Security and Scalability – A Match Made in the Clouds

March 4, 2025 • The Cloud Awards • Kevin Beasley

In 2024, data breaches continued to be an expensive challenge for organizations globally.

IBM's 2024 Cost of a Data Breach Report—conducted independently by Ponemon Institute and sponsored, analyzed and published by IBM—studied 604 organizations impacted by data breaches between March 2023 and February 2024. According to the study, the average cost of a data breach jumped to USD 4.88 million from USD 4.45 million in 2023, a 10% spike and the highest increase since the covid 19 global pandemic.

While the cost of breaches has steadily increased over the past few years, they've also become more frequent. The growth of IT outsourcing for remote and hybrid work has significantly contributed to the rise of cyberattacks. Outsourced processes rely on organizations granting vendors privileged access to their networks through remote-access software. These decentralized operations increase the chances of cybercriminals exploiting vulnerabilities within systems.

One of the examples of the increase in cyberattacks has been largely attributed to the expansion of IT outsourcing for remote and hybrid work. Organizations that use remote-access software to give suppliers privileged access to their networks are the foundation of outsourced processes. The likelihood of hackers taking advantage of weaknesses in systems is increased by these decentralized operations.

In addition, the prevalence of malware, and hackers in all commercial verticals has made everyone connected to the internet more susceptible to being breached. There are just too many criminal adversaries and too many entry points available to be reined in, controlled, and minimized. Unfortunately, in 2024, the cyber statistics will continue to remain alarming.

Attacks on software supply chains are extremely challenging to identify. Cybercriminals can use sophisticated strategies, such as malware outbreaks masquerading as genuine goods, to target networks at any point in the software development cycle. In addition to dishonest tactics, cybercriminals frequently employ technologies like artificial intelligence (AI), machine learning, and automation to extend and intensify cyberattacks.

For businesses, cyberattacks can lead to broken trust with customers and investors, diminish organizations' reputation, and damage business continuity.

To keep ahead of threat actors, businesses need to respond by developing a thorough cybersecurity plan. However, what is involved in that? Moving processes to the cloud is the first step. The additional security features in the cloud usually go much beyond what is offered on-premises, enabling businesses to successfully deploy advanced threats through prevention, detection, and mitigation.

Although there are security concerns around cloud migration, the benefits far outweigh the challenges—and having a cloud strategy can enhance your security profile.

Four ways cloud-based services enhance cybersecurity

Cloud-based services can offer crucial protection against software supply chain assaults in the current cybersecurity environment. Cloud providers make sure systems and networks fulfill regulatory compliance criteria by following the

most recent cybersecurity rules and practices. Cloud services also offer round-the-clock assistance and real-time data monitoring.

Additionally, cloud-based services enhance cybersecurity performance in other ways:

1) Regular penetration testing and vulnerability scanning

Vulnerability scanning in web applications and software is used to identify vulnerabilities that would need some level of remediation. Penetration testing, sometimes referred to as pen testing, is a routine procedure used by cloud providers to assess and test the security posture and regulatory compliance of your network. In these exercises, participants mimic the techniques used by cybercriminals to find network weaknesses, such as points of entry into the infrastructure of a system. To help you and your provider work together to perform essential system changes, regular pen testing can help uncover potential cyberattacks your network may encounter as well as the strengths and weaknesses of your systems.

2) Proactive patch management

Cloud providers can secure networks and systems to stop possible cyberattacks if weaknesses are found. The procedure entails finding, evaluating, and applying patches, which are typically code modifications, to solve system vulnerabilities, network issues, or security features. Cloud providers therefore give simplified software updates to enhance your cybersecurity capabilities. Additionally, this procedure guarantees adherence to security laws and improves network software interoperability with hardware components. Also businesses need to subscribe to and monitor NIST, CISA, and KEV's (Known Exploitable Vulnerabilities) and CVE's (Common Vulnerabilities and Exposures).

3) Disaster Recovery and High availability

Cloud providers with disaster recovery (DR) and high availability (HA) can quickly respond to and recover from data breaches and shutdowns. Networks with DR and HA deploy highly redundant infrastructure to ensure proper scaling and maintain automated online and offline backup systems to protect critical data. If your company has system issues, DR and HA also lessen the impact of downtime, which can enhance output, lessen data loss, and safeguard brand reputation. For example, a cloud provider with DR and HA, can relocate your activities to a different data center location in the case of a network cyberattack, preventing hackers from accessing vital company information. Despite the initial intrusion, your company can continue to function with this backup option. Cloud providers such as VAI Cloud have designed their infrastructure with this in mind.

4) Privileged access management

Cloud providers that use privileged access management (PAM) can restrict network access to reduce cybersecurity threats. In essence, providers control the information, accounts, and cloud systems that businesses and their users can access. Additionally, PAM establishes parameters according to company characteristics including worker roles, conditions, and location. An employee in the marketing department, for example, would require prior authorization to access IT-related accounts. Based on business requirements and other considerations, the system must verify the employees' identities before determining whether to grant access to the IT accounts. Additionally, by continuously monitoring and restricting who has access to your data, PAM lowers the likelihood that thieves would compromise networks. This is in conjunction with the principle of least privilege (PoLP), a cybersecurity concept that limits user and process access to only what's required to perform their job duties.

Develop proactive strategies to protect your organization against cyberattacks

Using cloud-based services is essential to improving your cybersecurity strategy. You may strengthen defenses against software supply chain assaults by taking some extra steps right now.

- Continue ongoing investments in your IT department to install and test security software.
- Vet your vendors to make sure they satisfy your security requirements and commercial goals. Inquire about the vendor's level of experience, credentials, security operation compliance (SOC), and security measures such yearly basis testing. For a more

thorough examination, review the vendor's references and performance history.

- Conduct ongoing training sessions for all employees to raise awareness about preventable cybersecurity risks. Often, human error is involved with cyberattacks, especially through phishing and social engineering.
- Update your hardware frequently to meet regulatory requirements and prevent outdated components from causing network vulnerabilities.

How can CIOs seamlessly transition from on-premise to the cloud?

Companies must develop a cloud migration plan which aids in coordinating the migration procedure with their unique business objectives and requirements. To identify potential risks, think about performing an impact analysis of your workloads and apps in advance. Then, develop and put into action a well-defined plan. Make a commitment to creating this plan to guarantee that all data that can be transferred to the cloud is done so accurately and on schedule.

Every cloud migration project is different, for instance, since some companies cannot use a lift and shift strategy because of the complexity of their workloads or because they only wish to maintain some apps on-premise. Businesses can guarantee a successful transition with the correct partner.

What are the advantages of cloud computing?

Moving to the cloud offers organizations many advantages, including enhanced analytics, cost savings, the removal of physical infrastructure, simpler scalability, disaster recovery, and more security capabilities. Because on-premise licensing may no longer be required, cloud databases can drastically lower the cost of running actual on-premise servers and in-office databases.

Another advantage of the cloud is scalability, which may be configured to operate automatically. Scalable cloud computing helps ensure companies don't pay for resources they don't need, which can lead to overuse and unnecessary expenses. Additionally, it makes the cloud more user-friendly, load-resistant, and responsive to customer demands.

Additionally, enhanced analytics with AI enables a company to incorporate AI services by leveraging advanced machine learning algorithms and data processing techniques to analyze large, complex datasets. This integration provides deeper insights by identifying patterns, trends, and correlations that might be difficult or impossible to detect with traditional analytics methods. AI-driven analytics can automate data processing, offer predictive and prescriptive insights, and support real-time decision-making, ultimately helping businesses optimize operations, improve customer experiences, and drive innovation.

Where do enterprises stand on cloud security?

Cloud security is something that businesses should be very concerned about. There are a number of advantages to moving from on-premise to the cloud, including access to the newest and most cutting-edge cloud features with the most advanced security services that use AI.

Although some companies may initially worry about security, they soon discover that the cloud is incredibly safe because many providers offer complete insight into your cloud environment and defense against threats like malware. Businesses are still reaping the rewards of a successful cloud migration effort in terms of security.

What do IT leaders need to think about when it comes to protecting sensitive data in the cloud?

There are several ways to secure sensitive data in the cloud, including database-level encryption, column-level encryption, and full encryption of all data while it's at rest. Furthermore, encryption in transit needs to be required. IT leaders must remain focused on the best practices and necessary tools.

For example, leaders should consider putting strong security controls in place, including multi-factor authentication, and putting preemptive measures in place. To achieve their objectives, IT leaders should also identify the finest tools, software, and services that enable them to monitor and audit every facet of their infrastructure and data access. The same is true for cloud providers and partners; it is essential to have the appropriate safeguards in place and to offer protection to clients that store data

in the cloud.

What are the common pain points of IT leaders when managing a cloud environment?

IT leaders might encounter additional difficulties in managing their cloud infrastructure, such as cost optimization, application sprawl, and size, whether at the beginning, during, or after a cloud migration project if not properly planned for.

Depending on the model used to deploy the cloud, for instance, IT leaders must keep an eye out for changes in storage and resource allocation to prevent unintended expenses from accruing or fees from the cloud provider if the cloud uses metered billing rather than a flat or contractual rate.

Before installation, the cloud provider should also be transparent with full disclosure about the expenses of the service. Scale and application sprawl are additional issues. It can be challenging for IT workers to have a single view of their cloud environment because IT leaders may already have on-premise apps that they have moved to the cloud or use other management or monitoring apps. Given that their technological stack may have become excessively complex, this lack of visibility and application sprawl can also make it difficult to scale the environment with additional workloads or apps.

To address this, IT workers should seek out suppliers who can combine their technological stack into a single platform or console, making visibility, management, and optimization simpler and more effective.

Since every company is unique, cloud providers must assist in tailoring cloud environments to meet each business' requirements. Any firm may succeed in the cloud by collaborating closely with C-Suite and IT leaders to establish clear objectives for a cloud migration project, resolve any obstacles, and guarantee high security and visibility.