

A black and white photograph of a modern office interior. A man in a white t-shirt and a dark cardigan stands on the right, gesturing towards a large monitor displaying a line graph. Three people are seated at a long table in the foreground, facing him. One person is wearing a VR headset. The office has large windows and a clean, minimalist design.

Machine learning-based
adaptive intelligence:

The future of cybersecurity



Executive summary

Most companies are adopting cloud technologies to accommodate digital business opportunities. Everybody loves the convenience—cloud services are easy to provision, deploy, and consume right away. However, security threats are not canceled by cloud adoption, and the scale of services across cloud and on-premises environments requires a new approach to cyber defense. Forward-looking companies are moving from manual security strategies to intelligent security operations centers (SOCs) that can forecast, detect, prevent, and respond to threats automatically, as well as correlate and distill vast amounts of event data into actionable intelligence.

As Oracle CTO and Chairman Larry Ellison explained during his keynote speech at Oracle OpenWorld 2017, “The way to secure our data, the way to prevent data theft, is more automation. And we need a cyber defense system that automatically detects vulnerabilities and attacks. Fix the vulnerability before an attack. And then, if there is an attack, detect the attack and shut it down.” He also said, “we need new systems. It can’t be our people versus their computers. We’re going to lose that war. It’s got to be our computers versus their computers. And make no mistake: It’s a war.”

How do SOC managers compensate for the loss of control over users, devices, and applications? How do they trust the external users—along with roving employees—that need access to their systems? According to a 2016 Ponemon Cost of Data Breach Study, the average cost of a breach at large enterprises is \$4 million, and takes 99 days to detect. 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.

To secure enterprise IT assets and protect against increasingly sophisticated attacks, forward-looking organizations are 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.

Security Operations Center managers are augmenting passive, static security strategies with more advanced and proactive security scenarios that are continuous, adaptive, real-time, and intelligent.

Mitigating sophisticated, automated threats

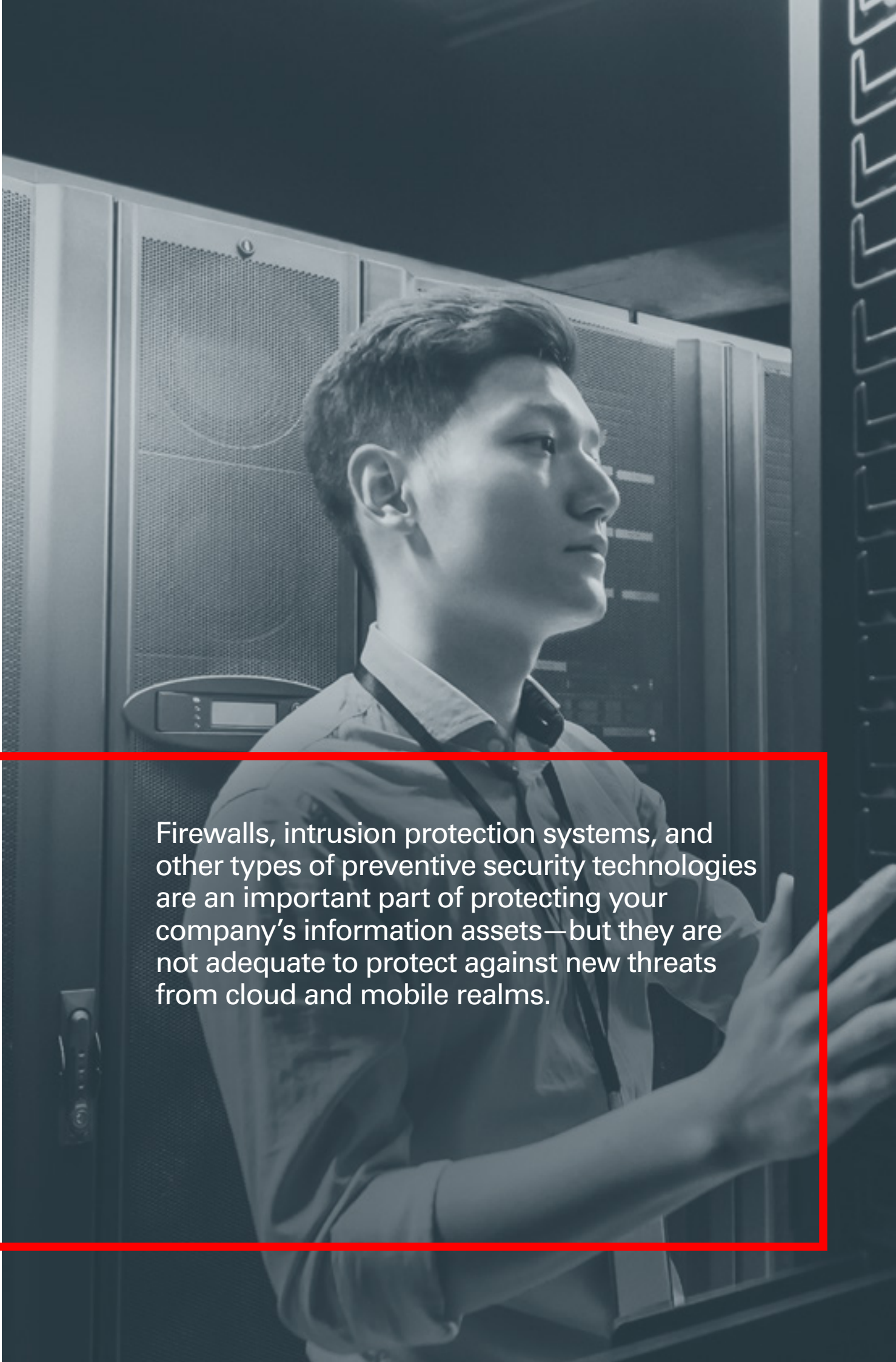
The security landscape is evolving more quickly than ever before. The network perimeter has dissolved even as the number of devices, services, and people allowed to access applications and data has increased. Automated threats—where it's not a human being sitting behind a console trying to compromise your IT environment, but rather an automated program running scripts in an attempt to infiltrate your systems—have become ordinary. Established security controls are in place but the number of security alerts coming from traditional security systems is exploding. In many cases, cybercriminals hide in the noise. Security operations centers are bombarded with millions of alerts; it is not humanely possible to keep pace without new paradigms to triage, automate, and respond to them all.

Moreover, most traditional security tools have not been designed for cloud environments and the unique challenges that cloud adoption presents such as verifying security policies and establishing visibility into infrastructure security. Decisions about who to admit and what resources to authorize must be made from moment-to-moment, based on the circumstances, or context, of each request. The spectrum of trust is no longer clearly defined. Security professionals must verify the identity of each user or application, consider which resources they wish to access, and pay attention to any sensitivities within the data or content in question.

Granting access to IT resources is rarely a black and white decision. Security teams must assess risk continuously to discern between friend and foe. Machine Learning and cloud-based analytics tools can automatically detect anomalies in user behavior, as well as intercept rogue applications that bypass traditional perimeter security systems. They augment rules-based security systems by scanning the data that these systems miss. This type of automation is essential to security operations centers because it enables rapid detection and response.

In order to dynamically establish trust and identify potential risks, security operations teams must be able to make sense of alerts regarding a huge variety of systems, applications, and data sets—everything from system and application logs, user session activity, and how sensitive IT resources are being accessed, to how security configurations are being changed. All systems and devices should be considered potentially compromised at all times, and all user behaviors continually assessed for malicious, negligent, or harmful activities—inadvertent or otherwise.

A comprehensive security portfolio should be based on a zero-trust model, which means that there is no implicit trust for any user, device, or application, and any form of trust must be established and built into an entitlement model or policy. Once authenticated, users should be allowed just enough rights and permissions to complete specific actions. To do this consistently, security professionals need contextual awareness, actionable intelligence, and a more complete assessment of the “gray areas” where so much of today's network traffic occurs. The same rigorous approach must be applied to cloud, on-premises, and hosted environments.

A man in a light-colored shirt and a lanyard is looking intently at a large screen in a server room. The room is filled with tall server racks. A red rectangular box is overlaid on the right side of the image, containing white text.

Firewalls, intrusion protection systems, and other types of preventive security technologies are an important part of protecting your company's information assets—but they are not adequate to protect against new threats from cloud and mobile realms.

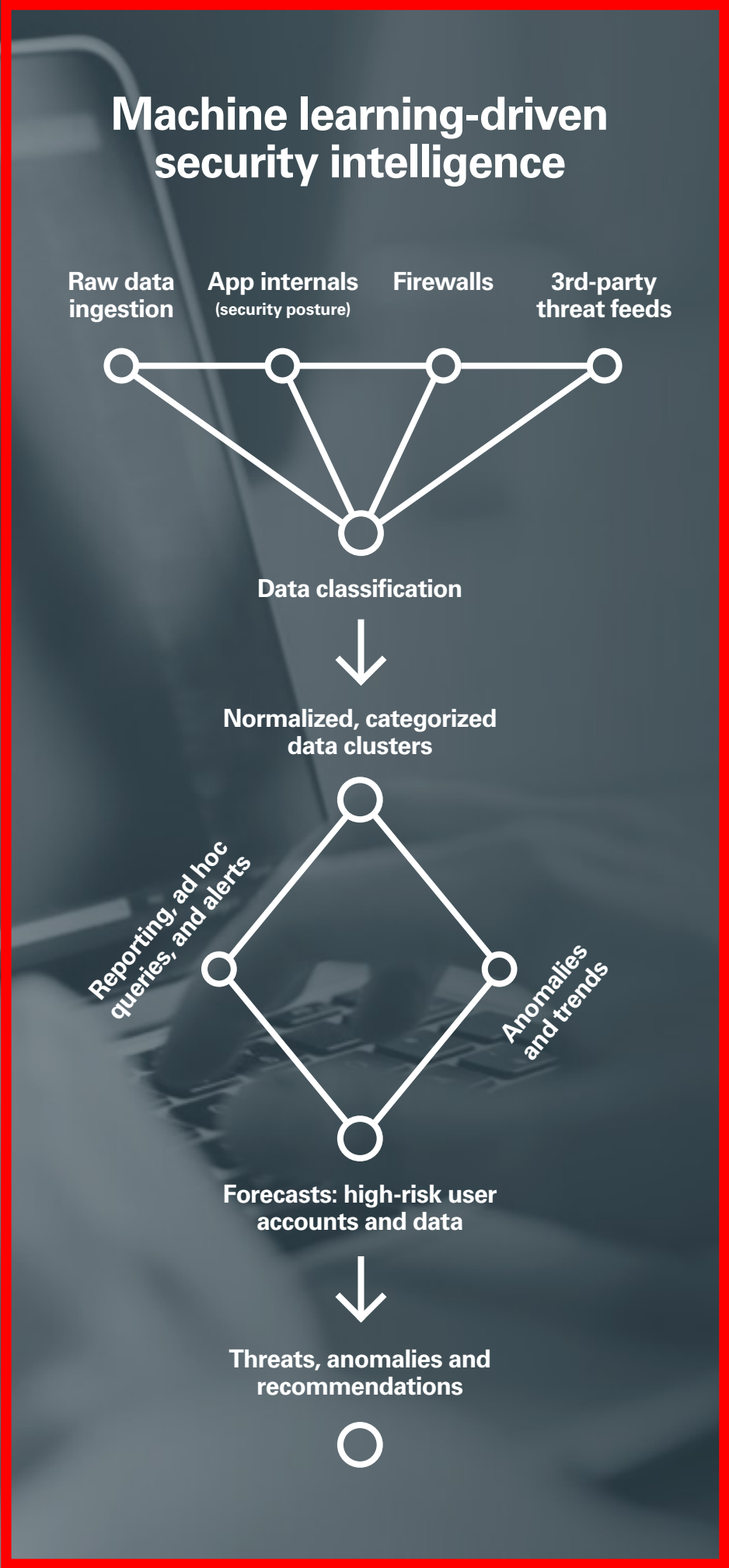
Detect quickly, remediate faster

Security operations boil down to two fundamental metrics: how quickly can you detect a breach, and how quickly can you respond to a known attack—two essential metrics known as mean time to detect (MTTD) and mean time to respond (MTTR).

Traditional security tools utilize known threat signatures and threat feeds supplied by trusted partners. This is not sufficient today as enterprise perimeters are dissolving and the first sign of a new and unknown threat may get recorded in an application log or by a user session monitoring tool. To make the most of the power of AI and machine learning, new solutions are incorporating systems management feeds such as log files, business transactions, application configurations, role/privilege assignments, and other sources unknown to the traditional security tool. AI and machine learning technologies can help you correlate events and apply heuristics to detect patterns, trends, and anomalies in the data, including detecting new alerts, adding context to those alerts, and responding quickly to address and resolve incidents. An automated cloud security solution can continuously evaluate millions of patterns and uncover anomalies and suspicious activity.

Machine learning algorithms scale well to accommodate large volumes of data when deployed in the cloud. Due to the massive amount of data involved, on-premises solutions quickly turn into large infrastructures requiring constant expansion to address compute and storage needs. An AI algorithm processes the data to identify patterns, create audit reports, and detect security risk indicators based on pre-defined threat models, baseline risk indicators, abnormal events, and suspicious user activity.

In the remainder of this paper, we'll examine how AI technology and machine learning technology can streamline fundamental activities like these in your network and security operations center.



Continuous detection

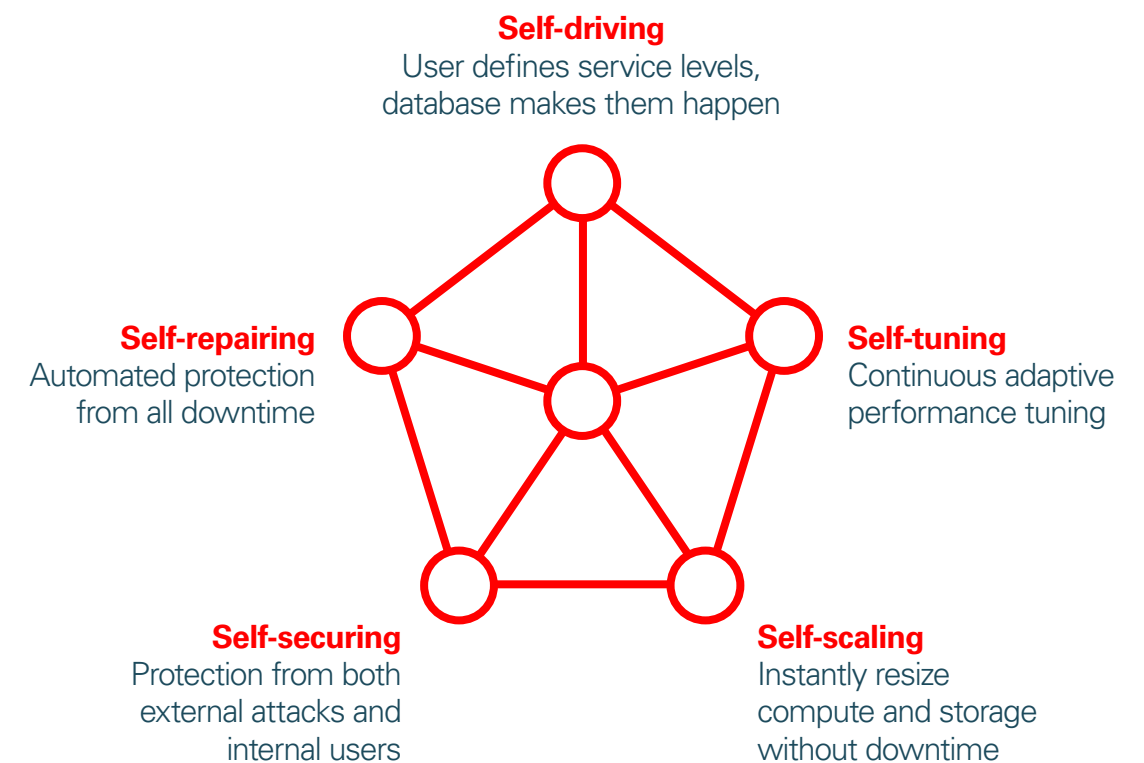
Today's diverse computing environments demand an intelligent security framework that can continuously monitor potential threats and challenge suspicious behavior. The goal is to get rid of false positives, minimize the minutiae within millions of alerts, and allow the machines to handle the simple stuff—like stepping up authentication when warranted to automatically prevent access by unauthorized users.

Oracle has a suite of cloud-based services that brings greater visibility, intelligence, and automation to cybersecurity activities. All of Oracle's security services are built on Oracle Management Cloud (OMC), an integrated set of monitoring, management, and analytics services that leverage machine learning and big data technologies against a broad operational data set. For example, Oracle Configuration and Compliance Cloud Service enables IT and business compliance personnel to assess, score, and remediate violations using industry-standard benchmarks in addition to user-defined rules. Oracle Security Monitoring and Analytics (SMA) Cloud Service enables rapid detection, investigation, and remediation of security threats and correlates the results with the privileges assigned in your identity and access management (IAM) platform or Active Directory.

Oracle Orchestration Cloud Service allows security administrators to automatically respond to issues, alerts, and events, and to set up custom rules with their favorite scripting languages and configuration software.

When Oracle's cloud-based cybersecurity applications alert the database of vulnerabilities, the database can patch itself on the fly. It can also detect anomalous SQL queries by parsing SQL statements to establish whitelist baselines by user, group, database, and application. It evaluates new SQL queries against this baseline to spot potential threats, raise threat scores, and take action to protect sensitive data. On the back-end, Oracle Autonomous Database Cloud Service simplifies database administration and tuning tasks, including automatically maintaining security configurations.

The world's first autonomous database



Less labor, lower cost, fewer errors, more secure, more reliable

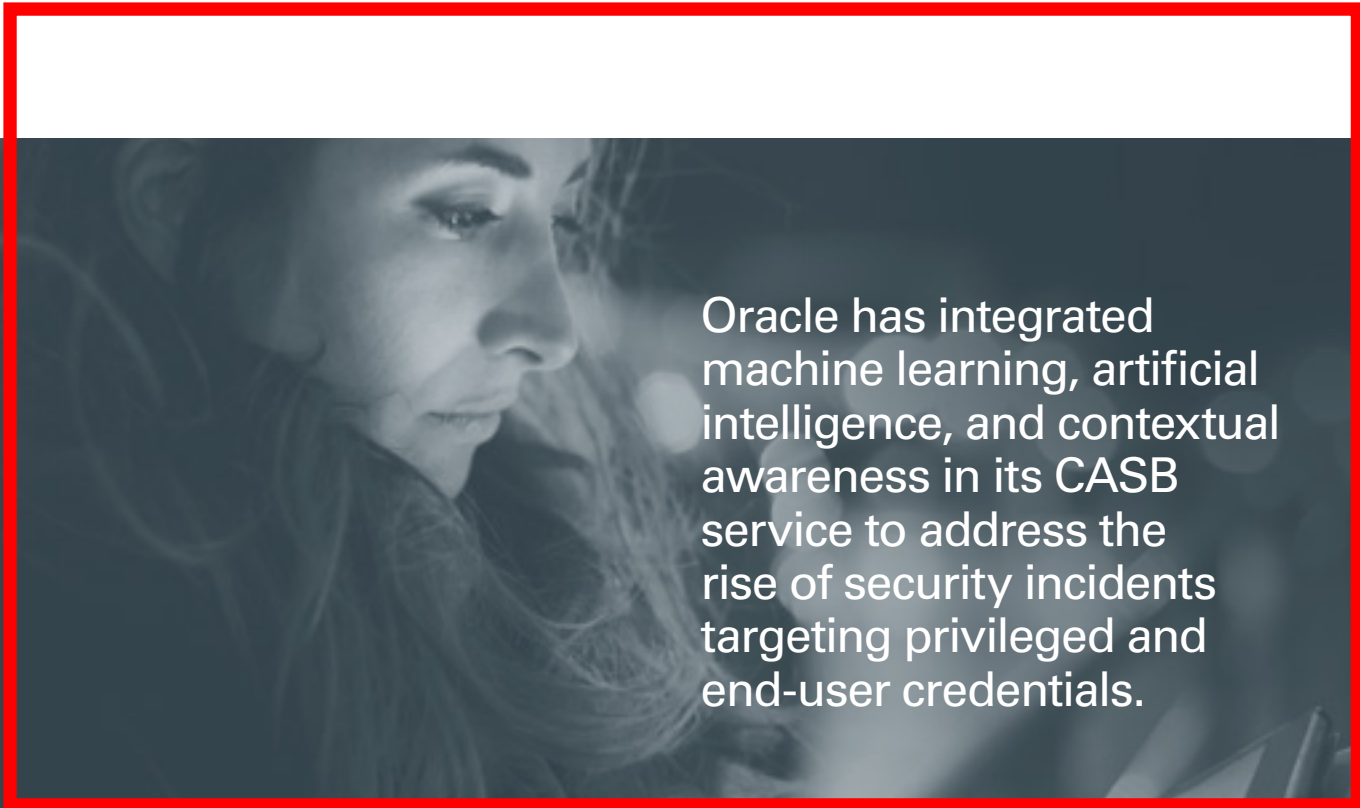
Adaptive responses

An advanced security system can adapt to changing conditions, driven by machine learning technology that automatically detects and fixes problems without human agents—a capability known as adaptive response. This type of automation is progressively more important in today’s hybrid cloud environments. For example, you may have little visibility into how people use their mobile devices to download apps and data via the corporate network. Many employees use Box, Dropbox, Evernote, Office 365, and other cloud apps for personal and professional tasks, and they may use personal Gmail accounts to send and receive corporate data. It’s convenient for users, but without strict policies, the IT department can easily lose control of how these applications are used, as well as how the associated data is managed and stored.

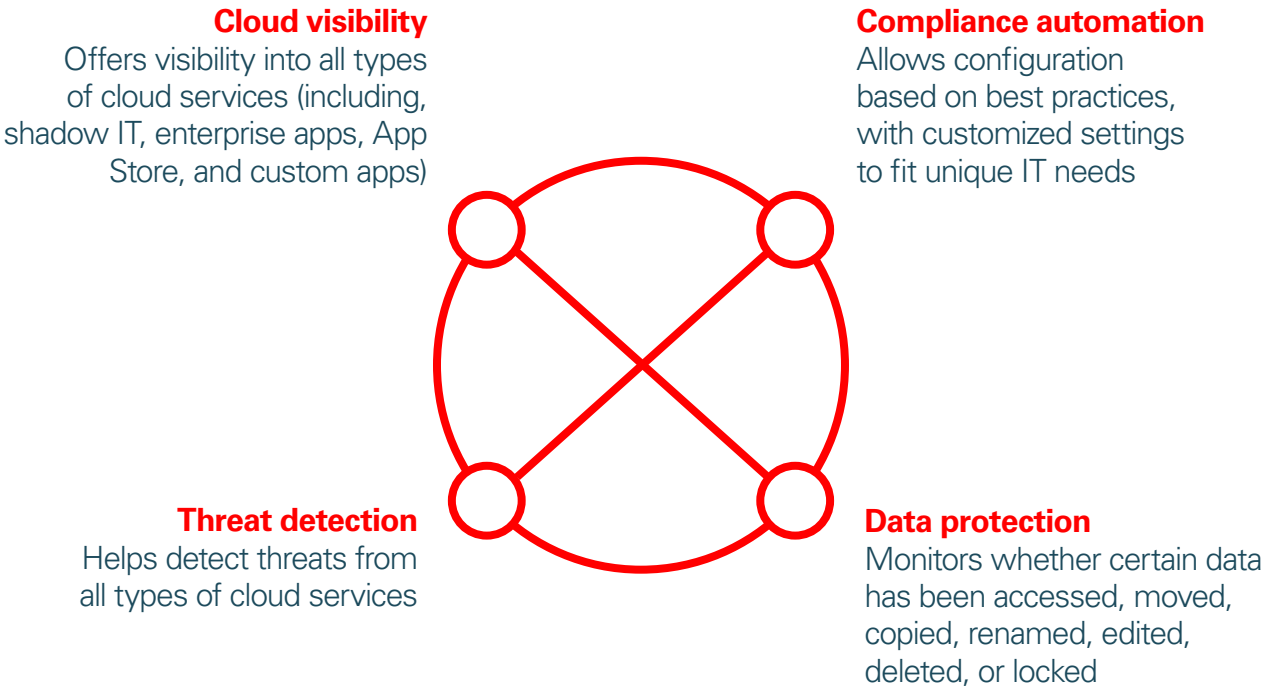
Large businesses typically have hundreds of cloud services. Top-tier cloud providers do a good job of securing their infrastructure, but customers are responsible for protecting their own data in the cloud. Data breaches and attacks can occur when companies have insufficient identity and access management systems. In addition, application programming interfaces (APIs), and user interfaces have IP addresses that can be accessed from outside of trusted organizational boundaries. Because they are exposed, these assets can be the targets of attacks via the internet.

A Cloud Access Security Broker (CASB) can assist with cloud management by brokering exchanges between cloud users and cloud providers, as well as by consolidating security policy enforcement activities. For example, Oracle CASB Cloud Service protects your critical data by combining visibility, threat detection, compliance management, and automated incident response for cloud services into a single platform. Situated between your on-premises infrastructure and a cloud provider’s infrastructure,

it acts as a gatekeeper, allowing you to extend your in-house security policies beyond your own infrastructure. Users can securely access cloud services, whether from a corporate PC behind the firewall, or mobile devices from a remote coffee shop. Your security team gains visibility into shadow IT processes, and can more reliably secure sanctioned cloud services, including Amazon Web Services, Google Apps, and Salesforce.



Oracle has integrated machine learning, artificial intelligence, and contextual awareness in its CASB service to address the rise of security incidents targeting privileged and end-user credentials.



Adaptive responses

continued

ABI Research forecasts that machine learning in cybersecurity will boost big data, intelligence, and analytics spending to \$96 billion by 2021.*

CASBs depend on user entity behavior analytics (UEBA) to establish unique historical baselines for each user and cloud service. They continuously compare unusual activity against these expected baselines to identify unusual, suspicious, or potentially risky behavior. Once the CASB detects a deviation, it orchestrates an intelligent response, perhaps integrating with a ticketing and incident management system to compare the incident to similar ones, and ultimately suggesting targeted remediation by a human agent.

Bolstered by machine learning algorithms, Oracle CASB learns what constitutes typical behavior for each application. It defines a baseline for typical user behavior, against which deviations can be measured. If a user exhibits behavior outside of those well-established expectations, that behavior can be flagged as an anomaly. For example, if an employee has family members in the Ukraine, and occasionally works from that location, logging in from there would not raise a red flag. However, if an employee who never travels to the Ukraine suddenly logs in from that location, the system could leverage the Adaptive Access engine in CASB and force Multi-Factor Authentication (MFA) by initiating a two-factor identity procedure to verify the user's identity.

In this way, the security system gets smarter over time. The more data it studies, the more users it gets to know, the more applications that come under its purview, the better it can understand rogue or suspicious behavior when it occurs. For example, the CASB might monitor the applications users typically use, the locations they log in from, how they access these cloud services, and the time of day when they are most often online. If it suspects an account may have been hijacked, it can require a password reset or two-factor authentication procedure.

Risk analysis through identity and context

Businesses that have embraced the cloud paradigm are less likely to fall out of compliance with industry and government regulations, guidelines, and standards. However, because of the new challenges and risks that come with the cloud model, it's more critical than ever to be proactive about cybersecurity. You must institute management processes to assess the state of compliance and evaluate the risks and potential costs of non-compliance. An identity-based SOC uses machine learning to combat fraud across cloud and on-premises applications by analyzing each login attempt in conjunction with data on location, device, and time of day. These intelligent applications are not only better at detecting and preventing threats, but they also automate post-event, investigation, and response activities.

Oracle is the first vendor to build this level of identity awareness into a native cloud service that integrates with the rest of the security fabric, offering complete security coverage for hybrid environments. Oracle Identity Cloud Service (IDCS) resides at the center of the security framework to improve compliance, risk management, database security, and application security. It is designed to simplify the deployment of applications such as Office 365, Salesforce, and Oracle Cloud Applications, as well as to bridge the identity gap with on-premises identity management systems and directories, such as Oracle Identity and Access Management and Microsoft Active Directory.

Oracle Identity SOC is the industry's first identity-centric framework for security operations centers.

Oracle IDCS provides administration capabilities such as user/group and app administration, access management capabilities such as single sign on, strong authentication, and adaptive risk-based policies. It works in conjunction with Oracle Security Monitoring and Analytics Cloud Service to detect, investigate, and remediate a broad range of security threats across on-premises and cloud environments. Oracle's modern identity-based SOC incorporates threat intelligence from open source and commercial feeds, IP white/blacklists, device reputation, known vulnerability databases, geo-location, and more. It facilitates rapid detection, investigation, and remediation of a broad range of security threats based on algorithms that can identify patterns in the data. As the system gets smarter, it can even make predictions about the likelihood of future breaches based on historical activity.

Trust-based review

It is relatively easy for a hacker to steal a sanctioned user’s credentials and then penetrate the network under the guise of an authorized worker. This may lead to suspicious or anomalous activity—different from how that user normally behaves, or how his or her peers normally behave. A CASB system will issue alerts and step up the security constraints—perhaps requiring two-factor authentication to access a particular application. In addition, a centralized identity framework will enable security personnel to audit which users can access which resources at which times. This allows them to identify situations in which users no longer need access, and to set outbound credentials for hosted applications in the cloud and inbound credentials from third parties.

Oracle uses machine learning technology to cluster users based on common aggregate behavior, such as where they come from, the internal assets they access, the cloud services they access, and the time of day they operate. This makes it easy to spot anomalous behavior, such as if an HR professional suddenly starts behaving like a finance exec—indicating a potential hijacked account or insider threat.

Automating this process is essential, given the sheer volume of alerts and incidents. For example, upon arriving at work in the morning, a SOC professional might receive a summary report that says there were 10,000 alerts over the weekend. The security framework automatically addressed 98 percent of them, the audit report explains—issued alerts, opened support tickets, and escalated potentially threatening issues—so that only 200 alerts need to be reviewed manually.

Architectural integration

As we’ve seen, a complete security architecture involves the integration of people, processes, and technology via a cloud-based, identity-centric approach. To tie it all together, you need a comprehensive management framework. Oracle Management Cloud includes a machine-learning engine that correlates the data and enables single-pane-of-glass management. It includes preprogrammed AI models, so you don’t need a data scientist on staff to program the system or keep it up to date. The machine learning algorithms add intelligence to DevOps and SOC processes. For example, one security module handles compliance and configuration management. Other modules handle security information and event management (SIEM) and event aggregation via a cloud access security broker (CASB).

Oracle Management Cloud blends these individual capabilities into a broad security fabric. It’s ideal for nimble DevOps teams that are adopting modern IT practices, since it correlates pertinent events from the network, applications, and users interacting with your systems.

Oracle has embedded machine-learning technology at the heart of Oracle Management Cloud to help you address security threats across on-premises and cloud environments. This management foundation promises a more productive integration of people, process, and technology.



Automated cyber defense: your tomorrow, today

IT professionals are losing control as legacy workloads are disassociated from the well-protected, carefully circumscribed physical infrastructure and moved into new domains, where the infrastructure, applications, and data are often managed by third-party providers.

Third-party cloud providers have limited or no oversight/visibility into the customers and their data owner. That's why forward-looking security directors are installing automated, intelligent, context-aware security solutions that give them broad control over the security risks to which their organizations are exposed. Rather than passively monitoring the network, they are creating proactive defenses that protect users, applications, content, and data. Most importantly, they are figuring out how to apply consistent security controls across cloud and on-premises environments.

Not properly securing against internal and external threats can have a negative impact on your bottom line, your brand, and your market valuation. Cloud and machine learning technologies can improve your security readiness and give you a more complete picture of your overall IT environment.

Oracle enables your team to establish a continuous security posture that can evaluate event data in real time. This adaptable system can learn new things—including where employees move, what devices they use, and how their personal computing environments change day to day.

Digital businesses can no longer survive without a high level of security intelligence and awareness. Manual and rule-based technologies are no longer adequate for today's cybersecurity challenges. You need automated, contextual, machine learning technology to detect and respond to known and unknown threats. Oracle's integrated security portfolio spans on-premises and cloud environments. It combines contextual identity-as-a-service, a cloud access security broker, security monitoring and analytics, and configuration and compliance capabilities—all from one vendor—which makes it easy to automate your cyber defense and win the cyber war.

Today's advanced threats demand machine learning and cloud—the new differentiators in the security landscape.

To learn more please click through to the following resources:

[Modernize Your Security Operations Center](#)

[Why You Want to Modernize Your Systems Management and Move it to the Cloud](#)

Machine learning-based adaptive intelligence:
The future of cybersecurity

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0118.

