TechVision Research presents

IDENTITY AND ACCESS MANAGEMENT

AN INTRODUCTION TO THE TECHVISION RESEARCH REFERENCE ARCHITECTURE FOR IAM.

TechVision RESEARCH

Contents

Quoted facts and figures in this e-book come from various sources including: Forbes, US Bureau of Labor Statistics, Pew Research Center, HDI

Letter from the author

This is the first release of the TechVision Research Reference Architecture for IAM. As we continue our research and advisory practices, we will continually update the architecture considerations, providing deeper and richer content. As this content grows and the pros and cons of various approaches are discussed in detail, we are confident our clients' architecture decision-making will become increasingly easier.

We are very excited about the benefits and opportunities this initiative will bring to our clients and invite anyone interested in reviewing their organizations' IAM architecture to explore the TechVision Research Reference Architecture for IAM at www.techvisionresearch.com.

Enjoy,

An architect has the last word in any argument.

Anything another IT person says after that is...

... the beginning of a new argument.

There's nothing more that IT folks love to do than argue about definitions. If you ever want to have some fun in a room of IT folks, try asking for a definition of "identity" or "architecture" and see what happens. Despite the entertainment such arguments provide, definitions are important to the common language we need to communicate the intent and benefit of the things we in IT are trying to convince business to invest in. One way to create that common language is through a reference architecture.

What is a reference architecture?

Reference architectures are standardized frameworks that provide a model for a domain, sector, or field of interest. Reference models or architectures provide a common vocabulary, reusable designs and industry best practices. They are not solution designs and as such are not meant to be implemented directly. Rather, they are used to guide more concrete efforts. Typically, a reference architecture includes common architecture principles, patterns, building blocks and standards.

Five reasons to use a reference architecture

Why would you want to use a reference architecture? Here are five reasons why adopting a reference architecture is a good thing.

1. A reference architecture helps you to get an understanding of a domain. It provides a starting point for your own enterprise architecture effort. And it provides you with a basic vocabulary and structures so you do not have to reinvent the wheel.
2. A reference architecture supports interoperability. In our increasingly networked world, organizations need to connect and cooperate with all manner of other parties. The standards and building blocks provided by a reference architecture facilitates these connections. A related benefit is that using standards improves flexibility, because it is easier to exchange building blocks that connect via standardized interfaces; vice versa, it is much easier to develop standards if the building blocks themselves are standardized.
3. A reference architecture supports digital transformation of the enterprise. For many enterprises, transformation means their value chain is being redistributed among partners, service providers, and customers. If all parties speak the same language, use the same standards, and recognize the same boundaries between functions, processes and/or services, it will be much easier to recombine their elements in new ways.
4. A reference architecture facilitates measurement. Often, the differences between companies are not in the design of their business processes, but in their execution. Using reference designs makes it much easier to compare progress and execution results with others.
5. Measurement leads us to a fifth reason why a reference architecture is important: regulatory compliance. Often, reference architectures are prescribed (or at least strongly recommended) by regulators. For example, in the EU General Data Protection Regulation (GDPR) privacy protection principles, practices and processes are standardized and mandated. This leads to audit requirements and business reporting standards that are supported by a proper reference architecture.

So what does that have to do with Identity and Access Management?

We all know why IAM was implemented in the first place. As a reminder, the business was looking to improve these areas.

- ✓ **Security** - Automation and centralized administration allows a company to align access with job functions, ensure security policies are consistently applied, and enhance the reliability of security processes.
- ✓ **Efficiency** - Self-service, automation, and improved resource allocation visibility helps reduce a company's cost inside and outside of IT.
- ✓ **Simplicity** - Single sign-on and federated identity reduces user frustration and improve their usage of key applications.
- ✓ **Productivity** - Automation, workflow, and self-service results in more efficient processes, delivering quicker response times and allowing staff to focus on higher-leverage tasks.
- ✓ **Compliance** - Centralization and automation allows for automated audit reviews, enhanced compliance-related tracking of user activity, expedient access certification, and improved confidence in IAM processes.

SPOTLIGHT

Most Americans hold strong views about the importance of privacy in their everyday lives. The majority of Americans believe it is important – often "very important" – that they be able to maintain privacy and confidentiality in commonplace activities of their lives. Most strikingly, these views are especially pronounced when it comes to knowing what information about them is being collected and who is doing the collecting. - ***93%*** *of adults say that being in control of who can get information about them is important;* ***90%*** *say that controlling what information is collected about them is important.* ***- Pew Research Center***

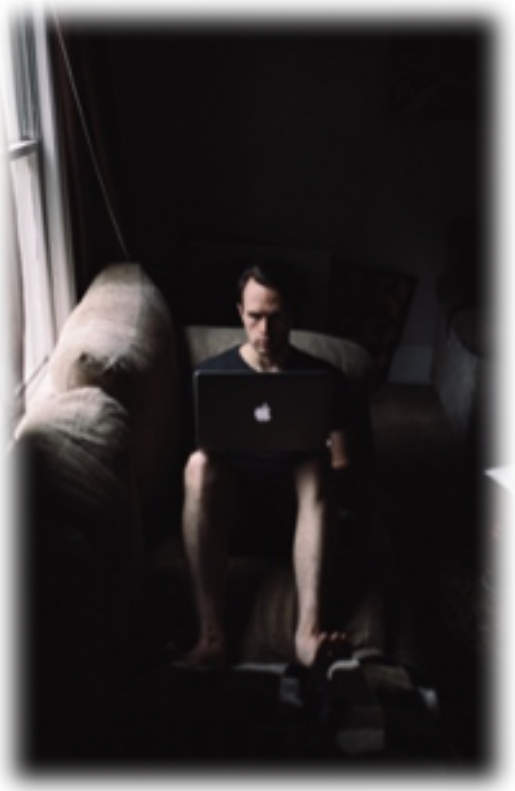
Bottom Line

Security and privacy are important to customers and employees alike. A single breach can cost millions in fines and permanently damage brand value. A well-tuned IAM capability is your best defense.

Security. Efficiency. Simplicity. Productivity. Compliance. While the benefits of deploying a robust IAM solution are clear, the cost and complexity of maintaining that solution can derail even the most well-intentioned organization given the following challenges.

Challenge:
An increasingly distributed workforce

It is said that all employment is temporary. The average millennial employee stays on the job for 2.8 years, 35% of the US workforce are freelancers, and outsourcing and offshoring are still strategic choices. Customers are fickle and any friction in the relationship drives them away. These divergent groups need access to the right corporate systems anytime, anywhere to be successful. The fluidity in the relationships between people and the business is causing enterprise IT teams to face a much more daunting challenge: maintaining a consistent frictionless experience in connecting to corporate resources without sacrificing security.



more people than ever are choosing to freelance, up to 55 million this year, or 35% of the total U.S. workforce.

Challenge: Distributed applications

With the growth of cloud-based, mobile, and Software as a Service (SaaS) applications, users now have the power to log in to critical business and productivity apps like Salesforce, Office365, Slack, and more anytime, from any place, using any device. However, with the increased use of line-of-business sponsored apps comes an increase in the complexity of managing user identities for those applications. Without a seamless way to access these applications, users default to simple but unsafe security habits while IT is faced with rising support costs and increased security risk.

The cloud has quickly become a mainstay in IT departments, with 95 percent of businesses using cloud technology in some form or another. .

Challenge:
Bring your own device

Access to corporate resources through personal and other non-corporate managed devices is no longer the exception. It is the rule. Employees, temporary workers, partners, and customers routinely blend personal and professional activities. The challenge with BYOD is whether IT can balance protecting the organization's business assets, productivity and freedom of choice for the benefit of all. To maintain the balance, the IT staff may struggle to manage who has access privileges to corporate data and which devices they're using to access it.

The vast majority of Americans – 77% – own smartphones. Nearly eight-in-ten U.S. adults now own desktop or laptop computers, while roughly half now own tablet computers.

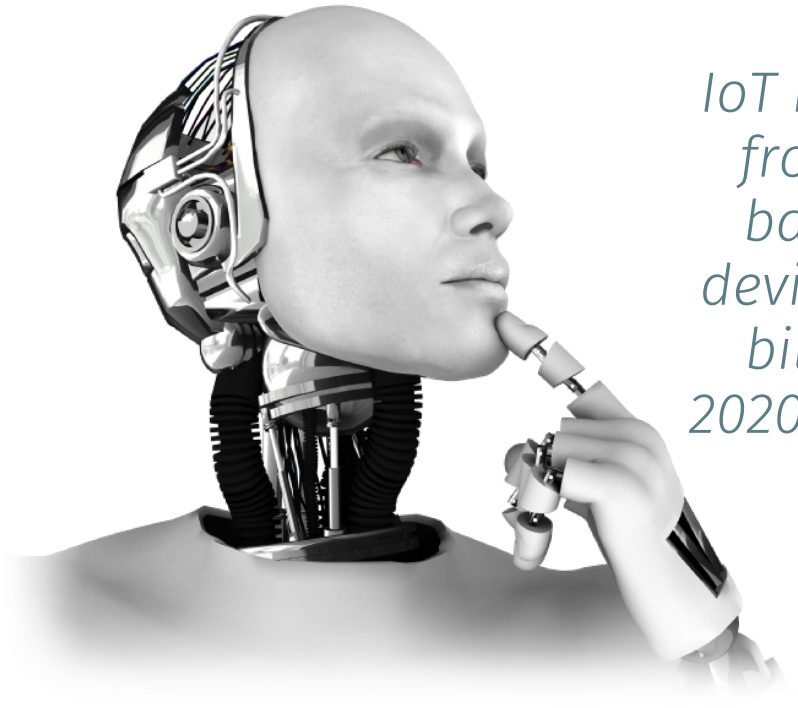
Challenge: User experience

Employees, temporary staff, suppliers, and customers are all being pulled into the digital transformation. When IAM prioritizes security over ease of use, the user experience suffers and that impacts the company's wealth. Plus, when users have trouble getting access to what they need, they most often contact IT staff for help, which can quickly and repeatedly drain important resources.

Number of support center calls due to account access problems range from 10% to 30% depending on the strength of the security processes employed.

Challenge:
The device is the user

While BYOD is still challenging for many enterprises, the next wave, connected devices as part of the Internet of things, is a game changer. IoT brings unprecedented scale, complexity, and risk associated with relationships, entitlements, and ownership. IAM solutions in the IoT era must be more flexible, context-aware, and able to scale seamlessly.



IoT market will grow from an installed base of 15 billion devices in 2015 to 30 billion devices in 2020 and 75 billion in 2025

Challenge: Regulatory compliance

Compliance and corporate governance concerns continue to be major drivers of IAM spending. And that won't change anytime soon. Financial and privacy rules are shifting in response to evolving technology and increased digital transformation. Ensuring support for processes such as determining access privileges for specific users, tracking management approvals for expanded access, and documenting who has accessed what data and when they did it can go a long way to easing the burden of regulatory compliance and ensuring a smooth audit process.

A hidden cost of GPDR is the requirement to hire 28,000 data protection officers, per the International Association of Privacy Professionals estimations.

These challenges are driving many companies to reevaluate their current IAM solution, but it's hard to tell where the current IAM capabilities may be impacted and how to prioritize any change efforts.

Enter the IAM reference architecture.

"Would you tell me, please, which way I ought to go from here?"

"That depends a good deal on where you want to get to."

"I don't much care where –"

"Then it doesn't matter which way you go."

– Lewis Carroll, Alice in Wonderland

As this exchange between Alice and the Cheshire Cat reminds us, if we don't have a vision of where we are going, if we don't know the right questions to ask, we may not get where we want to go. For the IT team to avoid Alice's predicament, it needs a point of reference, an IAM reference architecture.

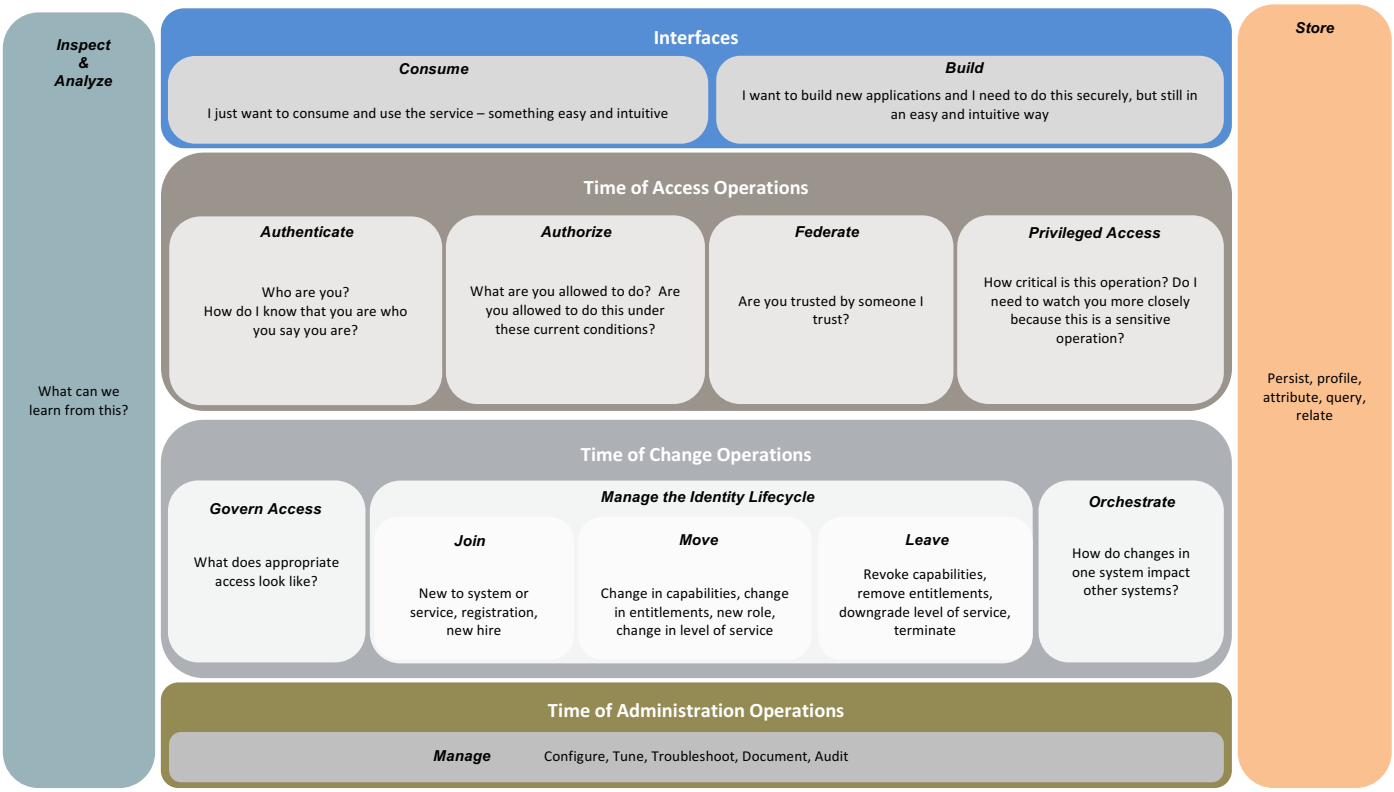
Introducing the TechVision Research Reference Architecture for IAM

TechVision Research is a leading research and consulting firm specializing in identity and access management (IAM). Our consultants' deep and extensive IAM expertise, based on more than 25 years' experience, has resulted in the development of the first TechVision Research Reference Architecture for IAM, a tool that provides a comprehensive methodology for assessing requirements and architecting optimal IAM solutions.

- ✓ **Interact** – how end-users and application developers interact with the IAM platform.
- ✓ **Access** – the rules that define the roles, rights, and obligations of any actor wishing to access enterprise assets.
- ✓ **Change** – the capability to define and manage the relationships between the user/ application developer and the enterprise assets.
- ✓ **Manage** – the capabilities required to manage and upgrade the IAM solution itself.
- ✓ **Measure** – the capabilities required to audit and improve IAM activities.
- ✓ **Store** – the capabilities required to share identity information and relationships between the components of the IAM solution.

The TechVision Research Reference Architecture for IAM is a master template that identifies the IAM capabilities (rather than technologies) that can be improved or enabled, allowing business stakeholders and technical architects to achieve a common language for IAM functions, which can then be refined over time.

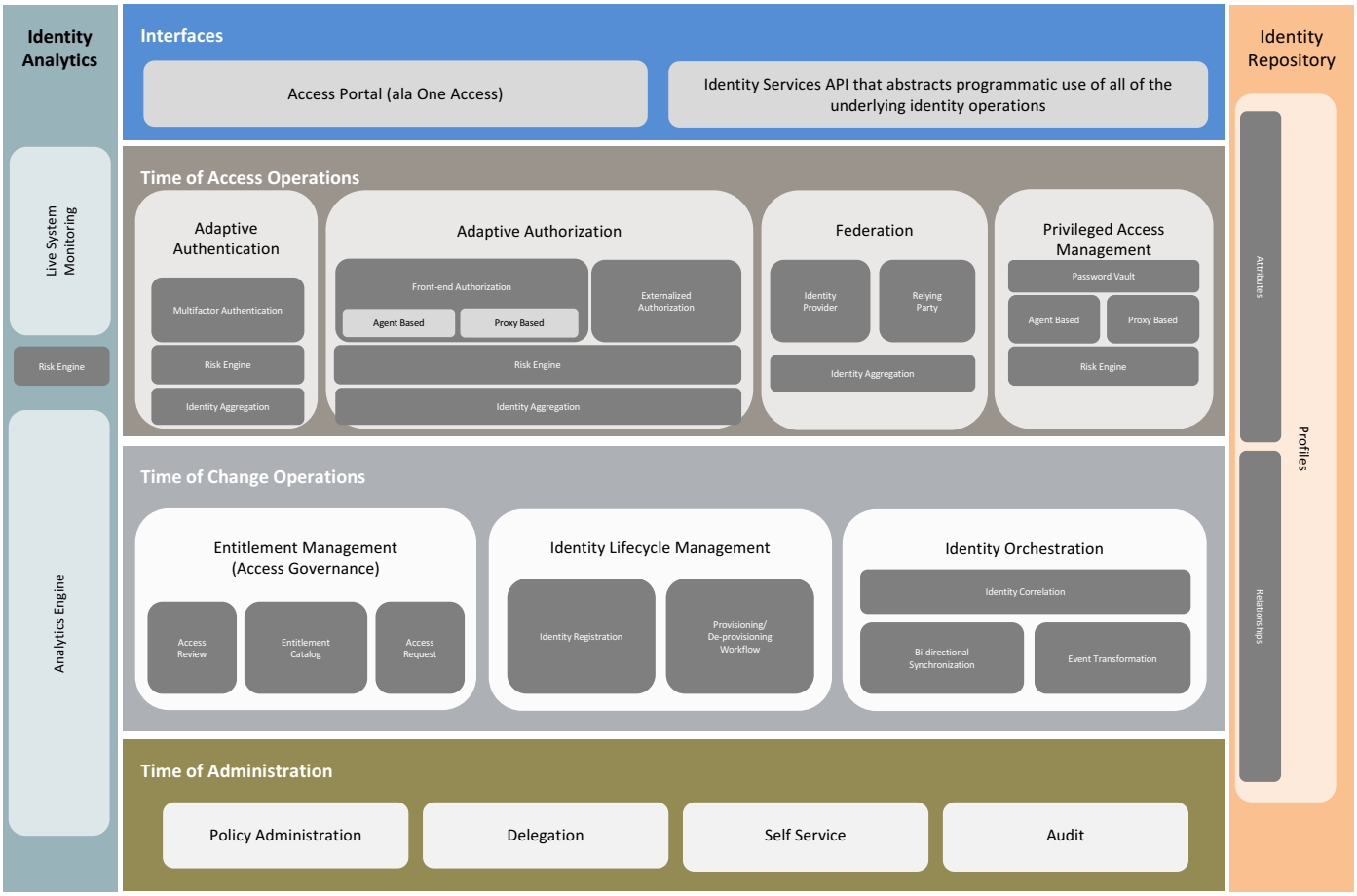
As discussions progress into deeper levels of discovery, this master template organizes discussions beginning with the high-level interfaces associated with both end-user and application developer IAM service consumption.



From either of these perspectives, clients can navigate deeper into the run-time functionality requirements for:

- ❖ access (e.g., authentication, authorization, federation, privileged access, etc.),
- ❖ identity lifecycle management (e.g., joiner/mover/leaver, access orchestration, and governance),
- ❖ IAM infrastructure administration,
- ❖ IAM data management and reporting.

Once the required capabilities are identified, the next layer of the TechVision Research Reference Architecture for IAM allows us to explore each of the specific technology or process elements comprising each capability in the form of a combined portfolio architecture.

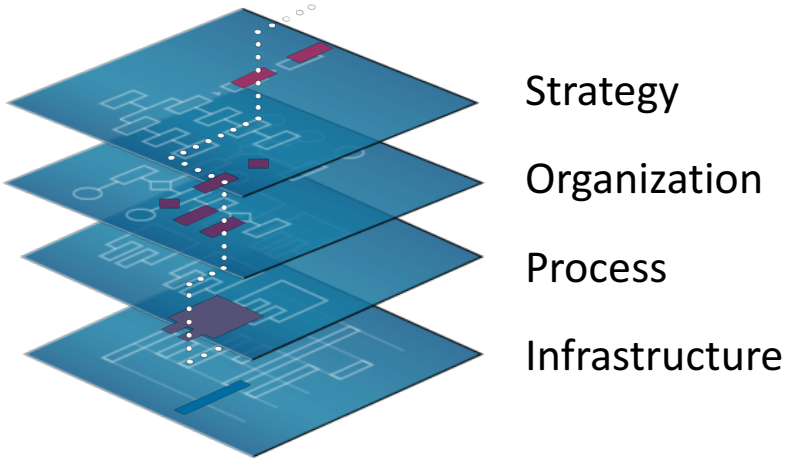


With this information, technical architects can rapidly zero-in on the current options (technology and process) their IAM architecture should evaluate to achieve the required capabilities for the business. In the form of architecture considerations, each of the options available is then described in more detail to help identify the right approach for an optimal IAM architecture and deployment strategy. As such, the TechVision Research Reference Architecture for IAM is a comprehensive 'checklist', a methodology to break down the business capabilities a client is endeavouring to facilitate, coupled with the technology and process necessary to achieve its objectives.

TechVision Research Advisory Services

Our advisors use this framework in all our engagements so that a TechVision Research client's IAM architecture and deployment strategy is well designed and ready to evolve with its business. Our assessments and workshops are designed to:

- ✓ Find & model pain points
  - Level-set business objectives, strategy, organizational roles, and IAM best practices.
  - Capture the current IAM process models
  - Create the "as is" IAM framework from which to go forward
  - Identify impact points in the organization
  - Document the linkage between processes and the business strategy, organization, services and IAM infrastructure
- ✓ Identify improvement opportunities
  - Quantify the benefit and cost of current processes
  - Identify and quantify future state operational cost and risk associated with adopting change
- ✓ Frame innovation priorities
  - Determine NPV of operational costs value and benefit for each course of action
  - Prioritize the roadmap for adopting changes
- ✓ Frame technology interdependencies
  - Find pain points, improvement opportunities, define innovation and act on the innovation definition
  - Includes impact on people, process and technology



All with the aim of delivering the roadmap and business case for the successful delivery of a secure, resilient, and future-proof IAM capability.

Related research

TechVision Research provides early perspectives on key technology trends to help our clients stay ahead of the most difficult technology challenges they'll face. Our research agenda uncovers key technology inflection points and defines their impact on organizations.

We take these inflection points and apply rigorous analysis leveraging technical depth, pragmatic business, industry and analytical skills. We augment this with experiential data collected from our advisory engagements.

We've included a sampling of the IAM research we make available to our clients. Please visit our website to access complimentary extracts of these reports.

Published

The Future of Identity Management
By: Gary Rowe, Doug Simmons, David Goodman, D. Phil., Bill Bonney, Principal Consulting Analysts

Blockchain-based Identity Management
By: Doug Simmons and Gary Rowe, Principal Consulting Analysts

Putting Identity into Context: Next Generation IAM
By: David Goodman, D.Phil, Principal Consulting Analyst

Opportunities in Europe with Electronic Identification and Trust Services
By: David Goodman, D. Phil., Principal Consulting Analyst

TechVision CrossTalk Report: Identity and Data Governance
By: Bill Bonney, Gary Rowe and Noreen Kendle, Principal Consulting Analysts
Moderated by Ted Ritter, CISSP

Getting to Know Your Customers: The Emergence of CIAM
By: David Goodman, D. Phil., Principal Consulting Analyst

Machine Learning and Artificial Intelligence on Big Data for Cybersecurity (New)
By: Fred Cohen, Principal Consulting Analyst

Upcoming

Identity of Things (IDoT)
By Bill Bonney and Gary Rowe, Principal Consulting Analysts

The Cloudification of Identity—IDaaS Market Overview
By: Gary Rowe, Principal Consulting Analyst

Banking, Identity and the Regulators (New)
By: David Goodman and Rhomaios Ram, Principal Consulting Analysts

Digital is disruptive. Digital has dramatically reduced barriers to entry and allowed more businesses to enter any market they choose. At the same time, digital is creating massive opportunities for your company to develop new products, services, and wealth.

For many companies, digital is moving from a bolt-on at the edge of the business to the center of core processes. As such, digital is impacting every aspect of the value chain.

Digital demands velocity. If you're not thinking of new ways to digitally engage your customers, others will. That makes digital transformation a journey, not a destination and change is the new normal.

At TechVision Research, we know the goal of safe digital transformation is the growth and stability of your business. That's why we've built a research company that is nimble, brings real-world experience, provides a pragmatic perspective, and makes its resources widely available to everyone in your business. Our team of expert consulting analysts combine deep technology and industry knowledge to connect business and technology in ways that others cannot. At TechVision, we help you:

- Identify and build upon your core strengths
- Focus on customer data as a foundation for a transformed business model
- Architect and deploy an operational backbone and make it accessible
- Define agile digital business platforms and responsive capabilities
- And all along the way, secure it all

At TechVision Research, we focus on your success. With a unique combination of cutting-edge research, high-impact workshops, and expert and actionable advice, TechVision helps you leverage technology to get the job done. Find out more at techvisionresearch.com

TechVision Research

Direct Experience, Pragmatic Advice, Great Value!