Cloud security trends to safeguard your enterprise

How the cloud can help strengthen
your organization's security posture

Introduction

Unified identity and access management systems

Threat detection with cloud services

Using automation to help reduce the risk of data loss

Layered security strategies that support a multicloud approach

Corporate board members with cybersecurity knowledge

What’s next for cloud security?

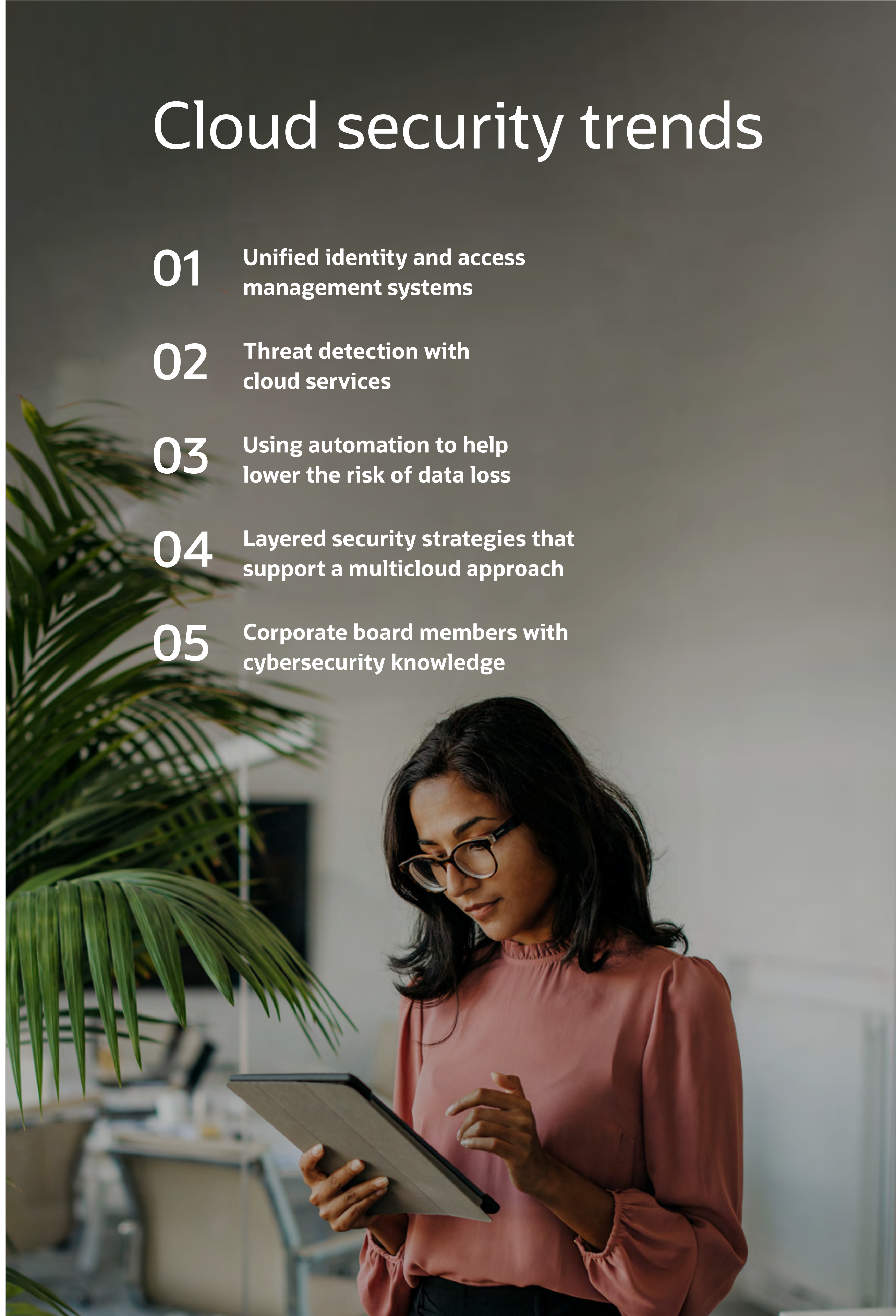
Organizations are addressing evolving security concerns with help from the cloud

IT and security leaders are faced with security challenges that continue to evolve as cyberattacks increase and IT infrastructure grows more complex.[1] Multicloud adoption, remote work, digital customer engagement, and the growing amount of data and devices have left organizations with expanding attack surfaces and an excess of tools that can create costly inefficiencies and unnecessary risk.

As organizations evaluate how to address these challenges, they are turning to the cloud for a simpler and more efficient way to strengthen security posture. For many organizations, cloud infrastructure can provide a more secure platform than an on-premises data center and help simplify cybersecurity with services that automate system security tasks and help reduce risk.

This ebook explores trends in how some organizations are using cloud services to address security challenges, provides ideas for IT and security leaders looking to reduce security complexity, and demonstrates how Oracle Cloud Security Services can be part of your security strategy.

[1] “Is your organization too complex to secure?,” PwC, 2022



Cloud security trends

01 Unified identity and access management systems

02 Threat detection with cloud services

03 Using automation to help lower the risk of data loss

04 Layered security strategies that support a multicloud approach

05 Corporate board members with cybersecurity knowledge

Introduction

Unified identity and access management systems

Threat detection with cloud services

Using automation to help reduce the risk of data loss

Layered security strategies that support a multicloud approach

Corporate board members with cybersecurity knowledge

What’s next for cloud security?

> “Security has been a critical design consideration across Oracle Cloud for years. We believe security should be foundational and built in, and customers shouldn’t be forced to make trade-offs between security and cost.”

Clay Magouyrk, Executive Vice President, Oracle Cloud Infrastructure

Trend

Unified identity and access management systems

To control identity sprawl, organizations are turning to unified identity and access management (IAM) platforms that provide a centralized view of customer, employee, and machine interactions.

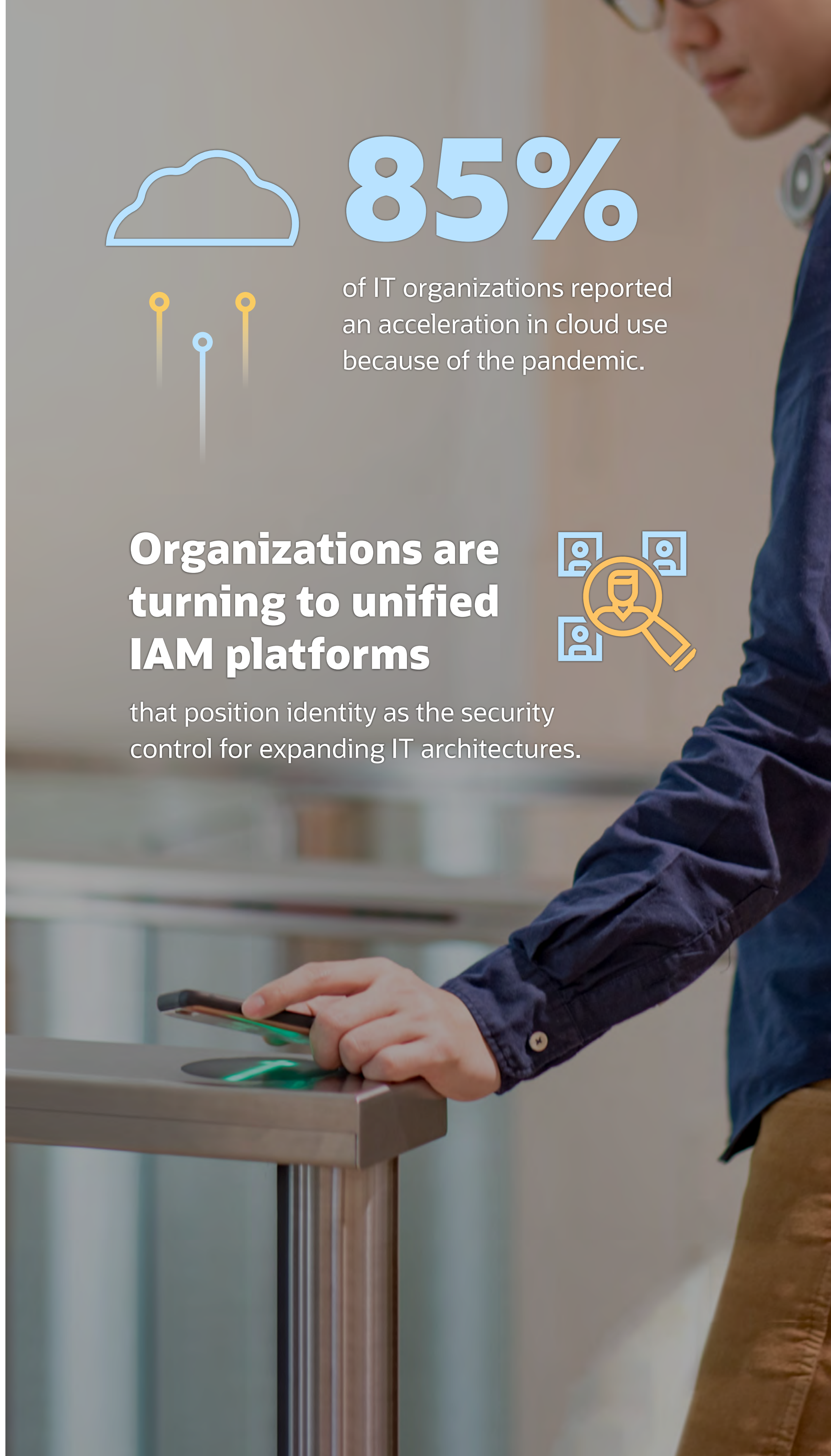
According to a recent survey from Enterprise Strategy Group, 85% of IT organizations reported an acceleration in cloud use because of the pandemic.[2] As cloud footprints expand to include more applications and services, new silos can emerge. Because apps and services each have their own provisioning mechanisms and systems for managing identities, new adoption can create opportunities for inconsistencies in how access and governance policies are applied. Without a centralized view of security across the organization, this "identity sprawl" can result in overprivileged accounts going unnoticed.

Identity sprawl can make rapid user provisioning or deprovisioning more challenging, leading to inconsistent entitlements and ghost accounts that can increase the risk of data loss and compromise. It can also result in inconsistent user experiences. According to Gartner, the top method for breaches involves misused credentials, which indicates that organizations without a strategy to address identity sprawl could increase their risk of a breach.[3]

IAM is at the center of a company's interaction with its users and devices, acting as the "front door" for an organization's data and applications. But the expanded use of identity-driven policies across cloud and on-premises environments makes it difficult to manage identities and achieve end-to-end governance.

Organizations are turning to unified IAM platforms that position identity as the security control for expanding IT architectures.[4] These platforms offer a centrally managed approach to security and help organizations prevent identity sprawl by managing entitlement across cloud and on-premises applications.

[2] "2021 Technology Trends to Watch," Enterprise Strategy Group, 2021 (PDF)
[3] Kasey Panetta, "The Top 8 Security and Risk Trends We're Watching," Gartner, November 15, 2021.
[4] See above



85%

of IT organizations reported an acceleration in cloud use because of the pandemic.

Organizations are turning to unified IAM platforms

that position identity as the security control for expanding IT architectures.

A unified identity platform that helps control identity sprawl

Oracle offers a unified cloud identity solution that positions user identity as the security perimeter and helps organizations pursue a zero trust security approach.

Address common use cases for human and nonhuman identities with IAM solutions and capabilities that include adaptive multifactor authentication, access management, single sign-on, and identity lifecycle management.

Integrate identities and systems to secure access from anywhere, at any time, and by any method by delivering risk-aware, end-to-end user authentication and single sign-on.

Enable a unified approach to identity and access management with cloud-based workflows that help address identity sprawl by consolidating enterprisewide identity silos into a unified platform.

Simplify lifecycle management and reduce the risk of a compromise with IAM services that improve visibility across the organization and provide advanced authentication.

Improve efficiency with a centralized view for managing policies and replace manual provisioning processes with a single manageable workflow to easily onboard new applications, users, and devices faster and with greater consistency.

Use your existing entitlements from traditional software-delivered IAM solutions or core business applications such as ERP or human resources management systems to quickly onboard new applications, users, and devices.

“We are seeing a lot of value with Oracle Identity and Access Management. It is more secure, cost effective, and resilient, allowing us to provide a highly available identity platform with improved user experience.”

Chinna Subramaniam, IAM and Directory Services Technical Director, City and County of San Francisco

Trend

Threat detection with cloud services

Organizations are turning to cloud services that can help identify threats more efficiently.

As IT infrastructure expands and business-critical applications move to public clouds, new vulnerabilities can be exposed, increasing an organization's risk of malicious activity. This increased risk means it's likely that more alerts will be generated, placing even more pressure on security teams that are already understaffed and suffering from burnout.[5]

According to Cisco's "2020 CISO Benchmark Report," many organizations are falling behind when it comes to investigating alerts, reporting that in 2020, the percent of alerts investigated fell to 48%, compared to 56% in 2017.[6] To help alleviate the growing burden on security teams, organizations are turning to cloud services to improve detection rates, reduce the impact of breaches, and shorten the time it takes to recover.

Cloud security services use data science and analytical monitoring to create a more efficient security response model. By providing a combined view of threat sightings, the urgency of alerts is reflected more accurately, removing the need to investigate anomalies individually.

Fewer than

48%

of alerts were investigated in 2020 compared to 56% in 2017.

Cloud security services use data science

and analytical monitoring to create a more efficient security response model.

[5] Kimberly Adams and Jesus Alvarado, "Cybersecurity professionals face burnout," Marketplace Tech, March 24, 2022.

[6] "2020 CISO Benchmark Report," Cisco, 2020

Cloud intelligence that helps improve threat detection

Oracle Cloud has built-in security capabilities and services that can help customers protect critical workloads and achieve a stronger security posture.

Get a unified view of cloud security posture across Oracle Cloud Infrastructure (OCI) customer tenants with Oracle Cloud Guard.

Aggregate threat intelligence data with prescriptive overall confidence assessments from Oracle Threat Intelligence Service.

Prioritize alerts and sort valid signals from noise using targeted behavior models aligned with the MITRE ATT&CK framework to detect malicious behavior with Oracle Cloud Guard Threat Detector.

Protect applications from malicious attacks and unwanted internet traffic with Oracle’s web application firewall service.

Check hosts and container images for potential vulnerabilities to help increase security confidence and reduce risk with Oracle Cloud Infrastructure Vulnerability Scanning Service.

> “There are a lot of benefits from using Oracle Cloud Infrastructure Cloud Guard. One of the biggest is the ability to go from detecting to actually responding and then enforcing security policies.”

Scott Shepard, Senior Director of IT Infrastructure and Information Security, Motorola Solutions

Trend

Using automation to help reduce the risk of data loss

To help prevent data loss, organizations are turning to cloud services that can reduce human error and infrastructure complexity with technology that self-updates, self-secures, and simplifies configuration.

Data infrastructure security continues to be a key concern for IT and security leaders. The top drivers of data loss are human errors and misconfigurations, both of which have been exacerbated by the rise of remote work.[7] With increased services, users, systems, and events—and a shortage of qualified IT and security staff—organizations are overloaded with data.[8] This has led to complicated IT infrastructures that can pose new security risks.

According to a PwC survey, 75% of executives report that their organizations are too complex, creating cybersecurity concerns.[9] But data breaches are not the only threat posed by complex infrastructures. Organizations coping with cumbersome infrastructures may also lose operational resiliency, the ability to swiftly recover from cyberattacks, and the ability to quickly innovate in rapidly changing markets.

The growing need to analyze more events and proactively plan and monitor for misconfigurations creates challenges that the cloud can help solve. As organizations cope with a shortage of skilled workers, a cybersecurity skills gap, and the growing complexity of IT infrastructure, they are shifting to cloud services that self-update, self-secure, and simplify configuration.

75%

of executives

report that their organizations are too complex, creating cybersecurity concerns.

Organizations are turning to cloud services

that can reduce human error and infrastructure complexity.

[7] Tony Pepper, "Remote Working Is Here to Stay," CPO Magazine, April 28, 2021

[8] Steve Morgan, "Top 6 Cybersecurity Predictions and Statistics for 2021 to 2025," Cybercrime Magazine, December 30, 2021

[9] "Is your organization too complex to secure?," PwC, 2022

Automated cloud security that helps reduce complexity

Oracle is focused on helping customers reduce the risk of data compromise through a comprehensive set of services.

Help keep your business protected using encryption and continuous monitoring of user behavior with Oracle Autonomous Database and OCI, further mitigating risk with our Oracle CASB Cloud Service and Oracle Cloud Infrastructure Identity and Access Management.

Automate the remediation of common security issues such as object storage that is publicly accessible with Oracle Cloud Guard by using security recipes to help security teams operate more efficiently.

Automatically set up and enforce security policies in OCI with Oracle Security Zones and help prevent human error for cloud compartments such as an immutable policy that a storage bucket shall never be internet accessible.

> “What I like about Cloud Guard is because it is continuously running and available to a wider group of people, it provides a continuous improvement process in our security posture. It's also included with OCI, which is a really good value.”

Tom Morgan, Threat Intelligence Lead, Cyber Security Group, Darling Ingredients

Trend

Layered security strategies that support a multicloud approach

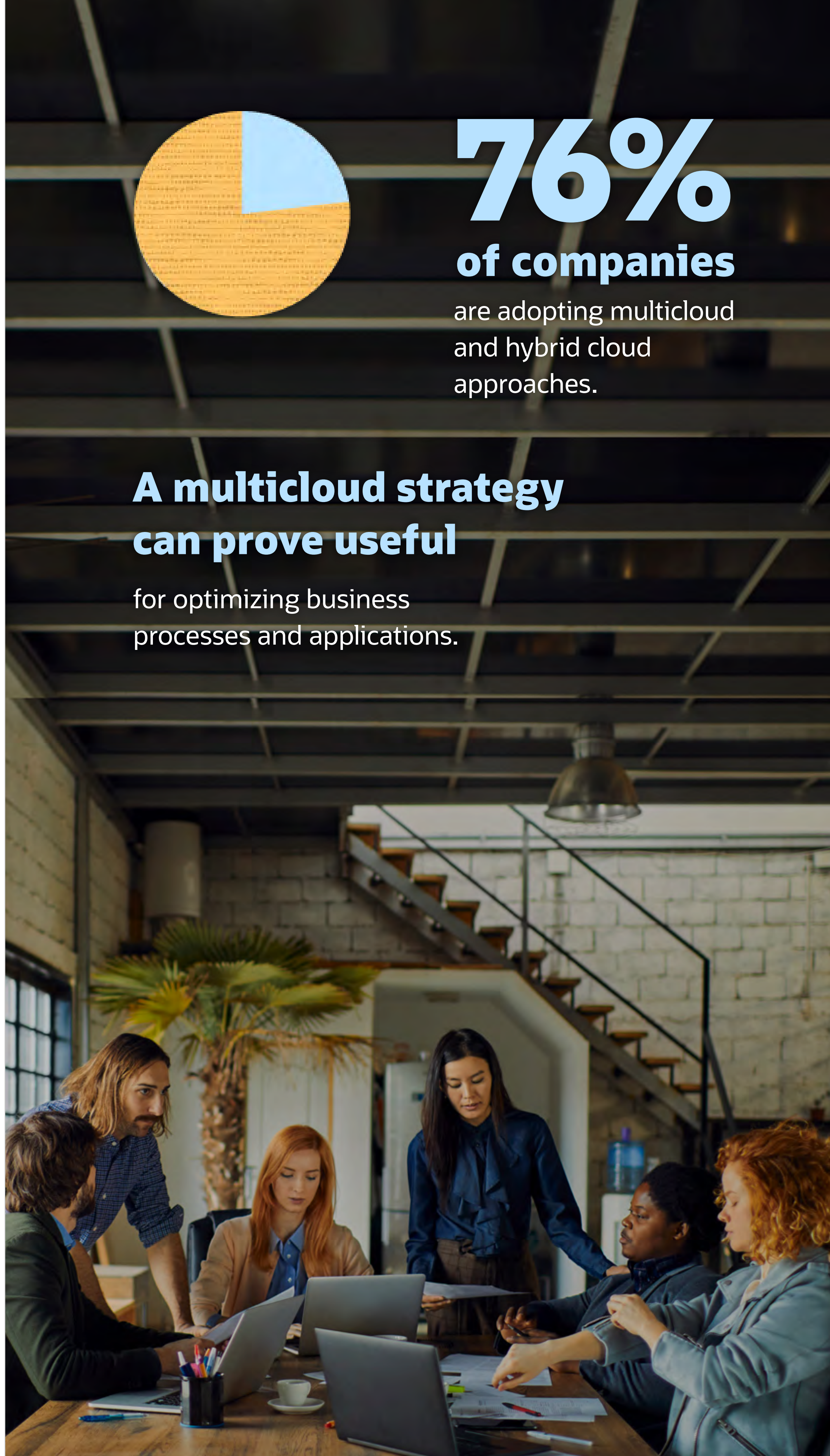
As more organizations adopt a multicloud approach, they are turning to layered security strategies that use cloud native services and integrated third-party tools.

Spending on cloud services surpassed US$1 trillion in 2024,[10] with 76% of companies adopting multicloud and hybrid cloud approaches. A multicloud strategy can prove useful for optimizing business processes and applications. But without a layered security strategy, this approach can lead to nonintegrated security tools spread across clouds, creating security tool sprawl.

Disparate security tools and multiple vendors can result in complex security operations and increased security headcount, which can lead to costly inefficiencies, ineffectiveness, and unnecessary security risk. A report from Oracle and KPMG found that, on average, organizations are using more than 100 cybersecurity tools, with 80% considering consolidating a significant number of their security technologies with a single vendor.

As organizations reevaluate their technology stack to consolidate cybersecurity and improve agility, scalability, and efficiency, they're seeking cloud service providers (CSPs) that offer products and services with built-in security and the ability to seamlessly integrate with third-party vendors. Today's security tools also need to work across different CSPs to make it convenient for organizations with a multicloud deployment to remediate issues caused by disconnected point products.

A layered security strategy can simplify your approach by using built-in cloud security services offered by the CSP combined with prebuilt APIs and CSP partnerships that integrate providers and common event models to process alerts at scale. As organizations continue to seek areas of opportunity for integrated partnerships and vendor consolidation, major CSPs will likely continue to strengthen built-in security and technical integrations with third-party vendors to support a layered approach.



76%

of companies

are adopting multicloud and hybrid cloud approaches.

A multicloud strategy can prove useful

for optimizing business processes and applications.

[10] "IDC Forecasts Worldwide "Whole Cloud" Spending to Reach $1.3 Trillion by 2025", IDC, September 14, 2021

Introduction

Unified identity and access management systems

Threat detection with cloud services

Using automation to help reduce the risk of data loss

Layered security strategies that support a multicloud approach

Corporate board members with cybersecurity knowledge

What's next for cloud security?

Multiple layers of cloud security

Oracle provides cloud native security, built-in security architecture and services, and connections to partners and other CSPs.

Easily implement Oracle's native security controls to help prevent misconfiguration errors and protect expanded attack surfaces using encryption and continuous monitoring of user behavior with Autonomous Database and OCI.

Extend security from the cloud to your on-premises environment with a single identity and access management service to manage user access and entitlements with a cloud native identity-as-a-service platform.

Establish a common information model for alerts by adopting multicloud designs, such as the Cloud Security Notification Framework(CSNF), which integrate with Oracle Cloud Guard through the efforts of the Open Community Networking User Group (ONUG).

Access a comprehensive set of multicloud solutions with OCI that includes database services, extensive monitoring capabilities, and strategic partnerships to fit your organization's needs.

Trend

Corporate board members with cybersecurity knowledge

Cyberattacks that can disrupt business processes are occurring more frequently, raising awareness and understanding of cybersecurity risks within corporate executive boards.

Cyberattacks are becoming more sophisticated and costly. By 2025, cybercrime is expected to cost US$10.5 trillion annually.[11] And by 2031, ransomware attacks are predicted to occur every two seconds.[12] As the frequency of cyberattacks continues to increase, organizations are responding by adding new board members with deep cybersecurity knowledge to better advise the business and protect corporate, consumer, and partner information.[13]

Cyberattacks require quick action—sometimes necessitating a response in a matter of seconds. Research from Ponemon Institute showed security breaches were estimated to cost organizations US$4.24 million per incident on average in 2021, an increase of 10% from 2019.[14] Nearly half of the breaches studied in the report exposed customers’ personally identifiable information (PII). The potential for breaches targeting sensitive information makes cybersecurity a key focal point for strategy and risk management. Boards without cybersecurity experts can lack the ability to take immediate action to counter the effects of a breach, leading to potentially adverse effects for business groups, customers, partners, and brand reputation.

To effectively prepare for and respond to cyberthreats, corporate boards should be equipped with an understanding of their organizations’ data assets, cyber-risk, incident response planning, and regulatory and legal obligation—and they should be prepared to discuss these issues regularly. Board members with cybersecurity knowledge can advise the business and make appropriate decisions that will reduce the risk of disruption and loss that can impact the organization, their customers, and their shareholders.

By 2025, cybercrime is expected to cost

US$10.5T

annually.

Cyberattacks require quick action

sometimes necessitating a response in a matter of seconds.

[11] Steve Morgan, “Cybercrime to Cost the World $10.5 Trillion Annually by 2025,” Cybercrime Magazine, November 13, 2021

[12] David Braue, “Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031,” Cybercrime Magazine, June 2, 2022.

[13] Kasey Panetta, “The Top 8 Security and Risk Trends We’re Watching,” Gartner, November 15, 2021.

[14] Abi Tyas Tunggal, “What Is the Cost of a Data Breach in 2022,” UpGuard, May 12, 2022

Solutions that help address your board's top security concerns

Oracle is focused on helping organizations reduce risk by providing a comprehensive set of simple, prescriptive, and integrated security capabilities that enable security leaders to provide insights to corporate boards.

Security: Oracle has decades of experience securing data and applications. Oracle Cloud incorporates built-in security that can help you protect your organization's infrastructure, apps, and data against cyberattacks and adhere to compliance mandates.

Data Privacy: Oracle helps customers comply with data privacy principles with Oracle Cloud Infrastructure privacy features.

Compliance: Oracle pursues many programs that audit Oracle Cloud and help customers address compliance with global, regional, and industry-specific certifications.

Introduction

Unified identity and access management systems

Threat detection with cloud services

Using automation to help reduce the risk of data loss

Layered security strategies that support a multicloud approach

Corporate board members with cybersecurity knowledge

What's next for cloud security?

What's next for cloud security?

As security strategies continue to evolve alongside changing IT infrastructure and business requirements, the need for simple security solutions is clear. And as cyberattacks increase with a sophistication and speed that matches that of IT innovation, security will continue to receive attention from all levels of the organization.

To stay ahead, IT and security leaders are looking to cloud services to help them outpace cyberthreats, reduce complexity, and protect critical business assets. Backed by the cloud and growing support from the C-suite and board members, IT and security leaders have new opportunities to innovate and strengthen security across their organizations.

Try Oracle Cloud Free Tier

Learn how customers are simplifying security with Oracle Cloud

Learn how

Read more about Oracle Cloud Infrastructure security

Read more

View more cloud strategy insights

View more

ORACLE