



AMAZON WEB SERVICES

Assessment: Do you have the right tools to protect your company data?





How adopting the cloud helps deter and mitigate threats

Small and medium businesses are adopting the cloud to help prevent unintended disclosures, unauthorized user access, bugs, and other security issues or events. Cloud technology and tools can help to deter, detect, and mitigate threats to company and customer data. In fact, companies that have already migrated to the cloud experience a 43% overall decrease in security events.¹

The cloud provides infrastructure that is built and maintained to provide enhanced security features. On top of this foundational barrier, cloud-based tools and services offer other layers of protection to automate security checks and lower the risk of threats before they impact company operations.

Can your company improve the security of its data against unauthorized access or unintended events? Check off the boxes next to each safeguard that your business has in place. The boxes you don't check represent gaps in your company's data protection tool set.

43%

**overall decrease in security events
experienced by companies that have
already migrated to the cloud**

Access restrictions

Your team needs customer orders, updated inventory lists, designs, applications, and other company resources to work productively. At the same time, your business must use all possible safeguards to protect company and customer information. Does your business have tools to provide:

- ☐ **Access controls.** Systems to easily grant — or revoke — access to data, applications, and other resources for specific authorized users, devices, or groups.
- ☐ **Multifactor authentication.** The ability to verify someone's identity beyond username and password to provide an extra layer of protection.
- ☐ **Encryption.** Tools to enhance the security of your company and customer data when stored or actively shared to other devices.

Threat monitoring

Having the right protections in place can help identify potential issues from outside parties or unauthorized users before they impact your business. Does your company have tools to provide:

- ☐ **Continuous scanning.** Ongoing network scanning for suspicious activity to detect, identify, and mitigate problems before damage occurs.
- ☐ **Intelligent detection.** Near-continuous monitoring to look for known and frequently occurring network issues so that they can be deterred.
- ☐ **Notifications.** Alerts that are triggered and sent automatically to notify users about potential threats or irregular system activity.
- ☐ **System insight.** Real-time views into activity across systems from virtually any location assesses who is using specific applications or data.
- ☐ **Firewalls.** Cloud-based firewalls to help protect against likely threats, deter employees from introducing unauthorized elements, and provide company-specific protection.

Compliance support

Four in 10 financial leaders in a Paychex survey say compliance concerns prompted them to adopt technology to reduce the risk of errors, audits, or penalties.² Companies that have adopted cloud-based tools enjoy the benefits of automation and advanced insight tools. Does your company have the tools to provide:

- ☐ **Automated updates.** Monitoring and reporting tools to surface industry and government regulatory changes and improve compliance reporting.
- ☐ **Local control.** Control over the regions where data is physically stored to enable compliance with regional and local data privacy laws and data residency requirements.
- ☐ **Compliance visibility.** Insight on activity across company networks from one location to help review compliance activity and locate potential issues.

Data backup

Most companies have some sort of data backup, but many solutions are labor-intensive to manage and not flexible enough to accommodate growth. In contrast, cloud backup is reliable, automated, flexible, and comprehensive. Does your company have tools in place for:

- ☐ **Redundancy.** Data backed up in two or more geographic locations to help ensure that critical customer and company information is not lost.
- ☐ **Automated and scheduled backups.** Automated backup of unstructured and structured data, so both quantitative and qualitative information can be stored easily.
- ☐ **Data durability.** Systems that will store data accurately and not degrade the quality.

System restoration

The ability to accurately and rapidly restore both company and customer data can reduce downtime and help your business resume operations quickly. Does your company have tools in place for:

- ☐ **Server recovery.** A way to quickly duplicate and protect uncorrupted versions of company servers if an event occurs.
- ☐ **Testing scenarios.** Simulations to test the efficacy and speed of restoration and verify the accuracy of restored data.
- ☐ **Bounce-back plan.** A plan to restore productivity quickly should an IT outage or other event occur.

Data archiving

Data must be both accessible and secure even if your team only needs it from time to time. Does your company have archive tools that allow for:

- ☐ **Usage-based pricing.** Archiving based on access patterns to provide a lower price for infrequently accessed data and to enable improved placement for storage.
- ☐ **Expedited retrievals.** Quick access to deeply stored data that you use infrequently so that you don't have to plan for what you'll need when.
- ☐ **Scalability.** Cloud storage space that can expand to accommodate your needs, so you don't have to buy storage hardware based on estimates of exactly how much data you'll archive.

Use what you've learned in this assessment to strengthen your company's ability to deter, detect, and mitigate security issues and events. Any section you haven't checked off may represent a potential data security vulnerability. By adopting the cloud, your business can access resources to strengthen data security, compliance, and backup, and bounce back more quickly if an event occurs. Now that you know where company data vulnerabilities exist, you can adopt the right tools and services to protect your data and safeguard your business momentum.

Learn more about AWS or ask an expert

1. Nucleus Research, "Understanding the Value of Migrating from On-Premises to AWS for Application Security and Performance," <https://pages.awscloud.com/rs/112-TZM-766/images/the-value-of-improved-availability-security-and-performance.pdf>
2. Paychex, "Pulse of HR 2020," www.paychex.com/secure/whitepapers/hr-pulse-2020