CC CONSULTING GROUP LLC
COST CONTAINMENT SOLUTIONS

Secure Your Business With the Cloud

EBOOK

aws
PARTNER

- MSP Partner
- Saas Partner
- Training Partner
- Marketplace Seller
- Network Competency

Table of 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. In this eBook, you'll learn: the increasing security challenges 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, and how Amazon Web Services (AWS) can help you protect your business.

Security challenges 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. Small and medium-sized organizations' resource and expertise limitations often result in more security vulnerabilities in software, hardware, and networks.

A global survey of small and medium-sized businesses revealed that 32% of small businesses (0–99 employees) and 57% of medium-sized businesses (100–999 employees) experienced a security breach in the last 12 months[1]. A security incident has costs in terms of reputation and business continuity. Yet, building an in-house security program can be expensive and complex. For that reason, many organizations are moving to the cloud to not only store their data, but also to ensure they have a more secure and resilient business.

Data security challenges for small and medium-sized businesses come in many forms. Security issues often cause site downtime and disrupt normal operations. In fact, small and medium-sized businesses reported they spend an average of more than $1 million to restore normal business in the wake of successful security incidents.[2] Downtime and business disruption directly impacts customer experience, which can impact revenue.

[1] Analysys Mason 2019 SMB Survey https://www.analysysmason.com/research/content/articles/smb-cyber-security-comment-ren04/
[2] Ponemon Institute: 2018 State of Cybersecurity in Small &Medium Size Business
https://www.connectwise.com/resources/smb-research-2021

Given that building an in-house security program can be expensive and complex, it can be unattainable for businesses with limited resources. This creates a number of conflicting priorities, forcing IT organizations to make undesirable tradeoffs between important business objectives like support for customer experience, supply chain management, revenue growth, or funding and supporting security efforts.

Further, small and medium-sized organizations also want the flexibility to adapt to changing business environments. 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. According to a survey of small and medium-sized businesses, only 35% of decision makers described their organizations as very well protected against breaches from remote devices and employees[2]. Keeping up with threats is a full-time activity and resources may not be available to make necessary security adaptations.

Central to the security challenge is the scarcity of experienced staff to manage security solutions. Security analysts are expensive and hard to find, which is why only about 6% of small and medium-sized businesses have internal cyber-security experts.[3] The demand for cyber expertise has become so high it is not feasible for many businesses to build an internal team to manage an effective security program. Even if staffing is in your budget, experienced personnel are often hard to find.

[2] Ponemon Institute: 2018 State of Cybersecurity in Small &Medium Size Business
https://www.connectwise.com/resources/smb-research-2021

[3] Vanson Bourne, "Cybersecurity in an Eraof Competing Priorities: The State of SMB Cybersecurity in 2021" https://www.connectwise.com/resources/smb-research-2021

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.

- **Less reliable.** Recovery is dependent upon established routine backup schedules so that systems can quickly be reset, and normal operations resumed.

- **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 cost of storing, managing and securing data, including the application of antivirus, malware software, and other security alerts can add up quickly.

Given how quickly the industry is evolving and how broadly security threats can impact critical systems, it is important that business decision makers have a clear understanding of the basic security functions and define the building blocks and how they work together to protect and improve the resiliency of your organization.

The building blocks of a cyber security program

Many technologies can be applied to identify threats and help prevent them from becoming full-fledged attacks, 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 risk is to identify the unique business context, resources, and risk specific to your organization.

- **Protect.** A key objective of any security program is to prevent a security breach. 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 ensure 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), and 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.

How cloud solutions reduce business risk

Managing security in the cloud allows you to safeguard your operating environment and customer and corporate data without compromising performance, cost or optimal architecture. Migrating security to the cloud enables you to automate manual security tasks so you can shift your focus to scaling and innovating your business while only paying for what you need.
A cloud security solution can support your business in the following ways:

- **Provide data protection**. Ensure 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.

- **Ensure compliance and data privacy**. Cloud gives you a comprehensive view of your compliance status and continuously monitors your environment using automated compliance checks. Timely updates help you meet security and compliance standards for your specific industry.

- **Detect threats through continuous monitoring**. Use of the latest technologies, including integrated threat intelligence, anomaly detection, and machine learning 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**. Network and application protection services enable you to 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.

Could your business benefit from cloud security?

Evaluating how well your current resources can support key security functions is a straightforward way to determine how quickly you would benefit from a cloud security solution. Review the statements below and check no on those where you don't have the personnel and tools to address these 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 are able to 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 answered no to any of the above tasks, a cloud security solution could enhance and improve your business's security and resiliency.

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 architecture that was designed to protect your information, identities, applications, and devices.

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 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.

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. With AWS solutions, customers like 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. We have reduced costs more than 100 times over the last decade, returning more than half a billion dollars to our customers.

- **The highest level of cloud security.** AWS security infrastructure is built to satisfy the highest requirements of the world's leading financial, educational, and governmental institutions that rely on it-ensuring you have the same level of security they do. Amazon customers report on average 43.4% fewer monthly security incidents, and 69% reduction in unplanned downtime.

- **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.

- **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 ensure cloud resiliency. With AWS, customers are able to achieve a 69% reduction in unplanned downtime, and our extensive investment in global availability zones and redundant networks, storage, and compute help ensure that you always have access to your critical data and applications. In addition, we bring experience and frameworks to ensure business continuity, including dedicated teams and partners who can provide on-demand expertise and support.

- **Support through best-in-class partners, programs, and training.** You need to maximize IT performance with limited budgets and resources. We help you plan, scope, and size your projects and offer a free, comprehensive library of digital, self-paced training courses and a range of skill certifications, workshops, and immersion days for your team. Further, our thousands of AWS certified partners and consultants are available to provide you with premier service-no matter your budget.

Take your first step

You don't have to leave your business open to cyber threats or compromise other strategic business initiatives to stay safe. 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 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. To learn more about how AWS can make securing your business easier, contact us today.

CC CONSULTING GROUP LLC
COST CONTAINMENT SOLUTIONS

Learn more

Discover Cloud for Small and Medium Businesses

aws PARTNER

- MSP Partner
- Saas Partner
- Training Partner
- Marketplace Seller
- Network Competency

Please contact us: https://www.cccgroupllc.com/contact-us/