WHITEPAPER

What’s Trending for Cloud Security in 2022

2022 brings new security vulnerabilities and significant cybersecurity threats. According to McKinsey, “Cyber risk management has not kept pace with the proliferation of digital and analytics transformations, and many companies are not sure how to identify and manage digital risks.”

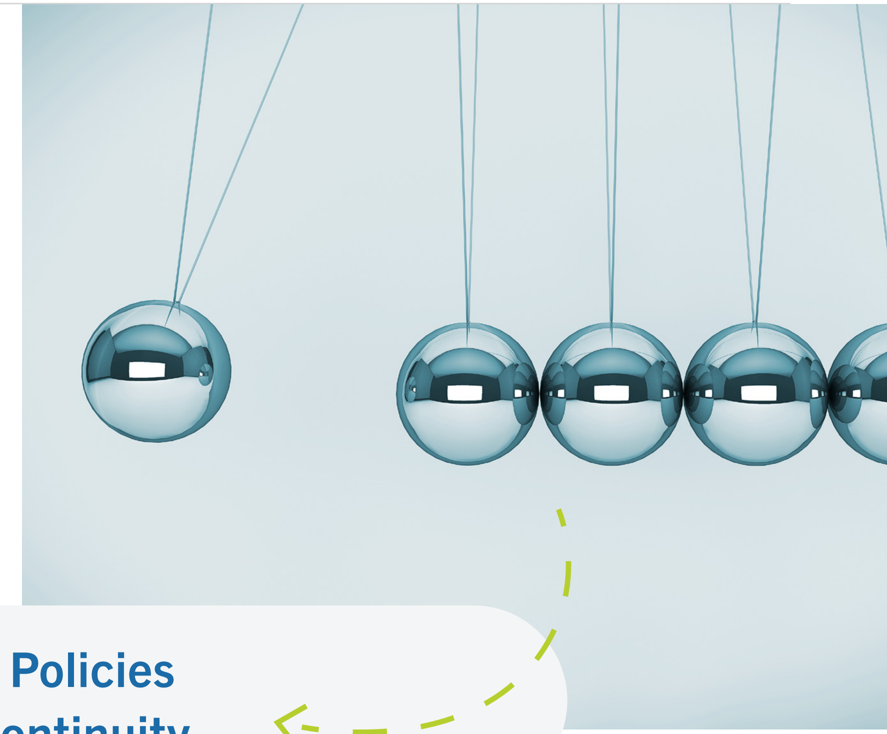
Top cybersecurity threats in 2022 include those related to mobile devices, data governance, disaster recovery, cloud security, and vulnerabilities—especially prevalent in remote work environments.

1 Costly Cybersecurity Risks Are Driven by Remote Work

The growing prevalence of both remote work and distributed networks makes airtight user provisioning and project controls management even more vital to maintaining the health and safety of IT networks. Remote workers must establish boundaries between personal and professional devices to reduce risk.

When networks and application infrastructure are expensive to maintain, a **cloud Platform-as-a-Service (PaaS)** establishes an impenetrable security landscape. Cybersecurity should be ever evolving, staying ahead of the threats regardless of workforce location. A cloud-based platform automates program updates and maintenance—making security and legal compliance worries a nonissue.

> *Cybersecurity should be ever evolving, staying ahead of threats regardless of workforce location.*



2 How Cybersecurity Policies Protect Business Continuity

For the last two years, as companies have wrestled with the economic fallout from the ongoing pandemic, business continuity has become a popular buzzword among industries looking to remain viable and join others taking part in digital transformation and the **Industrial Revolution 4.0**.

Digital transformation means that cybersecurity and business continuity are no longer siloed in departments or spheres of influence. Cybersecurity policies are critical, and in regulated industries such as healthcare and finance, lax procedures mean running the risk of hefty penalties.

> *Digital transformation means that cybersecurity and business continuity are no longer siloed in departments or spheres of influence*

3 Vulnerability & Cloud Security

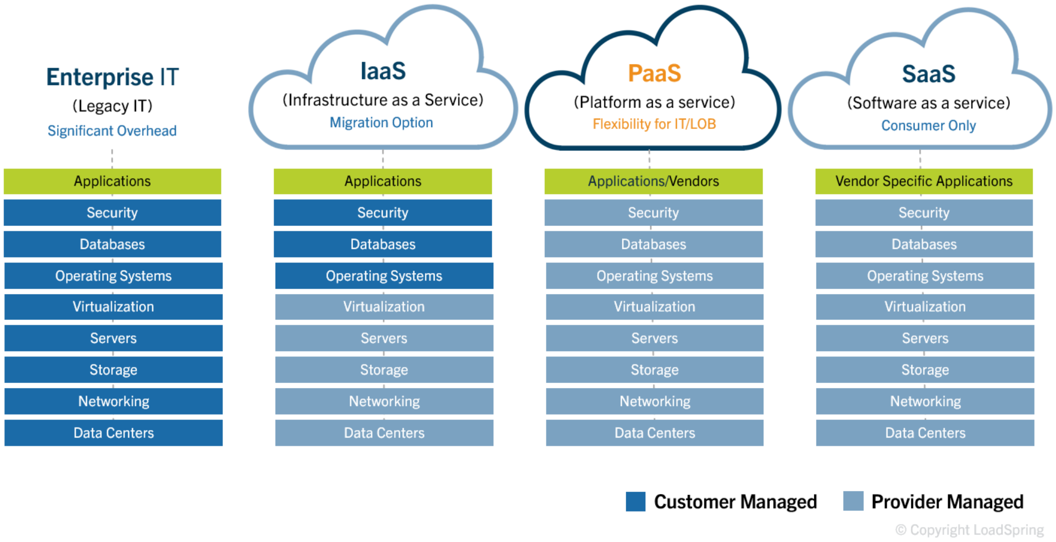
Security vulnerabilities often come in the form of software bugs, and unfortunately, vulnerability scanners can detect bugs quickly and easily. Here's the bigger problem: we are all too comfortable with the usual ideas about security: secure passwords, VSPs, two-step authentication, etc.

There are shared responsibilities with third-party vendors for security in the cloud. Because of this, each person needs to understand their respective role and the security issues inherent to cloud computing. How can your company be proactive against these types of vulnerabilities?

> *...we are all too comfortable with the usual ideas about security...*

Which Cloud Works Best for You?

Depending on your organization's needs and your network's current level of cloud maturity—entry-level, intermediate, or advanced—there are several different types of clouds to choose from:



Enterprise IT (Legacy IT) Significant Overhead	IaaS (Infrastructure as a Service) Migration Option	PaaS (Platform as a service) Flexibility for IT/LOB	SaaS (Software as a service) Consumer Only
Applications	Applications	Applications/Vendors	Vendor Specific Applications
Security	Security	Security	Security
Databases	Databases	Databases	Databases
Operating Systems	Operating Systems	Operating Systems	Operating Systems
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking
Data Centers	Data Centers	Data Centers	Data Centers

■ Customer Managed ■ Provider Managed

© Copyright LoadSpring

As you can see, customer-managed clouds require you to take on more responsibility than cloud-sharing management with third-party providers, such as **Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS)**.

Because of the need for On-Premises or Infrastructure-as-a-Service (IaaS)-based customers to take on full responsibility for security, more companies are opting to invest in PaaS models that can incorporate the same ease of use as SaaS products. Working with a managed-cloud services partner allows your IT team to shift their focus to on-site business objectives.

How LoadSpring Elevates Security in the Cloud

Regardless of which programs you choose, we offer more enhanced security. Your on-site IT team won’t have to worry about regularly updating all your applications and software programs.

The **four most common cloud vulnerabilities** are identity and access management, misconfiguration, shared tenancies, and vulnerability to the supply chain. Fortunately for our customers, LoadSpring takes a proactive approach by using several layers of security:

- Restricted outbound access to prevent payload downloads
- User-restricted server access via **LoadSpring™**
- Servers are accessible only via personalized URLs, eliminating the possibility of IP scans

If you choose to work with LoadSpring, our customer support team installs regular software updates and patches in a timeframe that works for you. LoadSpring’s secure login feature puts control back into your hands. Adopting an all-in-one cloud platform that integrates all your applications and **project controls** in one place ensures tighter security access—allowing for more peace of mind, as well.

Trust & Security

If you're unsure about your organization's current level of trust, **effective security management**—including asset identification and risk assessments—is essential to catching cyberattacks. Whether you expect them or not, attacks are hitting your system 24/7.

At LoadSpring, we shelter critical project management data around the clock. Our security team implements Zero Trust protocols that continually run in the background while offering real-time, live support and optional, automated support through our SmartSupport system. We also boast a 15–30-minute support response time. Our security team adheres to ISO/IEC 27002:2013 standards and is SOC 2 Type II certified—meeting and exceeding US government and Fortune 100 standards.

Consider the one centralized cloud platform with security support that will cover all your issues in 2022.

Get our security brochure,
then contact LoadSpring today!