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

# Contents

# Introduction

## About this eBook

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 ONE

# 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 intrude on software, hardware, and networks.

For example, the shift to flexible and remote work options 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, businesses reduce the risk of downtime and disruption to operations.

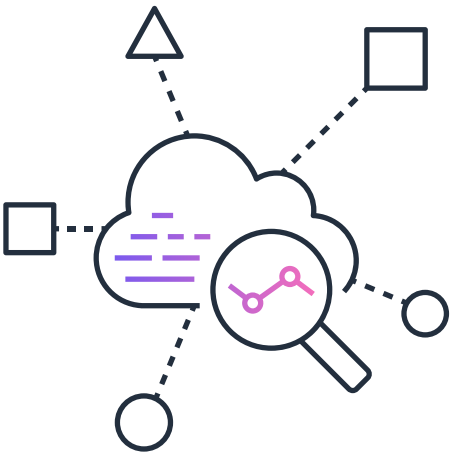
But for businesses with limited IT resources, building an in-house security program can be complicated and costly. And demand for cyber expertise is so high that many businesses have difficulty sourcing sufficient talent to support their own security programs.

As a result, many small and medium-sized businesses find that 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, which generally come at a premium.
- **Complex:** Security solutions are complicated and require up-to-date expertise and dedicated personnel to deploy, install, configure and manage.
- **Expensive to monitor and maintain:** The costs of storing, managing, and securing data—including the application of antivirus and anti-malware software, along with other security alerts—can add up quickly.

These challenges have the potential to create conflicting priorities, forcing organizations to choose between core business objectives or funding and supporting security efforts.

To effectively address these issues, business decision makers must have a clear understanding of basic security functions, how they work together to protect and improve the resiliency of an organization, and what opportunities and options exist to adopt them.



CHAPTER TWO

# The building blocks of a cybersecurity 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?

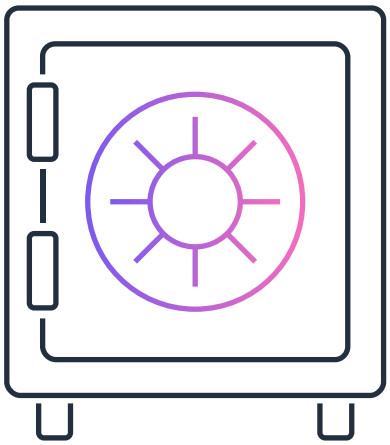
Most security products and services reflect five core principles of industry standard security frameworks: identify, protect, detect, respond, and recover.

- **Identify:** Specify the business context, resources, and risks unique to your organization.
- **Protect:** 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 offering remote employees secure access to company systems.
- **Detect:** Notice and track cybersecurity events. This is often performed by security monitoring tools including antivirus and anti-malware software, which collect and store large logs of system activity, often alerting a security analyst of unusual patterns or anomalies for investigation.
- **Respond:** React appropriately to detected threats. Response outcomes include planning, communications, and mitigation to provide a timely and proportionate 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.

These best practices consider the requirements of each function. This approach layers security throughout your architecture and organization to provide a comprehensive, risk-based approach to developing your security strategy. Every SMB's security strategy should consider each function and then ensure that the mix of technologies and services meets their 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), or the 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 THREE

# 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 unlocks 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.

A cloud security solution designed for your specific requirements can support your business by:

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

- **Detecting potential threats:** Use the latest technologies—including integrated threat intelligence, anomaly detection, and machine learning—to detect and stop malicious or unauthorized traffic and prevent it from becoming a business-impacting event.
- **Managing user and device access:** Cloud services can streamline the management of user identity, access policies, and entitlements, as well as business governance including user authentication, authorization, and single sign-on. As your organization grows, the cloud easily scales your identity and access management capabilities.
- **Enforcing network and application security:** Enforce fine-grained security policy at network control points across your organization. Cloud tools 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, issues can be detected early without straining your own resources. And with cloud services, you only pay for what you actually use.

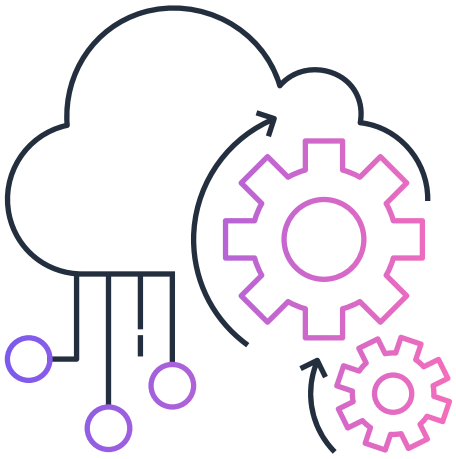
CHAPTER FOUR

# 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 FIVE

# 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'll gain the control and confidence you need to 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 designed to protect your information, identities, applications, and devices.

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, which reduces human configuration errors. Using AWS, you can analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities without the costly overhead.

AWS customers realize five main benefits:

- **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 facilitating continuous monitoring and threat detection, so you can work on what matters most.
- **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 to help you meet security and compliance standards for finance, retail, healthcare, government, and beyond.

And when you move to the AWS cloud, you also gain:

- **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've made cloud resiliency a top priority. 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 unparalleled experience and frameworks to provide business continuity, including dedicated teams and partners who can deliver 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 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.

# Take your first step

You don’t have to compromise other strategic business initiatives to start 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.

The most highly regulated organizations in the world trust AWS, and the same comprehensive security suite is available to your organization to help 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. Even if you’ve already gotten started, it can be hard to know if you are adequately protected.

Take an AWS Security Assessment, in which 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 properly sized for your business. **Get started with a 30-day risk-free trial today.**

aws small and medium business

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