to block suspicious traffic.
- ☐ We perform regular vulnerability scans on hardware and software and install patches/updates as vulnerabilities are identified.
- ☐ We perform daily backups of files and databases, operating systems, applications, configurations, virtual machines, hosts and management consoles, cloud-hosted infrastructure, and on-device data.
- ☐ We follow data compliance and data privacy regulations based on our industry and/or geography.
- ☐ We can quickly identify and detect security alerts and determine root cause.
- ☐ We have visibility into security alerts with clear prioritization to help guide our response.
- ☐ We have an in-depth backup and recovery plan for worst-case scenarios and test it regularly.

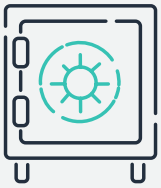
If you did not check yes to all of the above activities, a cloud security solution could be an essential step to increasing your organization's security and resiliency.

CHAPTER 5:

Secure your business with Amazon Web Services (AWS)

Moving to the cloud has big benefits, especially when you work with the industry's most experienced cloud solutions provider. With AWS, you will gain the control and confidence you need to securely run your business with the most flexible and secure cloud computing environment available today. As an AWS customer, you can improve your ability to meet core security and compliance requirements while benefiting from a network architected designed to protect your information, identities, applications, and devices.

AWS security solutions allow you to safeguard your operating environment and customer and corporate data without compromising performance, cost or architecture. Security is a shared responsibility between AWS and our customers. This shared model relieves your operational burden as AWS operates, manages, and controls the components from the host operating system down to the physical security of the facilities. Customers maintain responsibility and control of workloads running inside the cloud. Because AWS security solutions are deeply integrated, a high level of automation is possible reducing human configuration errors, and freeing up IT resources for work critical to your business. The ability to automate tasks in novel ways makes it easier to collaborate and more quickly and securely deploy code.



Using AWS you can analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities, without the costly overhead. A comprehensive set of services and features gives organizations of your size the ability to efficiently meet core security and compliance requirements, such as data locality, protection, and confidentiality without building a staff of security experts. AWS customers realize five main benefits, the ability to:

- **Scale Securely with Superior Visibility and Control:** With AWS, you control where your data is stored, who can access it, and what resources your organization is consuming at any given moment.
- **Automate and Reduce Risk with Deeply Integrated Services:** Automating security tasks on AWS enables you to be more secure by reducing human configuration errors and giving your team more time to focus on other work critical to your business.
- **Build with the Highest Standards for Privacy and Data Security:** We have a world-class team of security experts monitoring our systems 24x7 to help protect your content. And you can build on the most secure global infrastructure, knowing you always own your data, including the ability to encrypt it, move it, and manage retention.
- **Largest Ecosystem of Security Partners and Solutions:** We have carefully selected providers with deep expertise and proven success securing every stage of cloud adoption, from initial migration through ongoing day-to-day management.
- **Inherit the Most Comprehensive Security and Compliance Controls** To aid your compliance efforts, AWS regularly achieves third-party validation for thousands of global compliance requirements that we continually monitor to help you meet security and compliance standards for finance, retail, healthcare, government, and beyond.

Because AWS security solutions are deeply integrated, a high level of automation is possible, enabling you to reduce human configuration errors and give your team more time to focus on other work critical to your business. Our solutions are easy to use and allow you to automate tasks in novel ways, so your team can effectively collaborate and more quickly and securely deploy code. When you move to the AWS cloud, you benefit from:

- **Real savings you can see and measure.** Moving to the cloud provides the ability to reduce costs while increasing efficiency. Migrating with AWS leads to an average cost savings of 31 percent.[1] We have reduced costs more than 100 times over the last decade, returning more than half a billion dollars to our customers.
- **Built-in reliability and resiliency.** Businesses like yours cannot afford a breakdown in IT availability-that's why we have applied more effort than anyone else to provide cloud resiliency. Our extensive investment in global availability zones and redundant networks, storage, and compute help enable access to your critical data and applications. In addition, we bring experience and frameworks to provide business continuity, including dedicated teams and partners who can provide on-demand expertise and support.
- **A broad, deep, and constantly growing set of capabilities:** AWS has been continually expanding its services to support virtually any cloud workload, and it now has more than 200 fully featured services. When you collaborate with us, you continuously gain new, simple, trusted, and accessible solutions without having to make your own investments in capital and talent.

1. AWS, **"Accelerating your AWS Journey,"** 2021.

aws small and medium business

Take your first step

You don't have to leave your business open to cyber threats or compromise other strategic business initiatives to get started enhancing your security posture. With a pay-as-you-go model, the cloud offers a way to get exactly the solutions you need, when you need them. Instead of trying to keep up with IT maintenance, compliance standards, and changing business operations, you can reinvest in high-value business initiatives that differentiate your organization and increase its competitiveness. Get exactly the solutions you need, when you need them. Instead of trying to keep up with IT maintenance, compliance standards, and changing business operations, you can reinvest in high-value business initiatives that differentiate your organization and increase its competitiveness.

The most highly regulated organizations in the world trust AWS, and the same comprehensive security suite is available to your organization to help you protect your systems, users, and data from unauthorized access. Let us help you get started.

Request an AWS security assessment. Security is a journey of continuous improvement, and even if you've already gotten started, it is hard to know if you are adequately protected. Let us help by providing an AWS Security Assessment where your network, software, data, and devices will be evaluated against industry standards and our own AWS framework. Your custom report will give you an overall risk score, identify gaps, and provide a roadmap for what to address immediately and how to improve over time. Contact us for your free assessment today.

Small and medium-sized businesses do not have to become security experts to protect their data. Deploying security solutions from AWS in the cloud helps businesses like yours immediately benefit from a high level of protection that is easy to manage and sized for your business. **Get started with a 30-day risk-free trial today.**

Learn more about how AWS can make securing your business easier or **contact us**.