Accenture Technology Vision for Oracle 2016

Trend 5:
Digital Trust
Introduction

People First: The Primacy of People in a Digital Age

Leaders in the digital age do much more than tick off a checklist of technology capabilities. They know their success hinges on people. The ability to understand changing customer needs and behaviors is, of course, vital. But the real deciding factor in the era of intelligence will be a company’s ability to evolve its corporate culture to not only take advantage of emerging technologies, but also, critically, embrace the new business strategies that those technologies drive.

In this year’s Accenture Technology Vision, the overarching theme almost feels counter-intuitive. In a digital world, enterprises need to focus on enabling people—consumers, workers and ecosystem partners—to achieve more with technology. Taking advantage of technology to help people constantly adapt and learn, create new solutions, drive and manage relentless change, and disrupt the status quo is critical to compete, not only for the future, but more importantly today.

Building a competitive advantage into the digital world is where we focused our perspectives in this year’s Accenture Technology Vision for Oracle. With Oracle technologies, both on-premise and in the cloud, residing at the heart of so many of the world’s largest organizations, their contribution to achieving this ‘People First’ agenda is growing more important every day.
With this People First agenda in mind, we have again created our Technology Vision for Oracle to examine each of these five trends—Intelligent Automation, Liquid Workforce, Platform Economy, Predictable Disruption and Digital Trust—and how they're playing out in the Oracle world.

This report looks at one of those trends, Digital Trust, in greater detail. Pervasive new technologies raise potent new digital risk issues. Without trust, businesses cannot share and use the data that underpins their operations. That's why the most advanced security systems today go well beyond establishing perimeter security and incorporate a powerful commitment to the highest ethical standards for data. It's what establishing digital trust is all about.

Diving into report, you'll learn how creating and sustaining digital trust is achieved through a combination of security and ethics at every stage of each digital journey. Together, Accenture and Oracle address the core segments of data integrity, device security, application security, infrastructure security, business alignment, governance and compliance, identity management, and cyber defense management.
Technology Vision 2016 Trends: 
Reinventing the World Again and Again

Digital is now firmly embedded in every business. But even with technology as an integral part of the organization and its strategy, it is people who will underpin success in a world that continues to reinvent itself at an unprecedented rate.

This year’s Accenture Technology Vision highlights five emerging technology trends shaping this new landscape. Although each trend starts with technology, as you read you’ll see our ‘People First’ theme flows through each of them. Tomorrow’s leaders are taking these trends on board and executing strategies to secure their clear digital advantage.

Trend 1: Intelligent Automation
Intelligent automation is the launching pad for new growth and innovation. Powered by artificial intelligence (AI), the next wave of solutions will gather unprecedented amounts of data from disparate systems and—by weaving systems, data, and people together—create solutions that fundamentally change the organization, as well as what it does and how it does it.

Trend 2: Liquid Workforce
Companies are investing in the tools and technologies they need to keep pace with constant change in the digital era. But there is typically a critical factor that is falling behind: the workforce. Companies need more than the right technology; they need to harness that technology to enable the right people to do the right things in an adaptable, change-ready, and responsive liquid workforce.

Trend 3: Platform Economy
The next wave of disruptive innovation will arise from the technology-enabled, platform-driven ecosystems now taking shape across industries. Having strategically harnessed technology to produce digital businesses, leaders are now creating the adaptable, scalable, and interconnected platform economy that underpins success in an ecosystem-based digital economy.
Trend 4: Predictable Disruption
Every business now understands the transformational power of digital. What few, though, have grasped is quite how dramatic and ongoing the changes arising from new platform-based ecosystems will be. It’s not just business models that will be turned on their heads. As these ecosystems produce powerful, predictable disruption, whole industries and economic segments will be utterly redefined and reinvented.

Trend 5: Digital Trust
Pervasive new technologies raise potent new digital risk issues. Without trust, businesses cannot share and use the data that underpins their operations. That’s why the most advanced security systems today go well beyond establishing perimeter security and incorporate a powerful commitment to the highest ethical standards for data.

Winners will create corporate cultures where technology empowers people to evolve, adapt, and drive change.
Read any book about relationships and you’ll find trust defined as the foundation on which everything rests. And that goes for business too. A company’s relationship with its customers, business partners, and broader ecosystem all hinge on trust. Once, establishing that trust depended on a firm handshake and a steady gaze. But in the digital age, things are more complicated. Most relationships are sight unseen. The distances between entities are greater. And the interactions between business partners are infinitely more complex. Yet, establishing trust remains paramount.
Digital raises the security stakes

So how do you create and sustain digital trust? It’s through a combination of security and ethics at every stage of each digital journey.

As more and more companies become digital enterprises, they’re placing entire topographies of customer interaction online. They are transforming from traditional products to platforms. In the process, critical revenue channels become driven by a value chain of data, integration, infrastructure, and technical interactions—most of which the end user never sees. Instead they implicitly trust that the information they provide will be safe and protected. If security is breached, it won’t matter where it happens. As far as the customer is concerned, only one thing matters: their trust has been broken. And with that, an entire revenue channel is put at risk.

In the digital age, companies can lose a customer in a few mouse clicks. An unhappy customer has always been able to take their business elsewhere. But now, with the proliferation of social media, they can also take hundreds, or even thousands, of other customers with them. A violation of trust from a security breach can impact heavily on top and bottom lines. It can even cost C-level executives their jobs—a phenomenon that we’ve witnessed in the aftermath of various recent high-profile data breaches.1

If security is breached, it won’t matter where it happens. As far as the customer is concerned, only one thing matters: their trust has been broken. And with that, an entire revenue channel is put at risk.
Accenture’s Technology Vision 2016 defines digital trust as a combination of digital ethics and security. Although consideration of ethics should be a key part of digital transformations, it’s still a new concept for most businesses. Pressure to act is not just coming from customers. Knowledge workers are demanding that their employers put in place stronger ethical controls on data. Currently, most companies’ strategies align to a single vector: privacy. But that’s just one component of data ethics. Digital ethics is broader, encompassing the operational processes where data is applied to affect real-world outcomes.

**Figure 1: Digital Trust Wheel**

Currently, most companies’ strategies align to a single vector: privacy. But that’s just one component of data ethics. Digital ethics is broader.
To achieve the security aspect of digital trust, various components must be addressed in a complex web of interconnecting layers. These consist of executive directives, policies and procedures, preventive and detective security tools, security analytics, and timely threat recognition and response. The "Digital Trust Wheel" in Figure 1 shows all these components. Oracle products and Accenture's services address the core segments of data integrity, device security, application security, infrastructure security, business alignment, governance and compliance, identity management, and cyber defense management. As most of Accenture’s clients, many in the Fortune 500, run on Oracle, either Applications or Database, in some form, leveraging Oracle’s security products to protect the data makes perfect sense.

Customers invest their trust right from the start of any interaction, which normally means the user interface and functionality of a website or application. They trust that only authorized and authenticated users have access to their bank information, their order history, or their personal information. Accenture uses Oracle Identity and Access Management to deliver a scalable and secure solution for user authentication and authorization. For example, Accenture has supported several large US state governments’ migrations to platforms that provide millions of customers with covered care and health information exchanges. Applications like these are full of customers’ personal data.

---

**Oracle products and Accenture’s services address the core segments of data integrity, device security, application security, infrastructure security, business alignment, governance and compliance, identity management, and cyber defense management.**
Managing identity and access

Another aspect of identity and access management that we must consider is human behavior. Unfortunately, people are typically the weakest link in any technology chain. Risk-based access management has matured. It’s now a critical checkpoint to combat compromised credentials. At a large State entity, for example, Accenture integrated Oracle Identity and Access Management with adaptive access that would present additional challenge questions if an unrecognized pattern was detected (i.e., unknown location, device, or atypical login time).

Accenture has also now created an IAM-as-a-Service (IAMaaS) solution based on Oracle Identity and Access Management to provide the capabilities of an on-premises solution in the cloud. This helps enable customers to rapidly deploy an IAM solution—with extensive functionality—without worrying about technical expertise or maintenance of the application.

It can be an integral component of companies’ moves toward an agile development framework, helping them to establish the first step in digital trust.

Once a customer has finished an interaction with a company, their minimum expectation is that their data will be kept secure. In response, an identity and access solution controls the majority of authorized access vectors. But privileged access management also requires close attention. The 2015 Verizon Data Breach Investigations Report states that “60 percent of incidents were attributed to errors made by system administrators—prime actors responsible for a significant volume of breaches and records.” To address this, Oracle Privileged Account Manager allows companies to manage, monitor, report, and audit those critical accounts that have access to sensitive data.

Risk-based access management has matured. It’s now a critical checkpoint to combat compromised credentials.
Taking the right steps internally to gain customer trust is only half the battle. Making sure outsiders don’t gain unauthorized access to data and exploit hard-won trust is also crucial. The amount of data by 2020 is expected to exceed 44 zettabytes ($10^{21}$). And that’s why next-generation security mechanisms are ‘following the data’, taking user behavior into account and extending security well beyond the perimeter. Wherever data goes, security must follow. New products are addressing this challenge by integrating security solutions, such as security-aware application design, integrated database security, dynamic access controls, and runtime application protection.

A data-centric philosophy is also revolutionizing the layers and methods with which data is secured. For example, traditional security methods focused on perimeter security via firewalls and intrusion detection systems (IDS). However, threat modeling and vector-based approaches highlight why it’s paramount to add a layer of security directly to where the data is stored. Accenture is one of the only providers that currently delivers Oracle Audit Vault and Oracle Database Firewall as an appliance solution to protect that storage layer. While traditional IDS look at payload, Oracle can profile threats down to the SQL statement to identify security violations. This appliance works with traditional databases and also big data solutions such as Hadoop and MySQL.

Encryption is a well-known defense measure for securing stored data at rest. It should be a key component of every security strategy. But all too often, it’s missing or not being used. Companies often cite overhead and performance as barriers to its adoption. Even when encryption is in place, several aspects of data security are frequently overlooked. Even when encryption is in place, several aspects of data security are frequently overlooked. How is data secured when backed up? What about the secured state of data coming on and off the disk? This is despite the fact that memory-based attacks are on the rise and evolving fast, according to Mandiant’s 2015 trend report.²

All of the barriers to adopting encryption can be solved by using Oracle Engineered Systems. Using cryptographic acceleration, Oracle’s Supercluster M7 helps provide protection from attacks against data in-memory, on media, or transmitted over the network with limited overhead. By using Accenture Technology Labs and the Accenture Innovation Center for Oracle Engineered Systems, customers can ‘try before they buy’, validating the speed, performance, and security of their systems and customer data. It’s an essential next step.

Securing all states of data, at the data, is vital for digital trust.
Securing the legacy

In their rapid move to the digital economy, companies will most likely deploy new applications that still rely heavily on the integration of several unseen back-end applications (running legacy code and legacy security architectures). When it comes to security, this often gets overlooked. In the rush to the new, it’s often assumed that existing IT systems create no new threats. This could be a very costly oversight. To address it, companies can deploy Solaris zones, a method of virtualization to isolate applications and limit their exposure.

Insider risk can be mitigated by UNIX control and role-based access controls (RBAC) to fine-tune granular access. These applications can be managed with delegated administration, RBAC and process privileges. These help establish application root privileges and restrict access to the processes an application needs, removing the responsibility for security from the application developer and obviating the need to update or modify an application’s legacy code.

Connecting security with devices

Securing trust in the digital economy means establishing that trust directly with the customer and increasingly with their connected devices. The Internet of Things (IoT) is expected to embrace more than 50 billion such devices by 2020. In many cases, customers can be unaware of all the data that’s being captured, stored, and shared. However, their awareness (or lack of it) is beside the point. Companies are expected to act as responsible stewards of data, regardless of its source. The security points described above—identity and access management, data security, insider threats, and so on—apply equally to IoT. But there’s another dimension: the security of the device as an endpoint.

The security of a device versus that of a human is similar, yet also quite different. That’s why Oracle addresses security at both the data and device levels. For example, Oracle Internet of Things Cloud Service manages device endpoint metadata and lifecycle states. It also helps provide the registration and activation mechanisms needed to make all devices part of a secure IoT solution and it authenticates network communications and data streaming to help verify that all the components using data are part of the organization’s IoT network. Meanwhile, Java provides embedded security that facilitates reliable and secure messaging, and Oracle’s Database Security, Advanced Security, and Identity and Access Management products provide end-to-end security capabilities for allowing access, controlling access, and securing stored data at the network’s edge and in central data stores.
Reaping the rewards

Success in tomorrow’s digital business will largely depend on security decisions made today. Organizations should manage data and digital ethics as core strategies for mitigating business risks, just as they do with cybersecurity. Their reward? Unprecedented growth in an interconnected platform economy, with minimal downside risks.

Those who master this transformation can move beyond the first level of customer trust, namely that products will meet or exceed expectations, to a higher level where empowered individuals trust a company to lead them into the digital future. The road is not easy, but Accenture has the tools, such as Accenture Foundation Platform for Oracle, which can help kick-start the journey to a well-structured security landscape.

Success in tomorrow’s digital business will largely depend on security decisions made today. Organizations should manage data and digital ethics as core strategies for mitigating business risks, just as they do with cybersecurity.
Trend 5: Digital Trust
References

1 CSO magazine: http://www.csoonline.com/article/2859485/data-breach/9-data-breaches-that-cost-someone-their-job.html#slide1


The views and opinions expressed in this document are meant to stimulate thought and discussion. As each business has unique requirements and objectives, these ideas should not be viewed as professional advice with respect to your business.

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.