Symantec
A Division of Broadcom

Modern Identity and Access Management

BUILDING TRUST WITHOUT SACRIFICING SECURITY

The Next Era of the Digital Revolution

We are in the early stages of the Fourth Industrial Revolution—the App Economy. In its scale, scope and complexity, this revolution is unlike anything we have previously experienced. The app economy is global, responsive, customer-focused and technology-driven—with data at the center of it all. And in the year 2025, we will collectively create 175 trillion gigabytes of data—5x more than in 2018[1].

The winners of this next era will be those who can derive the most value from a vast pool of data, transforming every touch into a perfect, personal experience. But any organization seeking to capitalize on these opportunities must also be prepared to face exponentially more risk.

Digital Transformation Brings Risk

While data explodes in size and becomes ever more personal, our expectations around security and privacy will continue to rise—multiplying the legal, financial and reputational costs of failure. Current security models will soon be too slow, rigid, and error-prone to protect your digital infrastructure.

Organizations need powerful AI and automation to create a unified security platform that monitors data through its entire lifecycle, responds instantly to threats, and safeguards trust from mainframe to IoT—at the speed and scale of the next era.

1. Data Age 2025: The Digitization of the World From Edge to Core, IDC 44413318, November 2018

Balancing User Experience and Security in a Zero-Trust World

With the creation of the app economy, users have been given more choices for services than ever before and they are overwhelmingly choosing experience as the differentiator.

For most, the primary challenge in embracing the app economy revolves around developing agile approaches to software delivery to meet customers' expectations. However, rushing applications to market to stay competitive often comes at the expense of quality and security, and these defects can have devastating impact to the business.

Can security improve without impacting user experience?

"If people like you, they will listen to you, but if they trust you, they'll do business with you."

— Zig Ziglar

The answer is yes.

Leading organizations understand that data breaches have become the norm in today's connected world. With information being everywhere and personalized experience driving digital transformation, identity is critical. Identity is the foundation for trust.

But how do we establish this trust without burdening the users? There are five critical questions that need to be addressed by any modern IAM solution:

- How do I **secure the modern interfaces** without impacting software delivery timelines?
- How do I **identity a legitimate user** from a fraudulent one?
- How do I **unlock the full potential** of my data without increasing my exposure?
- How do I **reign in privileged users** and protect against insider threat?
- How do I **automate my threat response** without burdening the security team?

78%

of consumers responded that it is very important or crucial that their PII be protected online[1]

43%

of business leaders indicate that they sell PII data to other organizations[1]

48%

of consumers will stop using a service following a data breach or breach of trust[1]

1. Frost & Sullivan: The Global State of Online Digital Trust, August 2018.

How to Secure Mobile and APIs?

Mobile applications are undoubtedly the current wave for users to interact with organizations. The successful apps are easy-to-use, convenient, and almost always available to the user, but the next wave is here—the Internet of Things. Smart devices are proliferating our lives and Ericsson predicts that there could be 3.5 billion IoT devices connected over cellular networks by 2023[1]. Is your organization prepared to handle this new channel?

Embedding Security into the DevOps World

Developers are focused on delivering the optimal user experience, and for many, security is just going to be a speed bump in the development process. To address this, security must be easy to embed with but be flexible so that the business can configure the appropriate balance of trust and convenience.

A modern IAM solution must protect mobile apps and APIs but also support developer velocity by embedding security into apps without lots of coding. This ensures that developers can focus on building winning features that improve customer experience, not spending time learning to be security experts.

1. Ericsson: Mobility Report, June 2018

How to Identify Legitimate Users?

Because passwords—the most common authentication credential—can be easily stolen, guessed or given away, organizations have been exploring alternative methods to identify users, such as biometrics, one-time-passwords, and push notifications. Each can help improve assurance that the user is whom they claim to be, but each can impact to user experience is not applied in an intelligent manner.

Creating the triangle of trust

The universal SDK embedded by developers must not only support these modern authentication mechanisms and latest federation standards, such as OpenID Connect, OAuth, and SAML, but it should also be capable of uniquely identifying the user, app, and device.

A modern IAM solution must then be able to monitor the relationships between these three to deliver a triangle of trust. With this increased security, higher risk transactions can be enabled on the app to improve user convenience without added security exposure.

One of the biggest challenges in the app economy is establishing trust. Consider the most basic interaction with a user—authentication. How confident are you that the person logging in is the legitimate account holder?

How to Unlock and Share my Data?

The future will bring an explosion of data on a scale that is unprecedented. By 2025, IDC predicts that worldwide data will grow 61 percent to 175 zettabytes. Additionally, they believe that almost 30 percent of this data will be consumed in real-time and that the "average" person will have nearly 5,000 digital interactions per day by 2025, up from the 700 to 800 or so that people average today".

The winners of this next era will be those able to derive the most value from this vast pool of data, manipulating it on the fly to transform every touch into a perfect, personal experience. In today's world, you need to be agile and provide superior user experience without sacrificing trust.

Unlocking the Full Potential of Your Data

Organizations must unlock and expose their data to power the next generation of cloud, mobile, and API-driven transactions. But each interaction represents a threat vector and an opportunity for theft.

A modern IAM solution must securely connect disparate data and applications across a multitude of environments—from legacy to cloud to mobile, allowing you to unlock the value of your legacy systems and use your enterprise data with today's modern endpoints endpoints to meet customer expectations.

worldwide data will grow

61%

to 175 zettabytes

30%

of this data will be consumed in real-time

1. Frost & Sullivan: The Global State of Online Digital Trust, August 2018.

How to Reign in Your Privileged Users?

Cybercrime continues to rise with reported data breaches increasing by 75 percent over the past two years[1]. Many data breaches and insider attacks exploit privileged accounts or credentials. This is not surprising when one considers that privileged accounts have unrestricted access to the most sensitive data in your environment; they literally hold the keys to the kingdom.

Thankfully, there is a positive angle you can take. If privileged accounts are the common thread amongst innumerable attack types, then these accounts—and the credentials associated with them—are exactly where many organizations are focusing their protection efforts. But is this enough?

Governing your privileged users

Organizations have recognized the dangers of privileged accounts and are focusing their protection efforts in this area, but still many are failing to manage and govern privileged users on an ongoing basis.

A modern IAM solution must disrupts the kill chain by enforcing controls over users, accounts, and systems that have elevated or "privileged" entitlements, which protects against data breaches and builds trust and loyalty with customers.

[1] Information Age: Data Breach Reports Increase Last Two Years, September 2018

How to automate threat responses?

Perhaps the most frightening thing about the oncoming storm is the resources available to combat it. In their annual survey, the **Enterprise Security Group** found that "53 percent of respondents reported a problematic shortage of cybersecurity skills at their organization, and IT architecture/planning skills came in second at 38 percent".

With the predicted explosion in connected devices and data, and increased interactions between the two, security teams that are already understaffed will soon be overwhelmed. Current security models are built around point solutions that leverage static rules that generate alerts and rely on manual inspection. How can these teams hope to cope when the number of alerts expands exponentially?

Leveraging AI to Automate Security Mitigation

Automation and powerful AI are the key to solving this challenge and help enterprises detect and stop hackers and malicious insiders before they cause damage.

A modern IAM solution must provide continuously, intelligent monitoring capability that analyzes the access and activity, accurately detects suspicious and risky behavior and automatically triggers mitigating controls to limit damage to the enterprise. It must also tie into an Integrated Cyber Defense Platform so that data can be shared across attack vectors.

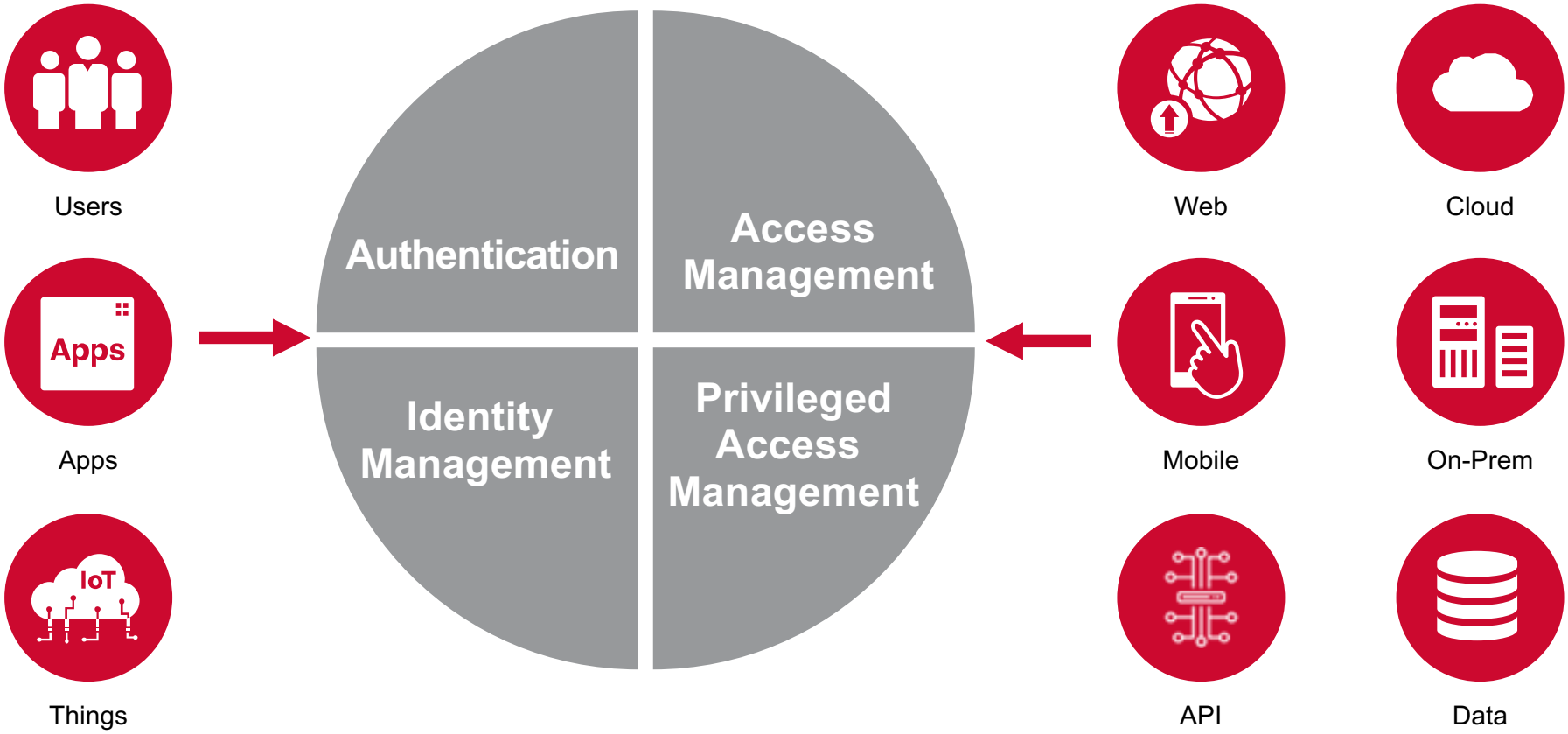
53%

of respondents reported a problematic shortage of cybersecurity skills at their organization

38%

IT architecture/planning skills came in second

Introducing Symantec Identity Security



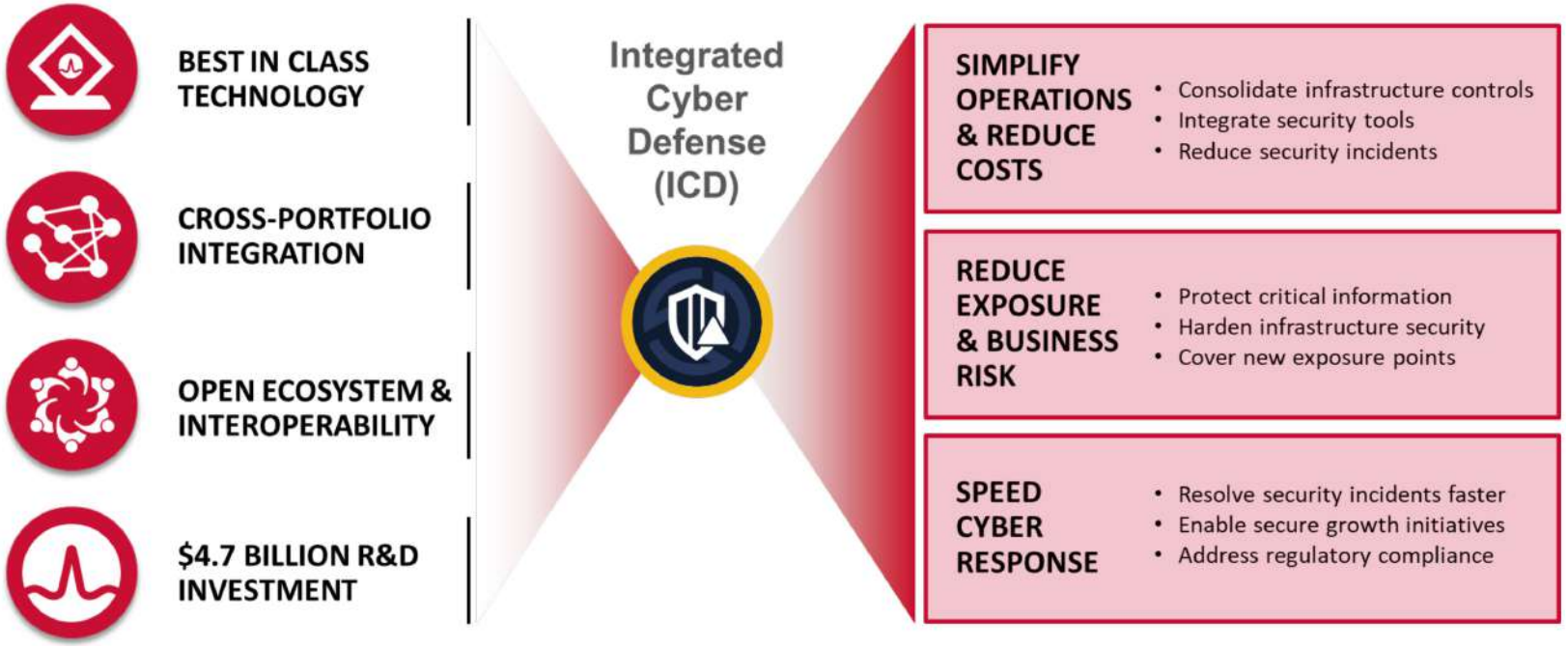
Transform
Enable the right people with the right access to the resources with IAM microservices

Secure
Protect and manage identities and their access to data across the hybrid environment

Simplify
Reduce cost of operations with scalability and automation for modern enterprise architectures

The Symantec Difference

In today's world, where breaches are the norm, information is everywhere, and personalized experiences drive digital transformation, Identity is the foundation of trust in a zero-trust online world. But, Identity is just one factor in your overall security strategy-you need an Integrated Cyber Defense Platform.



Symantec™
A Division of Broadcom

For product information please visit our website at: broadcom.com/symantec-iam

BC-0545EN-0120 January, 2020