TechVision RESEARCH

Identity as the New Perimeter

Abstract

Digital transformation, mobility and the proliferation of applications and networks have made traditional forms of information protection increasingly difficult to manage and enforce. Information is everywhere, access is widely distributed, but most security programs are still largely based on archaic, static security models that just don't work anymore…and it is getting worse. The latest evidence of this is recent breach disclosed by Equifax that has exposed identity information for over 140 million individuals. Enterprises continue to take on enormous risk by aggregating unnecessary personal data while customers can't manage the massive number of IDs, passwords and data required to interact with every on-line connection.

TechVision believes that the common denominator across most aspects of information protection is identity. An identity inextricably linked to a person, device, application, system or network is today the most dependable 'perimeter' we can rely upon to determine what and how to make information available properly and securely. Identity management will soon have to make the leap from our age-old approaches of multiple user IDs and passwords to a new, secure, privacy-centric means of identification.

The good news is that the bulk of the underpinnings for this more flexible, scalable and secure user-centric identity model can leverage existing technologies...but there are a few pieces such as blockchain and verifiable claims that can be added to accelerate the movement to self-sovereign identity and access management.

This new, user-centric identity model leverages personas related to verifiable claims that can both protect privacy (and reduced liability for the enterprise) and provide distributed access to authorized services. In such a way, we boil it down to identity as being the primary security perimeter that is applicable in enterprise, banking, commerce, social networks and other forms interaction. The lowest common denominator becomes identity and we recommend CIOs, CISOs and Line of Business (LOB) leaders carefully evaluate
this new approach for distributed identity .

This report covers:

- The new definition of identity
- The concept of a persona
- Verifiable claims (digitally signed attributes) that can comprise various personas
- The rise of reputation as a deciding factor
- The way forward into the new world of identity-centric security and risk management.

Authors:

Doug Simmons
Principal Consulting Analyst
dsimmons@techvisionresearch.com

Nick Nikols
Principal Consulting Analyst
nick@techvisionresearch.com

Gary Rowe
CEO, Principal Consulting Analyst
gary@techvisionresearch.com

Gary Zimmerman
CMO, Principal Consulting Analyst
garyz@techvisionresearch.com

Table of Contents

Executive Summary

TechVision Research believes the current identity services approach in the business to consumer (B2C) space is at a tipping point. The unmanageable and accelerating proliferation of identities and associated identifiers (user IDs) and passwords that need to be individually established and managed for every B2C connection is a model that is already collapsing under its own weight. From an enterprise perspective, collecting all this data and protecting it is a tremendous expense and a significant risk. From an individual perspective it is difficult to manage, invasive, and increasingly limits open engagement with potential business partners.

This report describes a future state solution TechVision sees as a fundamentally better approach to managing and leveraging external identities within an enterprise. Identity is the new perimeter, but that doesn't mean that the enterprise needs to own all of these identifiers and PII; they simply need to incorporate, support and use distributed identities based on the level of trust and the specific supporting data that is needed for a particular use case.

This report describes a new approach with Identity as this new perimeter with benefits in enterprise security, risk mitigation, and has the potential of better positioning the organization with those individuals or organizations digitally connecting. We describe a roadmap toward achieving this distributed, self-sovereign identity model that starts with better leveraging existing technologies and adds a few new ingredients to achieve enterprise and customer goals.

The good news is that we can start by repurposing many existing components including mobile devices, existing privacy-centric initiatives (like GDPR), cloud/SaaS services, and existing security and identity technologies such as PKI, federation, identity aggregation and orchestration, and contextual identity as a basis for this this new, self-sovereign, distributed identity model. But the secret sauce is to build on this foundation with a few new and evolving components; starting with blockchain, verifiable claims, and reputation systems.

What we are describing in this report isn't a "quick fix" IT program; it is a fundamental shift in how enterprises engage customers, trading partners and the general public. We recommend enterprises use this as a foundation for providing better security, limiting liability based on retaining unnecessary PII and use this to provide a better, more open, more trusting, customer friendly engagement platform.

Introduction

The proliferation of applications, devices (personal and at work) and networks (social, work, service provider, etc.) have made traditional forms of information protection increasingly difficult to enforce. Firewalls, for example, have so many holes opened in them that the properly managing and monitoring network and system access has become nearly impossible. The notion of the 'disappearing security perimeter' concept is not new. In fact, we introduced this over fifteen years ago when we were at Burton Group. What is becoming evident, however, is that the common denominator across most aspects of information protection is identity. An identity inextricably linked to a person, device, application, system or network is today the most dependable 'perimeter' we can rely upon to determine what and how to make information available properly and securely. Identity is the new perimeter and that concept is the focus of this research report.

Security is really about determining and enforcing appropriate access to information, assets and resources. Often this has taken on a very physical mindset, protecting these elements by locking them up in a vault, or behind a firewall. In fact, the very concept of a lock and key underscores a more fundamental relationship - that the key is the means by which the possessor can demonstrate that he/she is the appropriate person to be able to open the lock. In this example, the means by which this relationship is expressed is far from foolproof, but by providing a deeper focus on the nature of this relationship it becomes clear that a better understanding of the context of the identity that is attempting access will lead to much more dynamic, pervasive, and effective security models.

Establishing identity as the new perimeter starts, of course, by understanding what an identity is and how it might be used to establish this security foundation. The concept of identity is fairly simple in that it is a representation of real world objects. It can apply to people, organizations, devices, buildings, conference rooms, policies and all sorts of "things". So, even a collection of identifiers and attributes that describe these identities have the potential of being a flexible and pervasive means of protecting and securing business and personal assets. Security based on physical locations and well-defined perimeters breaks down when devices and identities can emerge anywhere and everywhere.

While establishing identity as the new perimeter is a noble goal and is inevitable, the mechanisms and models for the handling of identities, personas, identity management and personal control need to be modified to make this concept a reality. So, what does this new individual identity model look like? It starts with a focus on personal data privacy as this is critical in protecting against identity theft and fraud. This protection is critical for both individuals and for enterprises. The pervasive sharing of so many individual attributes with service providers--whether commercial, employment-related, personal, governmental or social media-related is at the root of the privacy challenge and should be addressed in the

new individual identity model.

This has led to the notion of a persona as a way to better address a balance between identifiers and individual privacy and control. Personas become snapshots of individuals, allowing a person to invoke pseudonyms to be appropriately identified in a specific context online. With pseudonymity, individuals are empowered to develop a relationship with various services by sharing a small number of attributes (or no attributes at all) that help define identities and a persona in a particular plane of existence, but this purposely falls short of sharing unnecessary or undesired attributes. In a way, we've transcended anonymity as the only form of non-personal interaction with online services by upping the ante to pseudonymity. With this in mind, the concept being introduced here - identity as the new security perimeter, might be better stated as 'persona is the new perimeter'. That may be splitting hairs at this point, but it is important to understand that identity in the journey we are embarking upon here is more than just a single user ID and password.

An understanding of pseudonymity and personas establish a conceptual foundation for identity as the new perimeter is a good first step, but only a first step. There is still a missing ingredient that limits the value of pseudonymity in our new identity model: trust. Establishing trust revolves around determining how a service provider (or employer network) knows that the endpoint identified as batman678 (or (908) 555-1212, or http://210.01.55.48) is the actual person they claim to be. Does the service provider trust this association to the degree they need to for the type of relationship they are engaging in? This is where definitive attributes that identify a person in terms of capability or verifiable historical transactions become most important.

A pseudonymous persona should be able to transmit and share one or more selected attributes with the service provider that vouch for this person's 'identity' in a way that does not share his or her entire identity and preserves and protects personal identifiable information (PII). These attributes - though 'opaque', must be trusted. How well the shared attributes are trusted is dependent on how well the entity or entities that vouched for the authenticity of these attributes is trusted. That is the notion behind the long-standing principle of transitive trust. This is the model for identity federation that has been in existence for nearly two decades, so is nothing new in and of itself.

How well the shared attributes are trusted is dependent on how well the entity or entities that vouched for the authenticity of these attributes is trusted.

What has been lacking over the years is a workable mechanism for individuals,

organizations or devices to accumulate and share trusted attributes about themselves on a case-by-case basis. This is what is meant by 'user centricity' and the concept of 'user consent'. The underpinnings for a more flexible, scalable and secure means of enabling user centricity and consent in the digital world are gradually becoming available but are still falling short of a new, much-needed user-centric form of authentication and authorization. Once these building blocks are more fully established, we'll be able to safely migrate to a world where 'bring your identity' (BYOI) is standard, desirable and secure for authenticating ourselves to virtually every form of digital service; whether it is commerce, employment, health care or financial-related.

In this paper, we'll identify the requirements more specifically for a user-centric identity model, which exposes identity as the new perimeter. Following that, we'll look at current and emerging technology and social advances that may make this a reality given that many of the necessary building blocks are already in place or taking shape.

The Starting Point - Moving from Fixed to Flexible Identities

Throughout history there have been hardwired forms of identification that pertain to very specific expectations. For instance, at birth there is often some form of national identifier (e.g., social security number, birth certificate) attached to us. An individual's physical attributes such as height, weight, eye and hair color are later published on drivers' licenses for virtually anyone to see. Pictures are on our passports and ID cards, along with home or work addresses. In many ways, society has been functioning by using physical, fixed attributes as the primary form of identification for centuries, if not millennia.

The movement from fixed, static models to more flexible, open models isn't, of course, limited to Identity Management; virtually every infrastructure area is moving to a more adaptive, flexible and inclusive model. And the need for this type of flexibility will accelerate as enterprises move more aggressively towards DevOps, microservices, cloud computing and digital transformation.

And it isn't just flexibility we need to aspire towards, it is the protection of personal information that may be stored anywhere, but is under the control of the enterprise that acquired that information. In a digital world, sharing unnecessary sensitive information for each transaction should no longer be required. Sharing more information than required for a transaction increases the liability of the organization collecting that information and can be viewed negatively by customers and regulators. But to do this we need to move towards this flexible identity foundation.

A great example of fixed, single purpose identities with more information than should be conveyed can be found with credit cards. Individual names are emblazoned on credit cards, and an individual's name along with the associated credit card number is traditionally

needed to purchase goods or services with credit cards whether online or at point-of-sale. Individuals are starting to question why merchants, service providers or even employers need more data than is necessary to conduct a transaction. Isn't the fact that the credit card has available credit for the merchant to receive funds from a customer's account the only important piece of information the merchant really cares about? The same is true with taxi drivers, hotel clerks and hundreds or thousands of transactions that individuals conduct every year. A name is emblazoned on the card for 'identification purposes', but it is apparent that in today's digital world, that information (personal name) is a rather meaningless form of verification, and in fact only puts the individual at risk identity fraud.

Historically speaking, it was more important to have multiple attributes available to merchants, service providers and employers so that they could theoretically "triage" this information into some form of assurance that we are who we say we are. Coupled with these shared attributes has been the concept of 'reputation'. Questions like "who knows this person?", "has he or she successfully performed a similar transaction in the past?", etc. are factored in the decision-making process as to whether to trust the individual. How well this pile of personal information – including reputation, was actually triaged (and protected from misuse) has always been suspect. And, with the onset of global digital transformation, the sharing of this information and its subsequent proliferation has radically increased the opportunity for and pervasiveness of identity theft and fraud.

Continuing this analysis, once some level of acceptable triage was performed a person was instructed to create a user ID and password specific for the intended purpose (e.g., online bank access, employer network access, etc.). It is generally understood at this point how problematic the proliferation of user IDs and passwords has become – each pair used as a form of rigid persona that is only usable or recognizable by a single entity/service provider.

Let's just say this system is broken in that the vast majority of people either use the same user ID and password everywhere or write them down somewhere that can be easily compromised—both practices are represent high risk for the individual and the systems to which the individual connects and trusts. As we stitch together more and more of these user IDs and passwords across tens or hundreds of individual sites, personal information becomes exponentially less secure. This is the unfortunate mess that individuals and organizations are in today.

TechVision believes there is a better way and it starts with the transition from fixed to flexible identities. This is critical in walking the fine line of providing secure identities when needed without sharing data that isn't necessary for a particular use case. While we'll introduce some new technologies (at least to some readers) and new approaches in this report, we can start by considering how some of the existing technologies and processes can be intelligently orchestrated to move us towards our goal of establishing Identity as the new perimeter.

About TechVision

World-class research requires world-class consulting analysts and our team is just that. Gaining value from research also means having access to research. All TechVision Research licenses are enterprise licenses; this means everyone that needs access to content can have it. We know major technology initiatives involve many different skill sets across an organization and limiting content to a few can compromise the effectiveness of the team and the success of the initiative. Our research leverages our team's in-depth knowledge as well as their real-world consulting experience. We combine great analyst skills with real world client experiences to provide a deep and balanced perspective.

TechVision Consulting builds off our research with specific projects to help organizations better understand, architect, select, build, and deploy infrastructure technologies. Our well-rounded experience and strong analytical skills help us separate the hype from the reality. This provides organizations with a deeper understanding of the full scope of vendor capabilities, product life cycles, and a basis for making more informed decisions. We also support vendors when they carry out a product and strategy review and assessment, a requirement analysis, a target market assessment, a technology trend analysis, a go-to-market plan assessment, or a gap analysis.

TechVision Updates will provide regular updates on the latest developments with respect to the issues addressed in this report.

About the Authors

Doug Simmons brings more than 25 years of experience in IT security, risk management and identity and access management (IAM). He focuses on IT security, risk management and IAM. Doug holds a double major in Computer Science and Business Administration.

While leading consulting at Burton Group for 10 years and security, and identity management consulting at Gartner for 5 years, Doug has performed hundreds of engagements for large enterprise clients in multiple vertical industries including financial services, health care, higher education, federal and state government, manufacturing, aerospace, energy, utilities and critical infrastructure.

Nick Nikols has more than 25 years of experience in the software industry, architecting solutions and developing innovative products for identity, security and compliance management, as well as directory services and directory/application integration.

Before working with TechVision Research, Nick was Senior Vice President of Product Management and CTO of Cybersecurity at CA Technologies, where he was responsible for CA's Cybersecurity Product Strategy and Roadmap. At CA, he was particularly focused on modernizing CA's Identity-centric Security portfolio and successfully promoted CA's Identity Manager and Access Governance solution into a leadership position within Gartner's Magic Quadrant for Identity Governance and Administration.

Gary Rowe is a seasoned technology analyst, consultant, advisor, executive and entrepreneur. Mr. Rowe helped architect, build and sell two companies and has been on the forefront the standardization and business application of core infrastructure technologies over the past 35 years. Core areas of focus include identity management, meta-directories, cloud computing, security/risk management, messaging, privacy and personal clouds.

He was President of Burton Group from 1999 to 2010, the leading technology infrastructure research and consulting firm. Mr. Rowe grew Burton to over $30+ million in revenue on a self-funded basis, sold Burton to Gartner in 2010 and supported the acquisition as Burton President at Gartner.

Gary Zimmerman is an experienced executive known for helping companies deliver new offers and expand markets. Accomplishments include launching four companies, 20+ products, building high-performance organizations, and generating millions in sales.

His experience at Neustar, Respect Network, and Sovrin allows him to provide a broad perspective on a variety of subjects including self-sovereign identity, blockchain, enterprise data management, and the data brokerage industry.