Intelligent, Automated Security

Reduce risk vs Reduce threats.

Navigating the new threat landscape.

The security landscape is evolving more quickly than ever before. As attackers use more-advanced methods and more-sophisticated tactics to infiltrate networks, undermine services, and steal valuable data, enterprises are struggling to keep up. Automated threats—where it's not a human being sitting behind a console, but rather an automated program running scripts in an attempt to infiltrate your systems—have become ordinary.

Nearly 90 percent of organizations experience data breaches[1], 55 percent have experienced one of the two major forms of a phishing attack,[2] and 66 percent say cyberattacks have interrupted operations in the past 24 months.[3] Organizations find it difficult to deal with the pace and persistence of attackers for the following key reasons:

1 Inadequate perimeter defenses.

Most organizations rely on traditional perimeter defenses to protect the network. But in the mobile-first hybrid-cloud world, the network perimeter has dissolved. So while antivirus and firewalls are still important aspects of any security posture, protecting the network does little to safeguard the data and services that reside in the cloud.

91% of organizations have security concerns about adopting the cloud

...only

14% believe traditional security is enough[4]

2 Alert overload.

Most security operations centers (SOCs) are overwhelmed by intrusion detection systems that issue too many alerts with not enough context. Dealing with so many false positives doesn't just waste security resources; it can also lead to dangerous *alert fatigue*, with the risk that genuine attacks could be missed.

36% of cybersecurity professionals say their top challenge is keeping up with the volume of security alerts

42% say they ignore a significant number of alerts because of how many they receive[5]

Cybersecurity professionals use an average of **46** different security tools[6]

According to a 2016 Ponemon Cost of Data Breach Study, the average breach at large enterprises costs US$3.62 million and takes 191 days to detect.[7] These alarming statistics are partially a result of alerts from so many vendors, products, consoles, and security tools: There is too much noise and not enough actionable insight.

3 Cybersecurity skills shortage.

The difficulty of hiring skilled cybersecurity professionals compounds the problem of alert overload. With too few skilled resources trying to assess too many alerts, many SOCs find themselves chronically understaffed.

The global cybersecurity workforce will have **more than 2 million unfilled positions** by 2019[8]

84% of organizations believe **less than half** of applicants for security jobs are qualified

Nearly 50% are currently evaluating and planning for security automation solutions

71% are using machine learning capabilities, or adding them to existing security tools[9]

Today's advanced threats demand intelligent and automated security solutions.

With a range of new security threats and risks, organizations need new solutions to help them secure critical IT resources. Automated tools offer new solutions that can help combat rising security demands. Able to automatically detect vulnerabilities and attacks, and fix them before they can be exploited, such security solutions will soon become an essential part of the IT security puzzle.

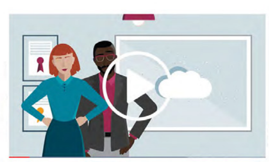
Forward-looking organizations are already adopting cybersecurity technologies that are continuous, adaptive, real-time, and intelligent. They rely on artificial intelligence (AI) and machine learning (ML) algorithms to manage configurations, monitor who has access to what resources, and encrypt sensitive data to protect IT assets.

Oracle Identity SOC

A context-aware, comprehensive SOC solution reduces threats with machine learning.

The world's first identity-based SOC framework uses advanced analytics and machine learning to put security risks in an identity context—delivering actionable intelligence that can help automate threat response.

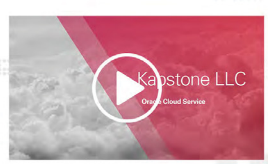
Oracle Identity Security Operations Center offers an intelligent, identity-driven, and context-aware approach to better protect users, applications, APIs, content, and workloads. It makes it far simpler and quicker to predict, prevent, detect, and respond to advanced attacks across your entire hybrid-cloud estate.



What our customers said:

"Oracle gives our customer a security framework that allows them to continue to embed Oracle or non-Oracle applications and helps accelerate time to market."

Saurabh Sharma, Principal Managing Partner, Kapstone Technologies



"We chose Oracle Identity Cloud Service because of our confidence in Oracle, the ability to integrate with the Oracle Cloud ecosystem, and the back-end support we received to help accelerate implementation."

Paul Van Hout, CEO & Founder, Pragmatyxs

Learn more about Oracle Cloud security →

1 "Perceptions About Network Security," Ponemon Institute survey, June 2011, juniper.net/us/en/local/pdf/additional-resources/ponemon-perceptions-network-security.pdf.
2 "The Oracle and KPMG Cloud Threat Report 2018," Oracle and KPMG, 2018, oracle.com/cloud/cloud-threat-report.html (registration required).
3 "The Oracle and KPMG Cloud Threat Report 2018," Oracle and KPMG, 2018, oracle.com/cloud/cloud-threat-report.html (registration required).
4 "Cloud Security: 2016 Spotlight Report," Crowd Research Partners, 2016, immun.io/2016-cloud-security-report (registration required).
5 Jon Oltsik, "Dealing with Overwhelming Volumes of Security Alerts," ESG Global, March 3, 2017, esg-global.com/blog/dealing-with-overwhelming-volume-of-security-alerts.
6 "The Oracle and KPMG Cloud Threat Report 2018," Oracle and KPMG, 2018, oracle.com/cloud/cloud-threat-report.html (registration required).
7 Larry Ponemon, "2017 Ponemon Institute Cost of a Data Breach Study," Ponemon Institute white paper, July 26, 2017, securityintelligence.com/media/2017-ponemon-institute-cost-of-a-data-breach-study/.
8 "2016 Cybersecurity Skills Gap," ISACA infographic, 2016, image-store.slidesharecdn.com/be4eaf1a-eea6-4b97-b36e-b62dfc8dcbae-original.jpeg.
9 "The Oracle and KPMG Cloud Threat Report 2018," Oracle and KPMG, 2018, oracle.com/cloud/cloud-threat-report.html (registration required).

ORACLE

Oracle Cloud Ebook

Intelligent, Automated Security

Reduce risk vs Reduce threats.

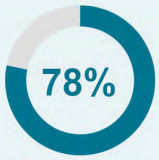
There was a time when security concerns made many organizations reluctant to move to the cloud. This attitude persists today in many IT organizations. In fact, in the Oracle and KPMG Cloud Threat Report 2018, detecting and reacting to security events in the cloud was seen as the number one cybersecurity challenge facing organizations.

While some are skeptical of cloud security, many are beginning to recognize that moving to the cloud can actually offer many security benefits. Today, 83 percent consider cloud security to be as good as (or better than) on-premises security.[11]

of organizations are concerned that employees are violating cloud usage policies

Only 31% understand their responsibilities with SaaS cloud service providers[12]

As organizations transform traditional, on-premises infrastructures into hybrid environments, they realize that top-tier cloud providers can offer much better security than most enterprises can deliver in-house.



of organizations say the cloud can improve both their security and their agility[12]

Oracle Cloud security aligns *people*, *processes*, and *technology*—augmented with robust *physical* controls—to provide integrated defense-in-depth protection and consistent security across complex hybrid and multicloud environments.

Technology

Security embedded at every layer of the cloud computing stack: SaaS, PaaS, and IaaS.

Processes

Proven best practices, including Oracle Software Security Assurance, to ensure secure coding standards.

People

Talented cybersecurity professionals, all trained in Oracle's rigorous best practices.

Physical

Nineteen Tier-3 enterprise-grade data centers worldwide, with multilayered physical controls—from mantraps to biometrics, and much more.

Learn more about Oracle Cloud security →

10 "The Oracle and KPMG Cloud Threat Report 2018," Oracle and KPMG, 2018, oracle.com/cloud/cloud-threat-report.html (registration required).

11 "The Oracle and KPMG Cloud Threat Report 2018," Oracle and KPMG, 2018, oracle.com/cloud/cloud-threat-report.html (registration required).

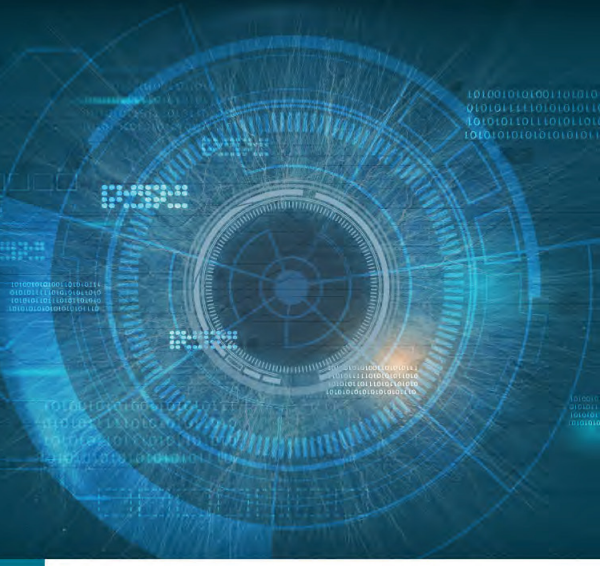
12 "A Secure Path to Digital Transformation," Coleman Parkes Research, 2016. http://colemanparkes.com/

ORACLE

Oracle Cloud Ebook

Intelligent, Automated Security

Reduce risk vs Reduce threats.



Gain visibility and consistent security with Oracle Cloud Access Security Broker Cloud Service

As your cloud footprint expands, so does your risk profile. It gets harder to keep track of shadow IT and user behavior, identify potential threats, and apply consistent polices and security configurations for all users, applications, data, and networks.

With a cloud access security broker (CASB), you can increase visibility and ensure consistency across your hybrid-cloud environment. And Oracle CASB Cloud Service makes it even simpler—providing clear visibility of all SaaS, PaaS, and IaaS deployments from a single pane of glass, as well as security automation to predict and detect threats, and respond quickly to incidents.

- See your entire cloud footprint from a single UI
- Identify internal risks with advanced user-behavior analytics and shadow IT discovery
- Tailor security configurations and get alerts when policies are changed or disabled
- Get maximum value from existing solutions by extending their benefits to the cloud

Oracle CASB Cloud Service also includes integrated machine learning, artificial intelligence, and contextual awareness, helping it address the rise of security incidents targeting privileged and end-user credentials.

> "Ooyala's cloud-first posture meant that our security coverage just got broader, but I can't afford to throw more bodies at the problem.
>
> "We needed a modern approach to security and to take advantage of new automation tools to allow me to 'trust but verify' what my vendors, service providers, and employees were doing in our cloud environment. With Oracle CASB Cloud Service, we now monitor user behavior across cloud properties as well as automatically detect configuration drift. This gives us consistent, detailed and clear visibility into user and application activity."
>
> **Bill Billings, Chief Information Security Officer, Ooyala (a subsidiary of Telstra)**

> "We chose Oracle CASB Cloud Service and Oracle Advanced Security to minimize risk exposure and gain transparency, high visibility, and control. This allowed us to stay a step ahead of threats while enforcing our cloud environment security configurations and EU GDPR compliance with minimum performance impact."
>
> **Dimosthenis Nikolopoulos, IT Operations & Program Management Director, WIND Hellas**

Learn more about Oracle Cloud security →

ORACLE

Oracle Cloud Ebook

Intelligent, Automated Security

Reduce risk vs Reduce threats.

Today's hybrid environments present many new attack vectors, and with the growing volume and sophistication of zero-day exploits, traditional network-centric security measures are no longer enough.

Some organizations are taking measures to improve IAM. 45 percent have implemented quarterly reviews of authorization levels and entitlements, while 66 percent are interested in using two-factor authentication to combat access anomalies. But these measures alone aren't always enough to deliver IAM that truly secures the enterprise.

As traffic bypasses existing security tools, cloud-based identity management—combined with analytics and machine learning—is the best way to combat the risk of advanced attacks.

Of course, while eliminating unauthorized access, you need to ensure that authorized users get a frictionless experience. To do that, you need the capability to seamlessly manage user identities across a multitude of cloud and on-premises applications.

That's why Oracle Identity Cloud Service enables you to maintain a single identity for each user across their on-premises and cloud services, giving them seamless, single-sign-on access while protecting your existing identity and access-management investments. With a range of automation and machine learning capabilities built in, Oracle Identity Cloud Service can help you combat emerging security threats—without compromising your users' experience.

In this new threat landscape, identity is the key to securing users, applications, and networks. Yet many organizations struggle with Identity and Access Management (IAM):

Over 33 percent say mobile devices and apps make IAM more difficult

have no central IAM strategy[13]

"The Identity Cloud Service is Oracle's most important new innovation in the cloud. You can use the same security architecture you use in your on-premises environment as you use in the cloud. They're really the only vendor that can do that."

Aaron De Los Reyes, Senior Director, Oracle Technology, Cognizant

"With Oracle Identity Cloud Service, we can reduce the time it takes to complete identity-management processes from months to just a few hours."

Ryu Taniguchi, System Architect, Ricoh

Out-Sourcing!

Outsourcing Inc. enhances security without compromising user experience.

A leading global provider of outsourcing services, Outsourcing Inc. was experiencing rapid growth through M&A activities and diversifying its customer base in new industries and geographies.

Challenge

The group's global workforce needed best-in-class security while working seamlessly on multiple cloud services and on-premises applications.

Solution

Oracle Identity Cloud Service enhances security and gives users single sign-on authentication to access documents and applications.

Benefits

Outsourcing Inc. has established an agile, secure environment to improve user experience, streamline operational management, and support the group's future business growth.

Get the full story →

"Oracle has a proven record of providing the best-in-class management solutions, and we are convinced that the Oracle Identity Cloud will be the foundation for the future growth of Outsourcing."

Kinji Manabe, General Manager, Business Management Department, Outsourcing Inc.

中国民生银行 CHINA MINSHENG BANK

China Minsheng Bank simplifies identity management for over 40,000 users.

China Minsheng Bank provides consumer and business banking services both domestically and abroad.

Challenge

China Minsheng Bank needed a new way to comply with strict commercial banking regulations while ensuring its business users could still seamlessly access critical systems.

Solution

Oracle Access Management Suite Plus offers a scalable identity and authentication-management platform.

Benefits

China Minsheng Bank has standardized identity management and access-control administration for over 40,000 employees, eliminating redundant workload to create and manage individual user identities.

Get the full story →

TATA DOCOMO

DOCOMO Systems deploys a secure, reliable identity authentication platform.

DOCOMO Systems is a subsidiary of NTT DOCOMO, which, with 60 million customers, is the largest mobile service provider in Japan.

Challenge

DOCOMO needed to introduce a cost-effective and easy-to-deploy identity management platform that supports various new and legacy authentication formats.

Solution

Integrating databases with Oracle Exadata and deploying Oracle Identity Management solutions has enabled DOCOMO to create a scalable, powerful authentication platform.

Benefits

DOCOMO's new platform enables flexible, reliable authentication while keeping costs low.

Get the full story →

Learn more about Oracle Cloud security →

13 "The Oracle and KPMG Cloud Threat Report 2019," Oracle and KPMG, 2019, oracle.com/cloudcloud-threat-report.html (registration required).

14 "The Oracle and KPMG Cloud Threat Report 2019," Oracle and KPMG, 2019, oracle.com/cloudcloud-threat-report.html (registration required).

ORACLE

Oracle Cloud Ebook

Intelligent, Automated Security

Reduce risk vs Reduce threats.

Safeguarding data has always been a critical priority for IT teams. But with increasing incidences of data breaches and growing number of data-privacy and security regulations such as the EU GDPR, data protection is at the top of every enterprise agenda.

To comply with the requirements of regulations such as GDPR, it's essential to enforce comprehensive security controls wherever your data resides across complex hybrid environments.

Oracle is a leader in preventive and detective controls for databases, and helps customers safeguard their most valuable data with a comprehensive set of hybrid-cloud data-security solutions, providing a layered, in-depth approach to data protection.

99.9%

of all data breaches exploited a vulnerable server where a patch was available at least a year prior to the breach.[1]

As organizations transition to the cloud, they gain security by design and default with Oracle Database Cloud Service, automatically encrypting data in transit and at rest. And with Oracle Autonomous Database Cloud, the database automatically applies patches and security updates while running—eliminating downtime and human error, and providing increased protection against emerging threats.

> "With Oracle Identity and Access Management, we reduced risk and improved compliancy. We quickly implemented this solution to our 10,000 users, both internal and client users, with Oracle Consulting and increased onboarding by up to 10%. The solution provides ISO to operational applications."
>
> **Guillermo Lanza, Project Manager, Telefónica Business Solutions**

Oracle's hybrid-cloud security services help you maintain continuous regulatory compliance by enforcing consistent policies and controls to protect users, applications, and data.

Learn more about Oracle Cloud security →

> "On our path towards EU GDPR compliance, we chose Oracle Database Security solutions including Oracle Advanced Security, Oracle Key Vault, Oracle Database Vault, Oracle Audit Vault and Oracle Database Firewall to streamline and simplify our Oracle deployment. With Oracle, we minimize risk and further enhance our overall security."
>
> **Henrique Zacarias, CIO, NOS**

UBI Banca

UBI Banca addresses GDPR requirements with end-to-end security.

With Oracle Security Service, the bank now has a comprehensive approach to security across its on-premises and cloud deployments, increasing control without impacting the user experience.

> "We have invested in Oracle Security Cloud Service to enhance our ability to detect and respond not only to potential threats but also data leakage, and to better meet our regulatory requirements."
>
> **Fabio Gianotti, Chief Security Officer, UBI Banca**

Rakuten

Rakuten Securities enhances data security for two million customer accounts.

Japan's largest online financial brokerage company needed to strengthen its data security to comply with the Japanese government's My Number national identification system.

Challenge

Rakuten needed to integrate access control for disparate security systems into a single platform and achieve defense-in-depth protection against unauthorized access.

Solution

The company deployed a new defense-in-depth security platform in six months with Oracle Database Security options and Oracle Consulting expertise.

Benefits

Rakuten now has superior data security and can meet stringent regulatory requirements with transparent data encryption for customer information, and monitoring and auditing unauthorized access.

Get the full story →

> "Oracle is the only vendor that provides a one-stop shop for security solutions, helping us to comply with regulatory requirements and protect sensitive data."
>
> **Hiroaki Terashima, Manager, Operation Management Division, Information Security Department, Rakuten Securities, Inc.**

DGOJ protects more than 160GB of sensitive data a month.

Spain's Directorate General for the Regulation of Gambling (DGOJ) needed to ensure the security, traceability, inalterability, and recoverability of online gambling data.

Challenge

The DGOJ needed to store, inspect, and protect data from thousands of daily transactions in Spain's online gambling market.

Solution

Oracle Advanced Security now provides high availability, data integrity, encryption, and access to massive quantities of sensitive data.

Benefits

The DGOJ can now supervise and inspect large quantities of data in a secure way, meeting its strict standards for data protection and privacy.

Get the full story →

> "Oracle Advanced Security enables us to securely store and encrypt more than 160GB of sensitive data each month. Nothing gives me more peace of mind than knowing that the data we collect is safe and helps us be more effective at our job of regulating gambling."
>
> **José Antonio García García, Deputy Director of Institutional Management and Relations, Directorate General for the Regulation of Gambling, Ministry of Finance and Civil Service**

PRAGMATYXS

Pragmatyxs Maximizes Customer Value and Minimizes Administrative Costs

Seattle-based consulting and solution provider, Pragmatyxs, needed to boost added value and security for its customers, while ensuring they didn't break their budget.

Challenge

Pragmatyxs was looking to provide maximum value to its customers, while maintaining security and minimizing administrative costs.

Solution

Oracle Database Cloud Service provides rapid application development, fast and predictable performance, transparent data-encryption security, and elastic scalability to support future growth—without the need for upfront hardware costs.

Benefits

Pragmatyxs customers now have complete peace of mind over the security of their data, thanks to lower risk of compromise.

Get the full story →

> "One of the key benefits of moving to Oracle Database Cloud Service was transparent data encryption—we could assure our customers that, right out of the gate, their data was secure, and the risk of compromise was minimum."
>
> **Paul Van Hout, CEO & Founder, Pragmatyxs**

Learn more about Oracle Cloud security →

1) "2015 Data Breach Investigations Report," Verizon, insider.zurich.co.uk/app/uploads/2015/05/Verizon%E2%80%99s-2015-Data-Breach-Investigations-Report.pdf