Security Architecture for the New Digital Experience

Security Architecture for the New Digital Experience

Designing Security Inside Out

SECURITY INSIDE OUT

Table of Contents

CHAPTER 1

Rise of the Security Architect

Today's enterprise architects find themselves confronting fundamental questions where business and technology intersect. How does the company plan to grow? What technology platforms will it use to achieve that growth? What security risks will the company face and how can security architects help mitigate those risks?

- → How does the company plan to grow?
- → What technology platforms will it use to achieve that growth?
- → What security risks will the company face?
- → How can security architects help mitigate those risks?

Providing knowledgeable answers to questions about security necessitates interacting not only with other stakeholders in IT, but also with experts in finance, HR, marketing, sales, product development, and risk and compliance. Security architects must address information security standards as well as stay ahead of an ever-changing array of industry regulations and compliance guidelines.

Enterprise architecture is an IT discipline that helps organizations simplify system design, align technical requirements with business requirements, and manage the lifecycle of complex systems. Enterprise information security architecture (EISA) has emerged out of enterprise architecture to manage the security fragmentation of distributed systems, collect requirements from business stakeholders, and address the growing security compliance and internal governance requirements for information security.

According to the Bureau of Labor Statistics, the demand for security architects is expected to grow 20 percent annually through 2018, driven by an epidemic of data breaches, rising regulatory challenges, and relentless modernization efforts in IT departments.

DEMAND FOR
SECURITY
ARCHITECTS

→

20%
growth annually
through 2018

As Oracle Chief Security Officer Mary Ann Davidson points out, security challenges continue to escalate, yet time, money, and resources are always constrained—particularly the availability of skilled security people. There are serious consequences for failing to adequately protect customer and partner data—everything from hefty fines to loss of strategic business relationships.

Video: With security spending at an all-time high, many CSOs are rethinking their priorities and focusing on risk.

Watch the Video (18:29)

CHAPTER 2

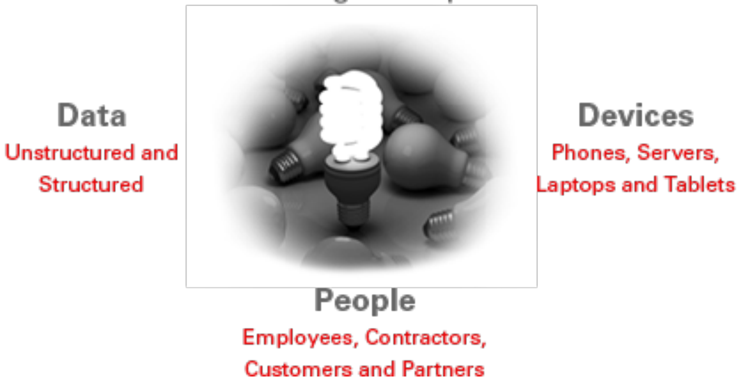
Transformation of the Perimeter

Before 1995 most companies ran their information systems on networks that were largely private. Only a handful of people had the capability to cross the network boundary, which kept information systems inside the organizations secure from anyone outside the company. The emphasis was on protecting the network perimeter, and IT organizations continue to spend more than 67 percent of their security dollars on network security. But today the new digital economy is dramatically increasing the level of value-added participation, requiring employees, customers, and partners to cross network boundaries every minute. For example, healthcare organizations need to enable doctors and patients to collaborate online. Manufacturing organizations give suppliers access to their inventory information and MRP systems. Each search on Google can potentially hit a page that downloads malicious malware. Every e-mail message offers the potential of a new phishing attack.

The people accessing these networks are not only trusted employees, but also a changing cast of contractors, customers, and partners. The data being accessed can include structured information from corporate databases as well as unstructured data such as documents, e-mail, and audio files. And users are continually on the move—as is the information itself. The new points of control entail verifying user identities and permission to access information systems, securing the devices connecting to the network, and protecting data where it resides.

THE NEW PERIMETER

The network is no longer the point of control


Data
Unstructured and Structured
Devices
Phones, Servers, Laptops and Tablets
People
Employees, Contractors, Customers and Partners

To further blur the perimeter, cloud-computing models often put data and applications outside of traditional enterprise boundaries, even as mobile devices represent a continually expanding perimeter. There is growing pressure to set up access portals for partners and customers, as well as to facilitate employee collaboration on mobile and social networks. Sensitive data that was secured behind a robust enterprise firewall is now accessible via low-cost smart phones.

Security architects are faced with a new set of questions: How do you protect applications, devices, and data in a world without a defined network perimeter? How can you ensure that corporate data is just as secure on a $100 smart phone as it is on a $100,000 server in an enterprise data center? How can you provide a consistent experience for users while guaranteeing protection and privacy for the organization's trusted information assets?

The most progressive IT architectures extend security controls across all information systems. Security architects utilize a "trust but verify" approach to both enable productivity and address security governance requirements. The objective is to establish one consistent security framework underlying all information systems. Because users and sensitive data are part of every transaction, identity management and database security are the common denominators of addressing most security requirements.

AN ORACLE WHITE PAPER | APRIL 2014

The New Perimeter: Keeping Corporate Data Secure in the Mobility Era

White Paper: "Identity is a powerful tool. It can be applied to people, devices, and data and therefore plays a vital role in securing the new perimeter."

Read the White Paper

> "For security professionals, IoT stands for an explosion of identities."
>
> Indus Khaitan, product manager, Oracle Mobile Security

Watch the Webcast

FOUR STEPS TO SECURING THE NEW PERIMETER

1. *Think inside out.* The threats are outside but the risks are largely inside.
2. *Develop a "defense-in-depth" strategy.* Create a framework of overlapping controls to address vulnerabilities.
3. *Simplify the user experience.* When security becomes a productivity barrier, controls get remanded.
4. *Design for compliance.* Security is as important to shareholder value as good accounting. Regulatory controls are on the rise.

> "Businesses now invest in security rather than spend on it. Security architects need to design security systems that complement business policies and processes."
>
> Chris Gavin, vice president, Information Security, Oracle

CHAPTER 3

The Great Re-Architecture

For many industries the fundamental organizational structure changed relatively little in the past 20 years. City and state governments are organized much as they were in the 1940s. Manufacturing organizations continue to achieve economies of scale through greater automation of the assembly line. Healthcare providers rely on IT systems to simplify back-office and front-office tasks, and thereby improve patient care. But now all of this is changing dramatically. Governments are delivering more types of citizen services online. Manufacturing companies are managing each component's lifecycle beyond the assembly line and providing manufacturing services on-line across an entire product lifecycle. Healthcare providers are orchestrating care among remote providers and sharing medical records for patients who may never physically visit a hospital.

Many of these services are being performed via software solutions that are architected in the cloud rather than on-premises. They require technologies that can support the real-time exchange of accurate information. Organizations rely on identity management technology to facilitate dynamic trust relationships and support regulatory compliance requirements.

Security architecture has moved to the forefront of these transformative initiatives to enable online interactions and secure the user experience.

Yarra Valley Water

One such example of a public utilities organization transforming its services to keep up with the changing technical landscape, Yarra Valley Water (YVW) in Australia used Oracle Identity and Access Management to implement an easy-access portal that supports self-registration, self-provisioning, access, and authorization for partners and citizens. The secure Oracle platform utilizes a federated security model to handle one-off requests from citizens as well as ongoing interactions with partners, with straight-through processing capabilities to streamline the workflow. An embedded compliance and security framework handles complex attestation controls and processes.

Video: YVW uses Oracle Identity and Access Management.

Watch the Video (1:52)

Beachbody is prime example of IT transformation in retail. The company has embraced a multi-channel customer engagement strategy that includes infomercials in which viewers can respond to special offers and promotions, a website for e-commerce purchases, a multilevel marketing company that engages about 100,000 coach affiliates, and a certification business. These channels focus on different types of consumers, each requiring unique offers and promotions. To enforce consistency, Beachbody adopted Oracle Identity Management to authenticate users and track their activities across different channels and personas. The operational scale across channels improves the volume of participation from coaches, consumers, members and partners. All of this means more affluence for Beachbody. Just as members drive the value of the business, reducing the friction of participation increases business velocity.

Video: Beachbody CTO Arnaud Robert explains how Oracle Identity Management allows his company to better serve customers through targeted campaigns and mobile applications.

Watch the Video (2:37)

> "Previously our disparate systems didn't allow us to maximize conversions or revenue or the long-term value of each customer."
>
> Arnaud Robert, CTO, Beachbody

Risk-Aware Architectures

Security architects are tasked with developing "risk-aware" architectures that factor in legal liabilities, the privacy of partner and customer data, and regulatory requirements. These security policies ensure that the organization is ready for internal and external audits. Oracle Corporate Security Architect Steve Deitrick lauds this approach, advising security architects to become fluent in both the language of technology and the business with which they are charged with supporting. "In today's strict regulatory environment it is strongly advised for security architects to have solid working relationships with their legal departments," he notes. "Successful security architects manage their discipline in three directions: upward for executive sponsorship, horizontally for effective strategy establishment, and downward for successful strategy execution and results. Moving beyond IT raises their value as key players in risk prevention."

Sabre Holdings

The airline industry is poised for a dramatic transformation in the next decade and anticipates growth in the number of both passengers and new services. In order to simplify its IT environment and modernize travel applications to meet these new requirements, Sabre is securing its applications by abstracting security policies in the database.

Video: Sabre Holdings uses Oracle’s data redaction solution to mask personally identifiable information in thousands of travel databases.

Watch the Video (1:14)

CHAPTER 4

Architecting Security for Mobile

"Next-generation security solutions are emerging that enable companies to integrate rigorous, identity-based mobile application management and containerization capabilities to control and protect corporate data while ensuring that employees have private access to the personal apps and services they enjoy."[1]

By 2020, 80 percent of access to the enterprise will be via mobile devices and other non-PC devices, up from 5 percent today. In addition, external providers will authenticate 60 percent of all users connecting with enterprises.[2] Meanwhile, the Internet of Things (IoT) is redefining the concept of identity to include what people own, share, and use. According to research conducted by Cisco Systems, by 2020 there will be more than 50 billion IP-enabled devices in use around the world.

[1] "The New Perimeter: Keeping Corporate Data Secure in the Mobility Era," a white paper by Oracle and IEEE, April 2014.

[2] IAM keynote presentation, "The Future of Managing Identity," (Gartner 2013).

REDEFINING IDENTITY AND TRUST

PERSONAL AND SOCIAL

More Social-Sign-On

Types of Interaction

TRUST AND INTROSPECTION

Devices Trust People

People Trust Devices

MASSIVE SCALE

High Scale

Reliable Interaction

Internet of Things

When it comes to securing the network, IoT and mobile technology are on a collision course. Nearly 90 percent of employees are using smart phones at work, and half of them are doing so without the permission of their employers.[3] Most of these employees neglect to follow simple precautions such as reading the terms and conditions before downloading an app, manually adjusting security settings, or verifying that the applications are trustworthy—not to mention the ever-present threat of malware targeting these mobile devices and spyware capable of stealing personal, financial, and work information.

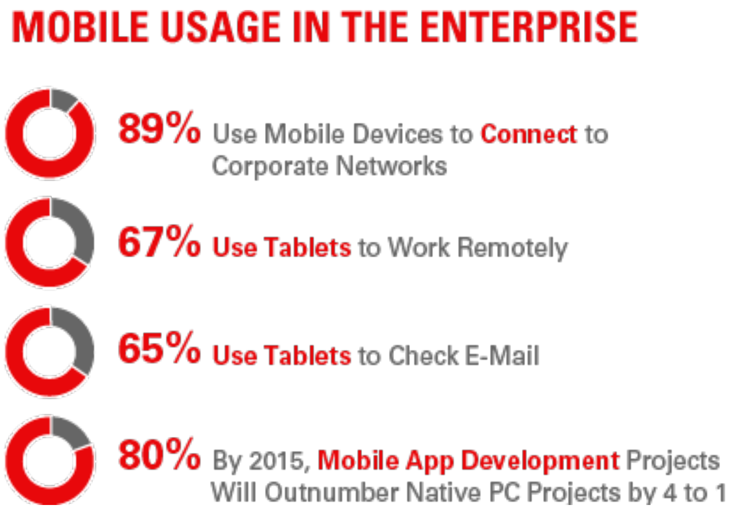
According to Vadim Lander, chief identity architect at Oracle, there are three types of security concerns associated with the Internet of Things:

- **Device Identity**
- **Application Identity**
- **User Identity**

"Security architects should look for solutions that include contextual, real-time, policy-based controls at the service/application layer to mitigate threats," Lander notes. "Adaptive authentication and authorization are two techniques for setting up policy-based security controls for managing who has access to what under what conditions."

Mobile Access

Mobile computing is reshaping the digital economy and changing the dynamics of corporate computing. According to research conducted by Forbes, 89 percent of today's mobile devices are already connected to corporate networks, 67 percent of workers use tablets to connect remotely to corporate IT resources, and mobile development projects will soon outnumber native PC projects four to one.



Read the White Paper: Oracle Mobile Security Suite: Secure Adoption of BYOD

[3] "Companies Slow to React to Mobile Security Threat," CSO Online, Antone Gonsalves, May 2012.

In addition, more than three-fourths of all enterprise data breaches are the result of weak or stolen credentials, according to the 2013 Verizon Data Breach Investigations Report. Many of the mobile devices that employees use at work include personal content. Family members often share these devices. The employees who use them also need corporate connectivity, which complicates security and privacy issues. Security architects must now focus on how to secure corporate data while maintaining the privacy of personal data.

Demo: Marc Boroditsky, Oracle vice president of product management, and Andy Smith, Oracle senior director of product management, demonstrate Oracle Mobile Security Suite.

Watch the Security Demo (9:19)

According to Oracle Vice President of Product Development Amit Jasuja, enterprise IT departments face three important bring-your-own-device (BYOD) issues:

- Figuring out how to develop mobile apps that support multiple platforms, from Apple iOS and Google Android to new versions of Microsoft Windows
- Creating a mobile architecture to expose back-end applications in a secure and consistent way
- Upholding corporate security policies across mobile, cloud, and enterprise application scenarios

Interview: Amit Jasuja chats with Oracle CIO Mark Sunday about the state of mobile security in 2014.

Read the Executive Interview

CHAPTER 5

Cloud Security

Cloud architecture presents significant challenges for security architects. Third-party vendors typically handle user administration, data management, and network access. According to Graham Palmer, Oracle's director of information security, these cloud solutions must be carefully controlled to manage costs and risks, yet 33 percent of organizations don't evaluate security when selecting cloud applications. "Enterprise information should not be trusted to companies with no track record, or that lack an auditable security framework based on international security standards such as ISO27001 and SAS-70," Palmer says. "Customers should look at security as a prime driver in vendor selection."

Oracle Chief Identity Architect Vadim Lander believes that cloud service providers should demonstrate that they are in compliance with established audit and security procedures. Customers that contract with cloud vendors need to be able to control the identity management process for external applications and on-premises apps via single-sign-on procedures. These solutions should also make it easy to provision and deprovision users and to extend entitlement credentials from on-premises applications to cloud applications. Such controls are even more important when securing databases. According to IDC, 66 percent of today's most sensitive data resides in relational databases.

Cloud services are the backbone of T-Mobile's infrastructure. To secure 35 million subscribers in a business model in which customer data has to be processed by many applications—and corporate valuation depends on subscriber growth—T-Mobile is using transparent data encryption to secure data in a cost effective way.

Video: T-Mobile explains how it reduced exposure to risk by using Oracle Database Firewall, Oracle Advanced Security, and Oracle Data Masking Pack to secure sensitive data in both Oracle and non-Oracle databases.

Watch the Video (1:54)

Adherence to Standards

Providing consistency helps security architects gain economies of scale and simplify administration. To improve the management of hybrid cloud/on-premises environments, security architects should ensure that service providers use HTTP-friendly identity management integration patterns. Lander insists that providers use the SAML protocol as the identity federation mechanism for establishing single sign-on between corporate identity management (IDM) systems and cloud IDM systems, and use the SCIM protocol for user provisioning. Adopting these standards makes it easier for the corporate IDM system to provision and deprovision users. Security architects should also look for cloud solutions that have a mechanism for importing user identities from the corporate identity store into the cloud provider's identity infrastructure.

Video: SaskTel offers Oracle Identity Management in the cloud.

Watch the Video (2:45)

SaskTel standardized on Oracle Identity Management to consolidate its internal and external identity management systems on a single platform. The telecommunications provider can authorize and authenticate internal and external users via single-sign-on procedures as part of a cohesive cloud service.

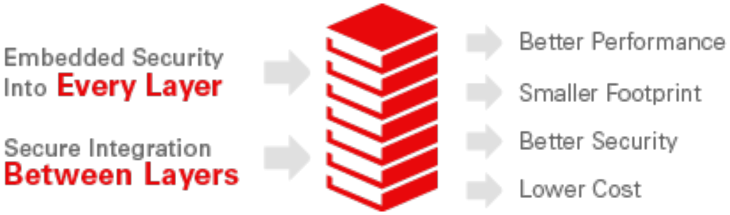
CHAPTER 6

The Oracle Security Taxonomy

Latency and consistency are two variables used to measure good security design. The objective is to reduce the latency of change and increase consistency across systems and applications. Typically these variables are inversely proportional: as the latency of change increases, the amount of consistency decreases. In a recent study by CSO Online, 44 percent of respondents blamed the fragmentation of IT systems for creating gaps in security. Attackers are taking advantage of inconsistency and weak policy controls to gain a foothold in many organizations. When users leave a company it can take months before their access rights are disabled across systems. The greatest opportunity for fraud happens during this time frame. In other cases organizations take months to apply security patches to their information systems. Hackers don't wait to exploit these known weaknesses.

Hardware
ORACLE ENGINEERS
HARDWARE AND
SOFTWARE
TO WORK TOGETHER
Software

Oracle engineers hardware and software to work together. This cohesive approach reduces the latency of change and increases consistency. By embedding security technology into every layer of the technology stack and securing the integration between layers, Oracle not only delivers better performance with a smaller footprint, it also provides better security at a lower cost.

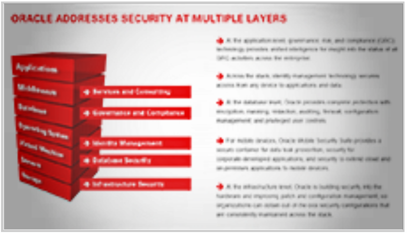


For example, at the middleware level, Oracle builds in identity management and access control technology to govern how data is used at the application tier. It also provides encryption, firewall, and masking at the database level. Oracle monitors and patches the software at the operating system and virtualization tier, and builds hardware encryption into the infrastructure. Encryption is provided across all tiers of storage, and at the application level Oracle offers complete governance and fraud prevention to detect anomalous behavior.

At the database level, Oracle's preventive controls provide encryption, redaction, and security for privileged users. To secure multiple database instances, Oracle provides discovery, data classification, and configuration scanning. Today many IT solutions are designed without security auditing in mind. Oracle Audit Vault and Database Firewall provide alerting, reporting, and conditional auditing.

By securing each layer of the stack, Oracle can ensure that one set of policies, roles, and controls are applied uniformly. In addition, Oracle's integrated family of security technologies is used to secure third-party applications and databases.

Finally, Oracle "defragments" identities across the enterprise to enforce consistency across systems. That means you can apply the same policies and constraints that protect your core internal systems to other systems, such as mobile devices and third-party applications. Oracle Identity Management Suite lets you create universal identities that transcend individual systems and devices by automatically provisioning user identities to multiple applications and tools.


ORACLE ADDRESSES SECURITY AT MULTIPLE LAYERS

- At the application level, governance, risk, and compliance (GRC) technology provides unified intelligence for insight into the status of all GRC activities across the enterprise.
- Across the stack, identity management technology secures access from any device to applications and data.
- At the database level, Oracle provides complete protection with encryption, masking, redaction, auditing, firewall, configuration management, and privileged user controls.
- For mobile devices, Oracle Mobile Security Suite provides a secure container for data leak prevention, security for corporate developed applications, and security to extend cloud and on-premises applications to mobile devices.
- At the infrastructure level, Oracle is building security into the hardware and improving patch and configuration management, so organizations can obtain out of the box security configurations that are consistently maintained across the stack.

Oracle addresses security at multiple layers.

Expand View

White Paper: "The most complete solution for managing people, data, and devices is through identity. Identity is the central component of how mobile devices access content, applications, secured communications, and more."

› Read the White Paper

Resources

The Rise of Security Architecture

- Webcast: "Securing Your Business Inside Out"

Transformation of the Perimeter

- White Paper: “Transformation of the Perimeter”
- Webcast: “Transformation of the Perimeter”
- Report: Verizon E3 Data Breach Report

The Great Re-Architecture

- Video: University of Louisville (3:13)
- Video: Beachbody (2:37)
- Video: Sabre Holdings (1:14)
- Video: Yarra Valley Water (1:52)
- White Paper: Privacy by Design

Architecting Security for The Internet of Everything and Mobile

- White Paper: Secure Adoption of BYOD
- Executive Interview: Amit Jasuja on Mobile Security
- Video: Oracle Mobile Security Suite (9:19)
- Screencast: Managing Secure Mobile Policies (27:51)

Cloud Security Architecture

- Video: UPMC Discusses Privacy / Identity / Security in Healthcare (2:58)
- Video: SaskTel Offers Oracle Identity Management in the Cloud (2:45)
- Video: T-Mobile Talks About Reducing Exposure and Risk (1:54)

The Oracle Security Taxonomy

- Website: Oracle Identity Management Solution Page
- E-Book: Oracle Identity Management E-Book
- Research Brief: Aberdeen Research: IAM Platform Approach vs Point Solutions

Security Architecture for the New Digital Experience

SECURITY INSIDE OUT