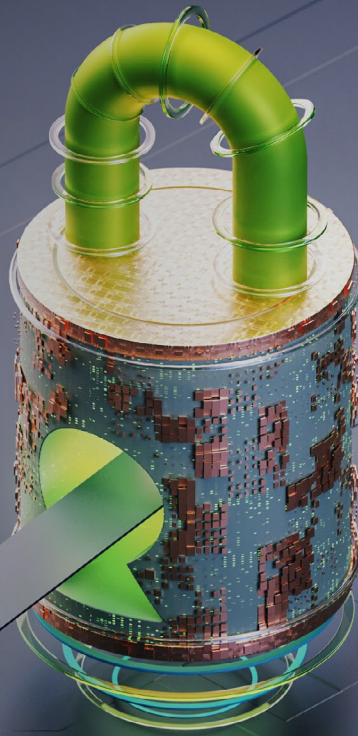


TECH TRENDS 2021

Creating an agile enterprise
built to evolve with Oracle

ZERO TRUST: NEVER TRUST, ALWAYS VERIFY



Porous perimeters and ever-expanding attack surfaces are making conventional castle-and-moat cybersecurity models irrelevant to continually evolving cyberthreats. Furthermore, greater reliance on a remote work environment, along with anticipated growth of smart devices, 5G, edge computing, and AI, is making the moat even shallower and the castle perimeter even harder to define. Enter the notion of zero trust. Based on the principle of “never trust, always verify,” zero trust is a conceptual framework that helps organizations secure the ubiquitous nature of modern enterprise environments. Although it is not new, zero trust is gaining traction in a world where there’s no longer a defined perimeter in which every user, device, and network is inherently trusted.






In zero trust architectures, every access request should be validated based on all available data points, including user identity, device, location, and other variables that provide context to each connection and allow more nuanced, risk-based decisions. Users, applications, networks, data, devices, and workloads are all treated as individual, manageable units. This allows for containment of breaches by providing access based on the principle of least privilege.

Zero trust can confer a number of benefits: it can help strengthen security posture, simplify security management, improve end-user experience, and enable modern enterprise environments. And, because it is a conceptual framework, and not a code-based solution, it can be applied to nearly every part of the Oracle stack.

Yet, adopting zero trust is a journey. It typically requires a shift in mindset driven by broader transformation efforts, along with an experienced guide who can help organizations take a holistic approach to cybersecurity in advance, rather than approaching it as an afterthought. This involves establishing strong foundational capabilities across the five fundamental pillars of users, workloads, data, networks, and devices, and supporting them further with telemetry and analytics, and automation and orchestration.

AN AGILE ENTERPRISE, BUILT WITH A ZERO TRUST FRAMEWORK

Evolving business models, shifting workforce dynamics, and accelerating technology trends are causing many organizations to begin adopting a zero trust cybersecurity posture as a means of securing a porous perimeter. Common business drivers include:

-  **Accelerated cloud migration and digitalization**
-  **Brand and reputation concerns**
-  **Supply chain risks**
-  **Workforce mobility and flexibility**
-  **Greater scale and frequency of cyberattacks**

Deloitte's zero trust framework is built on five pillars: identities, workloads, data, networks, and devices. Telemetry and analytics as well as automation and orchestration are implemented as supporting capabilities across all five pillars. Using this framework, Deloitte can help organizations to build zero trust thinking into their solutions by leveraging the security capabilities inherent in many Oracle offerings. This thinking can be applied to nearly every aspect of the Oracle stack, ranging from SaaS Oracle Cloud ERP deployments to bare-metal installations of Oracle Cloud Infrastructure (OCI).

ZERO TRUST IN ACTION

Oracle Cloud ERP: During a recent Oracle Cloud ERP deployment, Deloitte assisted the organization in developing an insider risk profile for privileged users. All users, whether privileged or not, must now adhere to the principles of "least privileged access" and "need to know," which are foundational to zero trust thinking. The team additionally integrated the Oracle Cloud ERP application with enterprise Identity and Access Management (IAM) tools to provide greater visibility and control over user access.

OCI: Users often require global, remote access to the high-value data contained within workloads that are migrated to OCI. Deloitte has experience in assessing the regulatory and compliance landscape for OCI migrations as well as in building a micro-segmented, zero trust network to minimize the blast radius of potential threats and reduce the potential attack surface. In many instances, traditional cybersecurity approaches, such as virtual private networks (VPNs), should be replaced with an application-specific approach based on the principle of least privilege.

Oracle Cloud Supply Chain Management & Manufacturing: Supply chain risks have been aggravated by the global pandemic, bringing the vulnerabilities of the extended enterprise to the forefront. Deloitte helps organizations to develop third-party risk management programs that prioritize risk, identify appropriate risk indicators, and augment traditional controls, such as anomaly monitoring, with analytics. Zero trust thinking can be applied across the various stages of the program, beginning with vendor risk assessments prior to onboarding vendors within Oracle Cloud SCM. Limiting user access within and outside the network, scanning for vulnerabilities during data uploads, and isolating external networks and apps are other ways to protect the extended enterprise during Oracle Cloud SCM implementations.

Data analytics: In addition to protecting data access, zero trust principles are helpful across the entire data management life cycle, including create, store, use, archive, and purge. To start applying these principles, organizations often need to enhance situational awareness of their data through criticality assessment and classification. During Oracle Cloud migrations, Deloitte helps companies implement data classification standards while leveraging native Oracle capabilities for data protection such as transparent data encryption, data vaults, and encryption in transit, among others. In addition, our teams have deployed role-based access controls, integrated IAM management solutions, rationalized data-related regulatory requirements, and implemented archiving and purging policies.

CONNECT WITH US

Jeffrey Davis
Oracle Chief Commercial Officer
and Principal
Deloitte Consulting LLP
jdavis@deloitte.com

D'Arcy Mathias
Global Oracle Offering Leader and Partner
Deloitte Canada
darcymathias@deloitte.ca

John Liu
Global Oracle Chief Innovation Officer and
Managing Director
Deloitte Consulting LLP
johliu@deloitte.com

Bhavin Barot
Global Oracle Cyber & Risk Advisory Leader
and Principal
Deloitte & Touche LLP
bbarot@deloitte.com

Ritesh Bagayat
Senior Manager
Deloitte & Touche LLP
rbagayat@deloitte.com

Goran Ristovski
Senior Manager
Deloitte & Touche LLP
goristovski@deloitte.com

Peter Hodge
Sales Executive
Deloitte Consulting LLP
phodge@deloitte.com

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.