ibml

Why Cloud Native Solutions are More Secure than On Premise Systems

The threats to mission-critical data have never been greater and have never emerged so fast.

- Leaked employee credentials are a never-ending problem.
- Viruses, spyware, worms, and other malware threats are proliferating.
- New website vulnerabilities are emerging each week.
- More employees are being targeted with spear-phishing attacks where fraudsters try to obtain sensitive information by impersonating a trustworthy entity in digital communications.
- Ransomware attacks are on the rise.

53%

Fifty-three percent of respondents reported having data breaches in the past two years, according to the Ponemon Institute's 2020 State of Vulnerability Management in the Cloud and On-Premises report.

No wonder that hundreds of millions of personal records are lost or stolen each year.

Remote working is putting data at even greater risk. The Federal Bureau of Investigations (FBI), Internal Revenue Service (IRS), and Interpol warn that the increased reliance on e-mail for managing mission-critical data is resulting in more phishing and Business E-mail Compromise (BEC) attacks.

Many organizations have been forced to make hard choices between established checks and balances for managing corporate documents and data, and getting work done as staff works from home.

Organizations are always on their heels with on premises systems.

Most on premises systems aren't up to the challenge.

While on premises systems are getting better at identifying suspicious transactions, they weren't built to prevent security vulnerabilities. By the time that a breach has been discovered, an attacker can do a lot of damage. And few on premises systems make it fast or easy to fix a security breach.

Systems that are delivered “as a service,” via a private cloud, or through a public cloud are only marginally better than on premises systems in preventing security vulnerabilities.

The longer that an attacker has access to an organization’s data, the greater the risk.

Take Back Control of Your Data

Cloud native solutions give organizations the upper hand in reducing risk across the enterprise.

For years, many organizations distrusted cloud solutions to protect their data. This was especially true among banks, insurers, healthcare organizations and government entities. In their eyes, the perceived risks of storing sensitive information in the cloud vastly outweighed the benefits.

But cloud technology has come a long way. While no solution can guarantee security, it’s fair to say that cloud-native solutions are much more secure than legacy on premises server-based systems.

A Deloitte survey of more than 500 IT leaders and executives revealed that security is the top driver of cloud migration.

Built with development and IT operations (DevOps) practices, a microservices architecture, and continuous delivery, cloud native solutions make it possible to proactively prevent vulnerabilities.

Cloud-native solutions were designed with the core idea that the faster an application changes, the harder it is for attackersto penetrate the solution, and the lower the potential risk of stolen data.

Ever-evolving security threats require ever-evolving software.

Cloud native capture solutions offer compelling benefits:

- Automation. Manual development and release processes are replaced by script and code.
- Innovation. Updates to cloud native solutions are continuously deployed.
- Consistency. Automated updates ensure all users have access to the same software.
- Resiliency. Problems within a cloud native solution won't bring down the entire application.

But the most compelling benefit of cloud native solutions may be its ability to protect data.

Why cloud native solutions are more secure than on premises systems

The way that cloud native solutions are designed builds security into the way the application is developed, delivered, and maintained, allowing for the fast detection and resolution of threats. This is a game changer when it comes to securing mission-critical information. Here are the ways that cloud native solutions are more secure than on premise systems.

Cloud-native solutions are more secure than physical servers.

Here are the ways that cloud native solutions are more secure than on premise systems.

No physical access. While it may be uncomfortable to consider, bad actors on your payroll may pose a grave risk to your data. Whether unscrupulous employees are motivated by selling data on the Dark Web or working with competitors, it can be hard to stop them from stealing data from on premises servers. On average, only 5 percent of an organization's folders are fully secure, Varonis reports. Cloud native solutions thwart insider attacks by storing your information off-site in a data center with limited access and high-level controls.

Sixty-one percent of cybersecurity professionals say that it is more difficult to detect and prevent insider attacks than it is to prevent external attacks, according to research from Crowd Research Partners.

Accessible security tools. The top-of-the-line security safeguards employed by large enterprises may be out of the financial reach of small and mid-sized organizations with one or two on premise servers. But cloud technology providers have economies of scale on their side, allowing them to offer sophisticated security at an affordable price to users of all sizes.

Cloud native solutions make it hard for attackers to gain and maintain a foothold.

Advanced technology. Cloud technology providers are investing a big and growing percentage of their research and development budget on security. Many cloud technology providers are investing in emerging technologies such as artificial intelligence and machine learning that can automatically identify anomalies and suspicious transactions and get better at doing it over time. With so much money going towards security, users can be sure that cloud providers will have the right tools to keep up with ever-evolving security threats.

Malware feeds on misconfigured and unpatched software.

Automatic software updates. Outdated server management tools and other software are a hacker's best friend. Yet many resource-strapped IT departments fall behind on installing software patches or updates, potentially putting data at risk. Keeping software current requires someone within an organization to track vendor announcements and cross-check known vulnerabilities against the software the organization has deployed. Another problem is that many organizations have dozens of servers loaded with software. Regularly patching all the software on all these servers can be a tall order, to say nothing of trying to do it fast when a security threat has been uncovered. Cloud native data capture solutions eliminate these security loopholes by automatically upgrading users to the latest version of the application and patching issues each time someone logs on. Consistent updates also eliminate the possibility of servers with unique and potentially risky security configurations.

It can take months to go into production with new on premises capture software. The time it takes an organization to update its capture software is time that leaves it open to attack.

Constant backups. If your organization has lost important data because it wasn't backed up, you are not alone. U.S. businesses lose millions of dollars' worth of data annually because it wasn't backed up. Poor data backups also leave organizations vulnerable to ransomware schemes. Without data backups to revert to, organizations may be tempted to pay fraudsters the ransom. Cloud native solutions automatically back up data, per the organization's needs.

The Ponemon Institute estimates an average data breach will cost $3.92 million.

Easy restoration. Undetected security attacks can cause significant problems over time. Organizations unwittingly allow security issues to fester by addressing suspected threats with incremental changes to their on-premises systems, rather than going through the burden of restoring the software to a last-known good state. Cloud native solutions automatically restore software to a good state, reducing the amount of time that an attack can occur.

Cloud native solutions make it easy for organization to rotate credentials.

Effortless system administration. Leaked credentials are inevitable. But cloud native capture solutions can mitigate the damage by enabling system administrators to effortlessly change the lifespan of credentials to hours or even minutes, quickly rendering any leaked credentials worthless. Managing credentials in this manner is a burden with an on-premises system.

Only 21 percent of security professionals say their organization is highly effective in patching vulnerabilities, according to the Ponemon Institute's 2020 State of Vulnerability Management in the Cloud and On-Premises report.

Some cloud native solutions also share knowledge about security threats in near real time. Each of these benefits of cloud native solutions is compelling. Together, they create an information management environment where threats are quickly identified and resolved, with minimal impact.

Take Control of Your Data

Compared on premises systems, cloud native solutions are a better way to protect data. That is a big reason that some of the largest organizations in the world including banks, insurers, healthcare firms, and government entities manage their mission-critical data with cloud native solutions.

No technology is risk free.
But cloud native solutions can mitigate a lot of the threats to your mission-critical data.

Get more details.

call: 205.439.7100
Email:sales@ibml.com | Visit: ibml.com

ibml