Secure and Manage Hybrid Clouds

Automated Capabilities Simplify Management and Mitigate Cyberthreats

Cloud **Essentials**

ORACLE Cloud

Take Charge of Diverse IT Environments

Cloud-based business models create tremendous new opportunities, but they also expose companies to new management challenges and security risks. Application portfolios are projected to grow at a rate of more than 50 percent in the years ahead—and most of these new applications will be developed using versatile cloud-based technologies such as functions, containers, and microservices. More than 70 percent of today's organizations have adopted multiple clouds, boosting security risks and necessitating more effective management practices. Today's cyberattacks are more advanced and well-funded than ever. Hackers and cybercriminals are intent on disrupting business operations and stealing sensitive assets.

Security teams struggle to innovate and keep pace with these persistent attacks as users, applications, data, and devices proliferate—a critical situation that has led to ever-expanding IT responsibilities in both scope and complexity. The corporate technology footprint, once confined to the data center, now includes a raft of new mobile apps, many types of structured and unstructured data, and a steady influx of SaaS applications and cloud services, creating a diverse and complex hybrid IT environment. IT operations teams and security operation centers (SOCs) must protect this environment, manage an untethered workforce, and support the activities of distributed DevOps teams that are creating new types of virtual applications based on microservices.

Use an Intelligent, Cloud-Based Platform for Automated Management and Security

Oracle makes it easy to secure and manage these evolving hybrid cloud environments with an intelligent, cloud-based platform that prevents, detects, and rapidly responds to performance issues and security threats, thereby easing the burden on overworked IT staff and streamlining routine administrative tasks. Building on more than 40 years of expertise managing and securing enterprise computing environments, Oracle recently introduced management innovations that take advantage of the latest artificial intelligence (AI) and machine learning capabilities. Read on to learn about this unique solution for managing and securing hybrid cloud environments.

> Oracle Cloud includes machine learning algorithms to detect suspicious activities without human interaction, making it easier to secure both hybrid and traditional cloud environments.

Security and Management Leader

- Improve visibility into applications and users of on-premises, Oracle Cloud, and third-party cloud environments.
- Automate preventative and corrective actions to ensure best performance and security for the entire organization's technology portfolios and users.
- Enhance efforts to discover shadow IT processes throughout the enterprise and enforce rigorous cloud security protocols.
- Better address strict regulatory and compliance mandates such as the General Data Protection Regulation (GDPR).
- Enforce access controls by authenticating and authorizing cloud applications and IT resources.

Oracle's Security and Management Cloud Solutions

Collect, normalize, and make sense of:

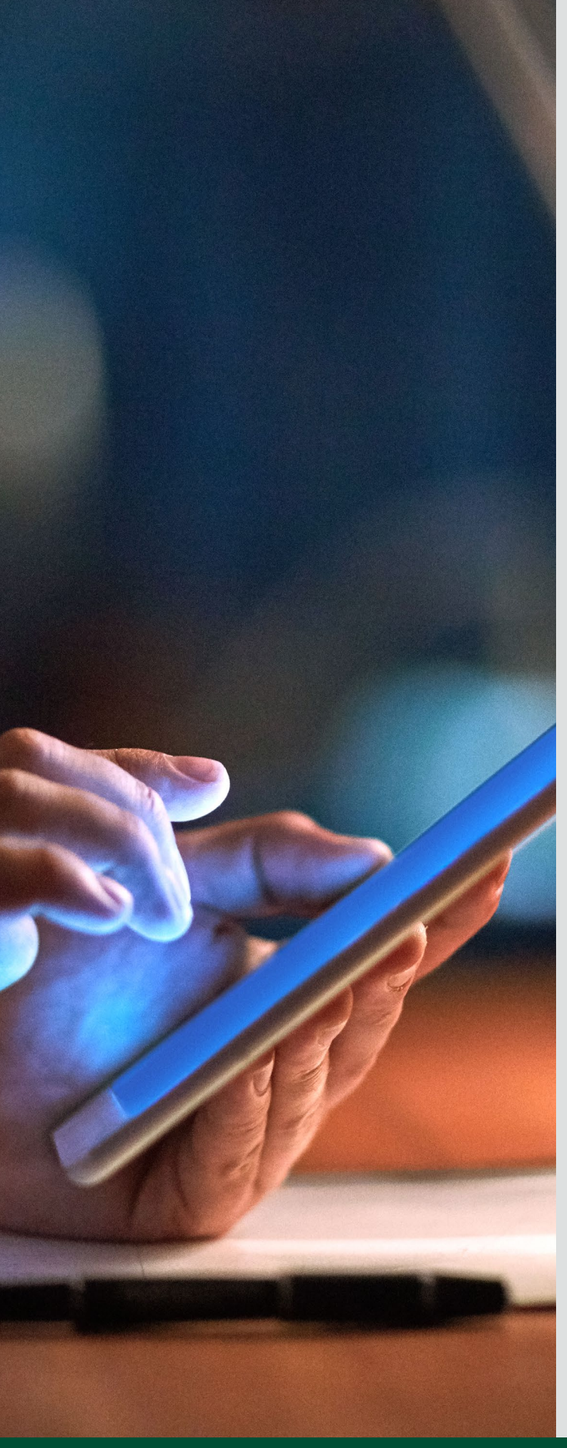
- Logs
- Security events
- External threat feeds
- User and entity activities
- Database transactions
- Application performance

Comprehensive data

Normalized, single source of truth

Automated anomaly detection and response

Heterogeneous and open



Get a Handle on Security

Managing risk is a daunting responsibility. For example, if a critical application goes down or performance slows unexpectedly, is it a distributed denial of service (DDoS) attack or an internal mishap? As data and applications multiply, in the data center and in the cloud, it becomes increasingly difficult for security and management teams to make these distinctions—and thousands of others—every day. Large organizations, on average, use 46 different security tools to address today's sophisticated attacks[1], yet 84 percent of IT professionals interviewed for a recent cloud security report said that these traditional security solutions either don't work at all in cloud environments, or have limited functionality.[2]

In the Equifax data breach of 2017, 140 million people were affected, and millions of sensitive records were compromised. Before Equifax could mitigate the risk by deploying an available patch, cybercriminals had created malware that exploited that unpatched system. This situation was unfortunate—yet all too familiar. IT teams often delay implementing critical patches to address software vulnerabilities because it can be a complicated process involving coordinated management of hardware, software, and networking personnel, including taking databases offline from production environments, installing the patch, and then rebooting the associated systems. While companies procrastinate, hackers seize the opportunity.

Rely on Self-Patching, Self-Securing Technology from Oracle

Oracle provides a suite of automated security cloud services to secure your users, applications, data, and infrastructure. The solution includes AI and machine learning technology to protect your information systems from both external attacks and malicious internal users. Best of all, Oracle's automated security cloud solution detects available patches and automatically applies them—without downtime—effectively eliminating vulnerabilities and human errors.

Encrypting production data and implementing strong controls over the behavior of privileged users can address many security and regulatory requirements. Now, you no longer have to perform these activities manually because Oracle's automated services do it for you. Data is encrypted transparently. Strong user controls prevent administrators from seeing sensitive data. And by automating the process of detecting and responding to security alerts, Oracle dramatically improves mean time to detection (MTTD) and mean time to remediation (MTTR).

1 "Oracle and KPMG Cloud Threat Report 2018: Keeping Pace at Scale—The Impact of the Cloud-Enabled Workplace on Cybersecurity Strategies," study sponsored by Oracle and KPMG, 2018.
2 Crowd Research Partners, "2018 Cloud Security Report," 2018.

Real-Time Insights Alleviate Information Overload

According to one recent estimate, security teams struggle to manually manage approximately 17,000 alerts each week per enterprise—only four percent of which are investigated.[3] It's a dismal success rate—with potentially catastrophic consequences. In some instances, data breaches have resulted in regulatory fines, legal fees, and class action lawsuits totaling hundreds of millions of dollars. In the case of new regulations such as the European Union's GDPR, organizations can face fines up to four percent of annual revenue for noncompliance.

Some companies don't address certain security and management tasks because they assume the cloud provider is handling them. However, when working with cloud vendors, you need to closely examine the service level agreements to determine who is responsible for what. Having agreements with multiple cloud providers exacerbates the challenge of gaining consistency for security and management across cloud environments. In a survey of 450 global security leaders, only 31 percent could correctly identify what they are actually responsible for.[4]

Most cloud vendor agreements stipulate a shared responsibility model. The vendor guarantees to provide a secure and continuously available application service, while the customer secures access to that service by its employees. In some cases, the customer is also responsible for securing the data in SaaS applications. In a shared responsibility model, customers own the identity access management (IAM) policies for SaaS applications as well as the customer data within those apps. This means that while a cloud provider is responsible for the security of its global infrastructure, each customer must implement security measures according its own corporate risk policies.

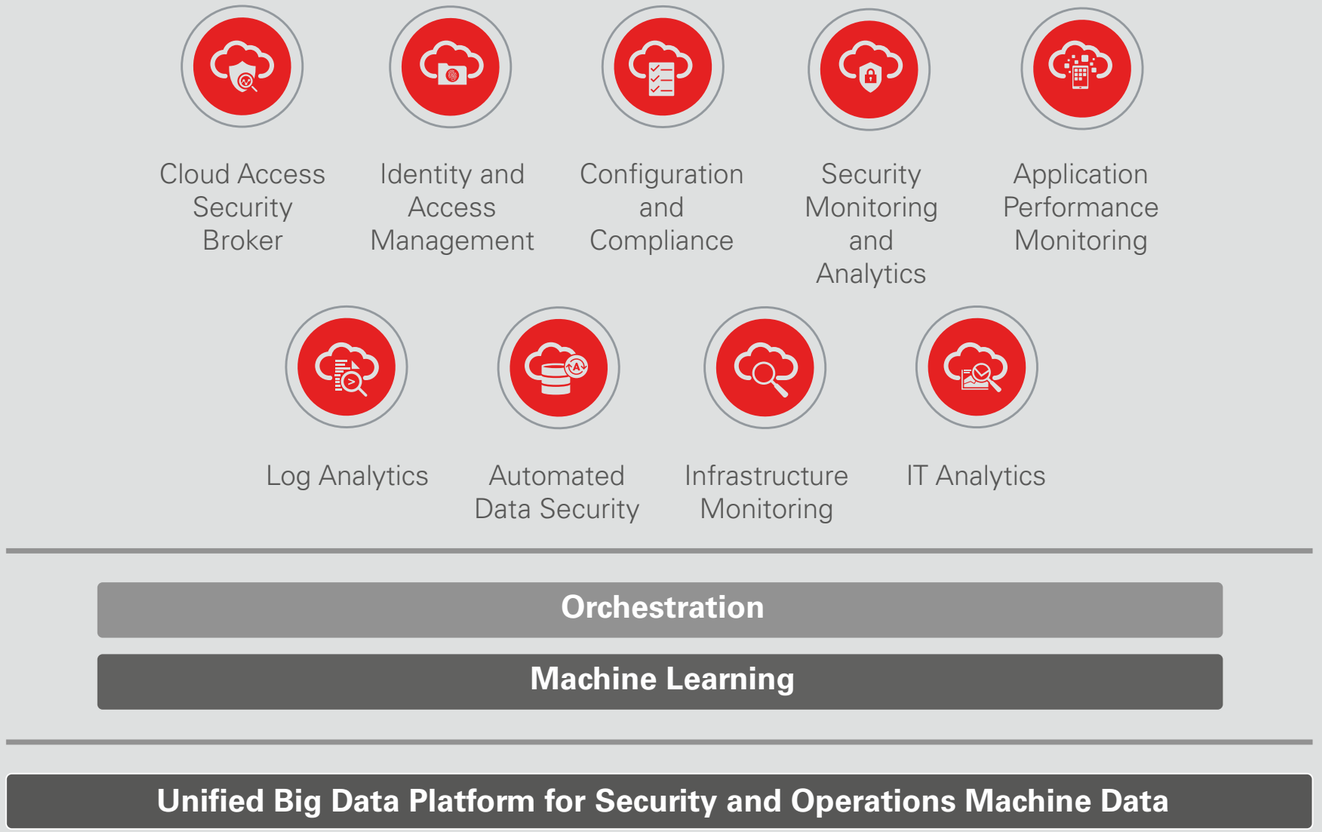
3 Ponemon Institute, "The Cost of Malware Containment," study sponsored by Damballa, 2015.
4 "Oracle and KPMG Cloud Threat Report, 2018."

Oracle Automated Security and Management

Oracle's security and management cloud services automatically collect and analyze operational and security metrics. Machine learning algorithms deliver insights to streamline diagnostics, capacity planning, operational forecasting, and business analytics. Armed with a comprehensive understanding of how your applications are performing, and backed by automated remediation capabilities, your security and management teams can expedite issues and take corrective action.

Machine learning techniques include:

- **Anomaly detection:** Flags unusual resource usage and identifies configuration changes
- **Clustering:** Combines related security alerts and aggregates topology-based data
- **Correlation:** Groups alerts based on related symptoms to discover dependencies
- **Forecasting:** Predicts outages before they happen



The Importance of Integration Between Security and Management

Identity management systems are essential for authorizing access to IT resources. However, as cloud apps proliferate, many organizations find themselves with too many silos of identity data. Automated capabilities within **Oracle CASB Cloud Service** and **Oracle Identity Cloud Service** enable a unified identity model that eliminates the need for manual identity monitoring.

For example, if a credentialed HR user logs into the financial database instead of the HR database, an alert will be issued to flag the anomalous behavior. Depending on the business rules, it may lock the user out of that application, raise the risk score, or initiate a multifactor authentication procedure.

Automate Essential Activities for DevOps and SOC Professionals

Oracle Management Cloud provides a unified platform for continuously collecting, classifying, and analyzing all machine data. The machine learning capabilities are pre-trained for operational and security pattern recognition. And with integrated tooling for security and management, it eliminates the human effort associated with traditional management toolsets across heterogeneous technology on premises, in Oracle Cloud, and in third-party clouds.

Oracle's identity-based SOC framework provides comprehensive monitoring, threat detection, analytics, and remediation tools across hybrid environments that include on-premises and cloud resources. These cloud services are designed to unify activity and contextual threat, user, and operational data from multiple sources and enable SOCs to respond in real-time to emerging threats.

Oracle Identity Cloud Service synchronizes user identities from on-premises sources such as Oracle Directory Services, Microsoft Active Directory, and other LDAP directories, extending on-premises identities to the cloud with appropriate access controls. It simplifies login procedures by federating access to multiple applications via single sign-on, while also automating account management, provisioning, and auditing of user activities. As new cloud applications come online, you can use Oracle Identity Cloud Service to securely provision the users of those applications based on their on-premises identities.

Oracle CASB Cloud Service uses machine learning to automatically detect risks when accounts are compromised—such as users logging in from unexpected locations and unrecognized devices. It can monitor changes to security policies, such as changes to role settings that impact access privileges for sensitive information.

The Value of a Comprehensive Platform

- Highly automated security and management
- Protection for hybrid, heterogeneous clouds
- Machine learning technology that automates the protection of systems, applications, users, and devices
- Single-window visibility that orchestrates management activities across cloud and on-premises environments

A Management Platform for the Future

Oracle's comprehensive security and management platform also employs user and entity behavior analytics to identify suspicious and malicious user activity. A unified data repository spans log, performance, user experience, and configuration data, while preventative controls intercept data leaks. Customers that use Oracle Autonomous Database will gain additional protection for their data with machine learning algorithms that automatically parse SQL statements and use these insights to establish whitelist baselines by user, group, database, and application. The database automatically evaluates new SQL queries against this baseline to spot potential threats, raise threat scores, and take action to protect sensitive data.

By establishing baselines of typical behavior, Oracle also uses automated technology to recognize unusual activities, such as when a user unexpectedly changes permissions, privileges, or configuration settings. Rather than manually investigating incidents separately in each application and at each level of the stack, your security team can obtain a complete view of a multicloud environment—including all users and devices—through a single pane of glass.

> "Customers who use Oracle Management Cloud obtain IT analytics to forecast their application landscape, security analytics to detect threats from inside and outside their company, and log analytics to identify bottlenecks in their applications. Some of them use the entire stack, especially the security monitoring feature to gain insight into security threats."
>
> **Michel Schildmeyer, Technical Solutions Architect, Qualogy**

An Automated Security and Management Platform

Betacom Resolves IT Issues with Oracle Management Cloud

Organization: Betacom is a leading Polish technology provider. The company supports business transformation projects executed by their customers, assisting medium and large enterprises in defining technology driven initiatives. Helping in partnership mode to simplify business models and use edge technology (such as AI, cloud and big data solutions) for the needs of individual business areas. Using products from Oracle, Betacom aims to increase the operational efficiency for clients and to release their potential for innovation.

Challenge: To improve application performance and security, Betacom sought a robust IT management solution to gain a holistic view of its clients' IT infrastructures. The company needed a more efficient way to analyze data from clients' mission-critical systems and accelerate the creation of critical reports. Company leaders wanted to minimize their dependence on on-premises systems management tools and reduce the probability of critical system failures.

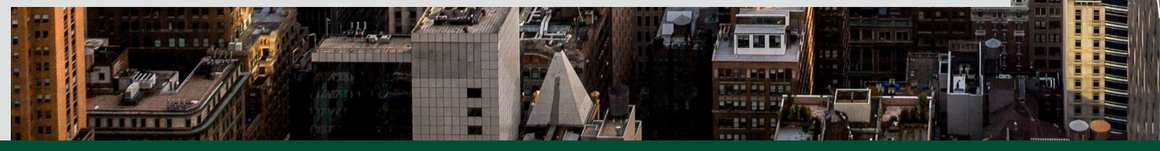
Strategy: Betacom now uses Oracle Management Cloud to analyze the health and security of its client applications. They chose Oracle Management Cloud for its proactive systems management rapid troubleshooting, and extensive performance monitoring.

Success: Betacom leveraged the Oracle Management Cloud to help a leading Polish energy provider analyze event data from its mission-critical systems, minimizing the client's dependence on legacy management tools and shortening issue resolution time from days to minutes. Now, Betacom can more easily analyze the health and security of its clients' applications, reduce application downtime by as much as 50 percent, and develop new security solutions three times faster than before.

Betacom

"Oracle Management Cloud provides a holistic view not only for today's needs but also prepares us for the future in terms of understanding health status of a core infrastructure. Oracle Management Cloud played an important role by reducing drastically time required to run complex testing procedures, which we developed for our customer, one of the largest energy providers in Poland."

Bartlomiej Antczak, Chief Executive Officer, Betacom



Your Automated Future

Artificial intelligence (AI) technology is fundamentally altering enterprise computing by changing how organizations receive, manage, and secure business data. By 2020, Oracle predicts that 90 percent of all applications and services will incorporate AI at some level—and that more than half of all enterprise data will be managed autonomously.

Intelligence at Every Layer

Oracle's complete, integrated cloud platform includes intelligent solutions that span the SaaS, PaaS, and IaaS layers. For example, Oracle embeds intelligence into all of its apps. Oracle also extends intelligence into the platform, making it available for any developer to build upon.

The goal is to make cloud technologies simpler to access, easier to create, and more efficient to secure, manage, and run—so you can achieve real business outcomes.

Bring Your Own License

Oracle recently introduced two new programs to make it easier to buy and consume cloud services, helping you get more value from your hardware and software investments.

- **Oracle Universal Credit Pricing** enables you to access current and future Oracle Cloud Platform and Oracle Cloud Infrastructure services under a single umbrella contract.
- **Oracle's Bring Your Own License** program enables you to apply your on-premises software licenses to equivalent Oracle services in the cloud.

These popular programs alleviate cloud adoption challenges by simplifying the way your organization purchases and consumes cloud services.

Cloud **Essentials**

Learn more at oracle.com/security and Oracle Autonomous Database, or visit cloud.oracle.com/tryit to try Oracle Cloud today