ORACLE

Top 5 cloud security trends

Leading change with confidence

Adapting to change without compromise

As technology changes and businesses shift their priorities, the one constant is the need to protect critical information. The pandemic prompted industries to adapt and reshape operations, with almost one-third of organizations citing the adoption of cloud services as "significantly more important" than before the pandemic[1]. And 55% of organizations say most employees will continue working remotely after the pandemic at least one day a week[2]. With this in mind, businesses must invest in a secure cloud to stay competitive.

In 2020, IT leaders faced unprecedented challenges in how to modernize key infrastructure without increasing costs or sacrificing security. They took on new levels of responsibility, kept systems secure, and contributed more strategic value.

Whether it's moving workloads to a public cloud, enabling new levels of automation, or reducing complexity, a robust cybersecurity posture is important. Oracle has decades of experience securing data and applications, and we're committed to delivering a more secure cloud with Oracle Cloud Infrastructure (OCI)—building trust and protecting valuable data.

Staying ahead is crucial, which is why we're sharing the security trends expected to have the greatest impact in the coming years, highlighting how Oracle can help address an organization's security needs.

[1] Omdia's 2020–2021 ICT Enterprise Insights Survey

[2] PwC 2020 U.S. Remote Work Survey

1 **Trend 1**

Remote work is increasing the need for a zero trust approach to security

2 **Trend 2**

Increased investment in intelligent security

3 **Trend 3**

The secure automation of DevOps

4 **Trend 4**

CISOs are wearing more hats than ever

5 **Trend 5**

Better security management requires higher levels of visibility

Trend 1

Remote work is increasing the need for a zero trust approach to security

Cybersecurity attacks have gone up by 47%[3], in part due to remote work.

The COVID-19 pandemic has accelerated an already-vigorous level of cloud adoption, while also creating new opportunities for threat actors. The rapid increase in employees working from home, combined with virtual meetings and a greater reliance on ecommerce, has exposed many organizations to cybersecurity attacks that exploit the expanded use of cloud services.

As many as 70% of businesses are having challenges with endpoint cyber hygiene, and they are reporting a 47% increase in cybersecurity attacks, including phishing attempts. The decentralized nature and rapid adoption of cloud services demand greater precautions. However, enterprises use an average of 573 shadow IT applications, many of which have not been vetted, which often leads to improper configurations and unsupervised use. With many employees now working outside an organization's physical corporate walls, it's easy to miss warning signs exhibited by malicious insiders. Meanwhile, misconfigurations in the cloud are becoming a leading source of fraud, with the top threat being overprivileged accounts (44%) over the last 24 months.

A zero trust approach to cloud security will play a critical role in managing threats, as more organizational data flows outside the typical network perimeter. In fact, 87% of organizations want to implement a zero trust architecture post COVID-19. With a zero trust approach, there's no pre-defined level of trust ascribed to a user, workload, device, or network. This approach should be built from the architecture to the application, with every access request validated based on all available data points—including user identity, device, and location. This additional context uses multiple factors to drive a policy-based approach in triggering a two-factor authentication. This is based on the principle of least privilege, with users given only the privileges and access levels required for their specific job roles.

[3] Wipro's State of Cybersecurity Report 2020

Cybersecurity attacks increased

47%

87%

want zero trust architecture post-COVID-19

70%

have challenges with end-point cyber hygiene

Zero trust model with OCI

THE ORACLE DIFFERENCE

Oracle Cloud Infrastructure Security

Risk of constant threats is reduced by utilizing built-in tenant isolation and least privilege access in the cloud security architecture

Isolated network virtualization security is designed to prevent lateral movement of threats and bad actors

Built-in identity and access management easily controls who accesses cloud resources

Secured access is offered with user authentication and single sign-on (SSO) from a variety of devices and locations, as well as risk-based authentication and proactive real-time fraud prevention

Context-aware computing collects and leverages identity, device, and location

Trend 2

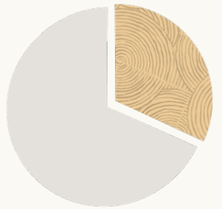
Increased investment in intelligent security

AI and ML have become foundational requirements for cybersecurity technologies—beyond just malware.

While organizations are tightening their budgets as a result of the pandemic, they are still willing to invest in Artificial Intelligence (AI) and Machine Learning (ML) as core elements of their security posture. In fact, 9 out of 10 respondents point to these technologies as fundamental to their cloud security strategy, and 32% of organizations are prioritizing cybersecurity with AI as a top investment over the next 12 to 18 months.

AI and ML have largely been used to detect and prevent threats (e.g., new malware variants, exploits, or phishing attacks). However, the expansion of cloud services is pushing for even more uses of AI and ML beyond detecting malware. The automated security features in next-generation clouds can reduce the time and resources needed to manually manage user access, while also decreasing human error. Accordingly, 40-45% of individuals believe that AI can outperform security analysts in: identifying fraudulent actions, maintaining configuration controls, identifying anomalous user activity, and triaging and prioritizing security events.

The global cybersecurity workforce shortage is projected to reach a staggering 1.8 million by 2022. This is a major reason why 88% of all workloads will be autonomously updated within the next three years, leveraging advanced automation and intelligence. With organizations relying more heavily on AI and ML, cybersecurity teams will gain a critical tool in preventing breaches, while also having more time to focus on innovation that drives the business forward.



32%

prioritize cybersecurity with AI

40-45%

believe AI can outperform security analysts

88%

of workloads will have autonomous updates

Read the IDC report

THE ORACLE DIFFERENCE

Oracle Autonomous Database and Autonomous Linux

Autonomous Database

Self-securing: automates data protection and security; automatically patches the database; and helps prevent unauthorized access/attacks with "always-on" end-to-end encryption

Self-repairing: protects against downtime with rapid, automatic recovery from outages without downtime—AI based autonomy runs diagnostics and minimizes operational disruption

Reduces security administration costs by up to 55%

Autonomous Linux

Zero downtime patching of the OS kernel and key user space libraries without restarting or scheduled downtime

> AI/ML isn't just about collaboration; it is about enabling perpetual change. The ability to adapt at speed and scale is a competitive advantage and, in the case of cybersecurity, can be a matter of survival.

accenture

Trend 3

The secure automation of DevOps

As DevOps becomes increasingly automated, 46% of organizations want DevSecOps to utilize security controls for continuous integration.

The evolution of business in 2020 increased the demand for new applications. This demand has increased so rapidly that organizations are producing apps faster than they can introduce new security controls into existing frameworks and compliance programs—thus creating a "pace gap." Businesses must respond to this pace gap by incorporating security automation into their production lifecycle to avoid inefficiencies and overhead, while also guarding against potential exposure if services go live before security implementation. This scenario has triggered incremental improvements in application security over the past several years.

Retooling for the cloud starts with people and processes, and security has emerged as a top DevOps use case—often referred to as "DevSecOps." DevSecOps automates cybersecurity processes, while controlling the continuous integration and continuous delivery (CI/CD) toolchain that orchestrates the application lifecycle. Security must be integrated with CI/CD automation, otherwise it is left out of development, integration, and delivery of production. Given this, 40% of organizations report that DevSecOps has fostered a high level of collaboration between their development, infrastructure management, application owners, and cybersecurity stakeholders. Additionally, 40% also noted that DevSecOps allows them to gain greater operational efficiency through automation.

Employing DevSecOps can not only improve efficiency and collaboration—it can transform an organization's focus from reacting to security incidents to proactively strengthening its security posture. By continuously folding security controls into the DevOps process, IT leaders can spend less time managing day-to-day problems, and more time contributing value to the business.

46%

want DevSecOps to utilize security controls for continuous integration

40%

report DevSecOps has enabled

high level of collaboration

greater operational efficiency

Oracle Cloud Security blog

THE ORACLE DIFFERENCE

Intelligent, automated security

Automates security to reduce complexity, prevent human error, and lower cost with automated patching for Autonomous Database and Autonomous Linux – and threat mitigation by Cloud Guard, and Oracle Identity Cloud Service

Automates basic security controls, including encrypting data at rest and in motion, along with automated testing as new features are added, security is continually refined and updated. Read how to integrate Jenkins with Oracle Cloud services for automated testing

Identifies configuration choices that pose a risk and highlights configuration drift with Data Safe

Enables the continuous delivery (CD) process through cloud automation: Oracle Cloud Infrastructure (OCI) exposes all our services to operators and developers. Our services natively support open source provisioning tools to help DevOps teams construct immutable infrastructures by using code

Adopts cloud security posture management to detect misconfigured resources, while providing administrators with the visibility to triage and resolve issues

Trend 4

CISOs are wearing more hats than ever

CISO roles will demand greater cloud-centric expertise as they become more engaged with digital transformation and business initiatives.

The last year has emphasized the need for cloud readiness and digital modernization. As a result, organizations are leaning more heavily on their chief information security officers (CISOs) than ever before. As CISOs wear more hats, they've become the changemakers of their organizations—being tasked to support digital transformation (DX) as well as cloud computing initiatives. CISOs are spending more time working with LOB leaders, aligning business processes with cloud computing, anticipating cyber risks, updating threat models tied to cloud computing, and identifying shadow IT applications. In fact, 73% of organizations have hired or plan to hire a CISO with greater cloud computing skills, while 53% employ or plan to employ a business information security officer (BISO) to integrate cybersecurity into their business processes[4].

With the CISO focusing more on business, Oracle is also seeing the emergence of the DX CISO. These executives will be called upon to refine business processes while redefining how work gets done. They must integrate cybersecurity into DX initiatives and embed strong cybersecurity within all aspects of IT—especially public cloud computing. DX CISOs must not only rationalize the technology portfolio, but transform it into a tightly-integrated and scalable security stack. This requires a high performance data pipeline for stream and batch data processing, API integration between tools, threat intelligence ingestion for data enrichment, and process automation for immediate incident response and risk mitigation.

CISOs will need to integrate security with agile development, DevOps, and automated continuous integration and continuous delivery (CI/CD) pipelines. Furthermore, they should get their teams to understand the cloud shared security responsibility model, and then build a synergistic hybrid security model that covers all aspects of IT infrastructure. Finally, they must work with the business to create policies for least privilege that can lock down accounts, manage privileged users, and safeguard sensitive data.

73%

hired or plan to hire a CISO

53%

employ or plan to employ a BISO

Read about the cloud-centric CISO

[4] The Mission of the Cloud-centric CISO

THE ORACLE DIFFERENCE

Oracle Cloud Infrastructure

Delivers customer isolation and protections with data residency, sovereignty, and cloud security

Offers full-stack protection: with our zero trust approach to security, you decide how infrastructure, users, devices, and applications interact with data

Provides for automated detection of common security misconfigurations to minimize risk through tools such as Oracle Cloud Guard

Provides security solutions to detect threats, fix errors, and protect from attacks

Offers integrated cloud security series: every Oracle Fusion SaaS application includes Oracle Identity Cloud Service (IDCS) for consistent, identity-based security

> The DX CISO is not just a new title, but rather an evolution of the CISO role, and his or her relationship with the business and digital transformation. To ensure priority, DX CISOs should report directly to the CEO.

KPMG

Trend 5

Better security management requires higher levels of visibility

Organizations are investing in new tools to integrate the security stack across their cloud solutions, and enabling full visibility across all applications and infrastructure.

As companies seek stability in the wake of a global crisis, the cloud has become a lifeline. Cloud computing has increased the speed with which organizations can address difficulties and create new opportunities—but growing complexities pose new challenges to security and visibility across the technology stack. Cloud native applications introduce new tools, processes, and personas that are often immature, lacking the same level of operational oversight as traditional applications. Growth in SaaS options and applications has given rise to unsanctioned cloud usage, with more than 1,000 such unauthorized services in use at each business today. And with supply chains more vulnerable to fraud, organizations must implement a zero trust approach for extensive visibility and auditing across the business.

As our digital ecosystem grows, businesses will need to leverage new tools to address increasing pressures over data privacy and regulation. The volume and variety of data makes data discovery and classification difficult, while also making it problematic for security teams to enforce consistent security policies. In fact, 30% of organizations have discovered "cloud secrets," including passwords, encryption keys, and API keys stored on cloud-based servers. With compliance and industry regulations evolving, they demand greater mechanisms to ensure compliant execution.

With remote work triggering rapid cloud adoption, understanding cloud access and privileges is increasingly difficult for security teams who are also monitoring activity. Companies must anticipate and navigate the complexities of securing their cloud environments. Because many large organizations work with multiple IaaS, PaaS, and SaaS providers—each with its own version of the shared responsibility model—businesses become susceptible to misconfigurations, software vulnerabilities, human error, and process redundancy. To reduce risk and drive continuous protection, companies need to consider their infrastructure, along with the security of databases and applications, corporate security and privacy—as well as identity and access management.

1000+

unauthorized services used daily

30%

found cloud secrets stored on cloud-based servers

Data security and protection eBook

THE ORACLE DIFFERENCE

Oracle Cloud security monitoring, management, and mitigation

Provides complete SaaS security controls to application owners, auditors, and security operations teams through: Oracle Identity Cloud Service (IDCS) and Oracle Risk Management Cloud (RMC)

Offers response and remediation: Oracle Identity Cloud Service (IDCS) delivers behavioral monitoring and secondary authentication

Delivers a self-securing autonomous database: Managing security across the database, using Oracle Data Safe to: analyze activity; manage audit policies; detect configuration drift; and remove risk from the test and development process

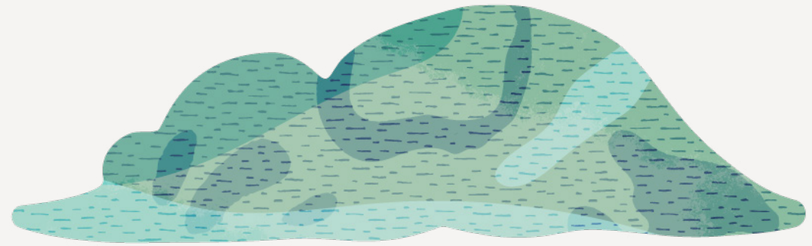
Uses Cloud Security Posture Management: Oracle Cloud Guard helps you gain a unified view of your cloud security posture across Oracle Cloud Infrastructure customer tenants

Oracle Cloud Guard detects misconfigured resources and insecure activity across tenants and provides security administrators with the visibility to triage and resolve cloud security issues. Security inconsistencies can be automatically remediated with out-of-the-box security recipes to effectively scale the security operations center

What's next

By now, it's clear that 2020 has permanently changed the way business gets done. What's also apparent is that a security-first approach can go a long way in reducing complexity while also driving innovation. With the right tools in place, organizations can automate security, prevent human error, and lower costs. And with remote work and cloud computing becoming the new normal, senior IT leaders will be taking on a greater role in shaping a more secure future for their business for years to come.

Try Oracle Cloud Free Tier



Discover how to navigate change with Oracle Cloud

Learn more

Hear stories from customers who made meaningful changes

Watch now

Read more about cloud infrastructure security

Read more

ORACLE