Modernize your identity security strategy

by One Identity

Silos and Sprawl

Most of the challenges we face with identity security arise from the diversity of the systems to which access and permissions must be controlled, the complexity of managing disparate solutions and platforms, and the shifting of users and the ever-evolving ways in which they access those systems.

Every time a system is introduced, we face a decision on how to secure access to that system. Do we approach it as a stand-alone system or as part of a unified whole that includes all critical assets and systems?

Often because systems are siloed from one another – and so is the identity data for each user and action. With so many systems making up the modern enterprise, you end up with identity sprawl.

In a recent survey, nearly all respondents (95%) reported they had challenges managing identities, over 50 percent of large organizations are trying to manage more than 25 separate silos of access data, and 1 in 5 said they manage over 100 separate silos of data. That's too much and too risky.

But we can't throw out existing systems simply because the new investment doesn't work well with them. So, we're left doing the best we can with existing processes, but often that isn't enough.

Risk doesn't go away simply because we're trying hard. Compliance requirements don't rest because we have the best intentions. And users don't forgive inefficiency simply because systems don't work well with each other.

No one can afford to wait for the future to arrive before making critical **identity security enhancements.**

95%

Of respondents reported they had challenges managing identities.

50%

of large organizations are trying to manage more than 25 separate silos of access data.

The unified approach to identity security

One Identity's cloud-first approach to product development is based on five fundamentals that build into our identity security portfolio.

1. Invest in simplicity

One of the foundational concepts of the One Identity family of solutions is a modular and integrated approach that ensures that each identity security solution can stand on its own, and the cumulative effect is greater than the sum of its parts.

"One Identity" connotes the concept of simplicity. It helps you to get to one set of policies, one set of access controls, and one set of rights to audit. Removing the need to define new identities or controls every time a system or a access scenario is introduced to your enterprise brings simplicity to your organization, helps to control identity sprawl and strengthens cybersecurity.

2. Embrace open standards

Open standards allow for new functionality to flow into any organization, resulting in improved collaboration and interoperability, and a competitive edge. One Identity solutions draw upon the latest standards, while embracing the proven standards that form the foundation of identity security success.

This is true whether it's the myriad standards (Kerberos, LDAP, SAML, WS Federation, OAuth, OpenID Connect, etc.) that allow communication across diverse systems, or the specialized standards (for example PAM, NSS, and RADIUS) that enable specific functionality in specific systems and for specific use cases.

This means that One Identity's single sign-on solutions work across everything from the most modern federated application to legacy applications; or a multifactor authentication solution can be implemented across virtually any system or user population. With One t. Standards are the essence of flexible, modular and integrated identity security.

3. Think cloud first

One Identity solutions are flexible and adapt to needs as they evolve. One Identity embraces the concept of configuration as opposed to customization, open standards rather than closed systems, and long-term interoperability instead of solving the problem-of-the-day.

One Identity solutions provide the path to the next step in your **identity security evolution.**

For example, automating and securing enterprise provisioning enables you to address governance needs, without additional investment. Overcoming the management and security challenges of Active Directory with One Identity solutions expands control to non-Windows systems with the simple addition of an AD bridge; addressing federation needs for the latest SaaS application automatically can solve the single sign-on needs for legacy applications, the need for secure remote access, and the emerging requirement to deliver context-aware security – all from the same solution.

4. Build end-to-end security

Unified identity security allows organizations to protect the people, data and applications essential to them. But you don't adopt new technologies just because they are new – you adopt them because they accelerate and support your business objectives.

The technologies themselves are great and help you reach business objectives, but the security those technologies require (if done the wrong way) can counteract any gains that drove the decision to adopt.

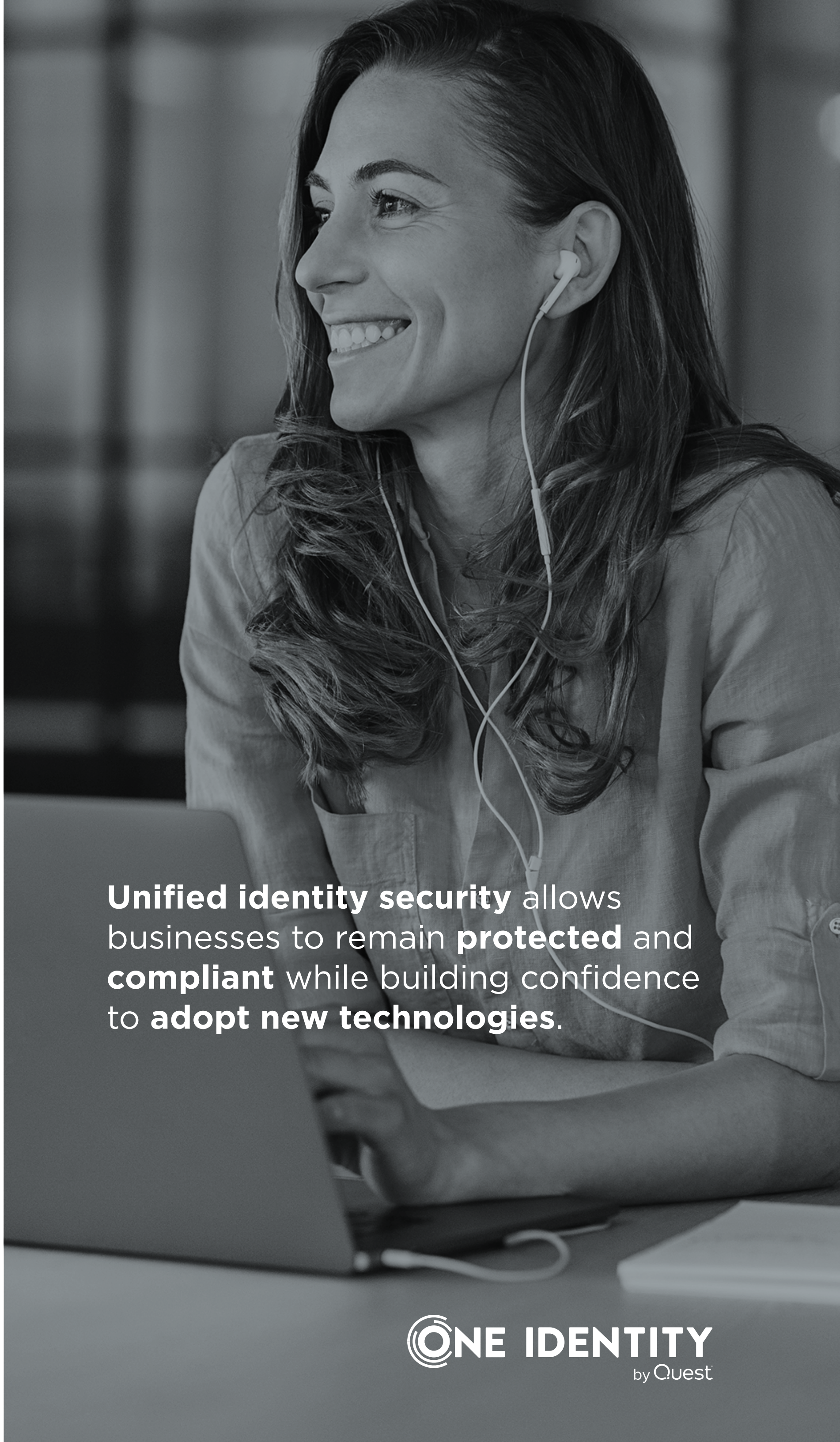
Similarly, a typical identity security deployment addresses provisioning first and then adds governance after, with an entirely different solution from an entirely different vendor, along with all the integration headaches and retro-fitting that prevent future-readiness. The same can be said for privileged access management (PAM). Implementing one type of solution (lets' say a Unix root delegation solution) from one vendor and another (perhaps a privilege safe) from another, can lead to incompatibilities and less-than-optimal functionality.

However, One Identity solutions extend the end-to-end security concept into the realm of identity security. Provisioning and governance are tightly linked. That governance is broad, covering user access, data access, and privileged access, privileged access management is about all the use-cases—not just the ones we like, and authentication covers all the bases including the ones you haven't needed… yet.

5. Modernize and automate

Modern systems save money, enable differentiation and automate manual processes.

Even more than poor technology choices, poor operational choices are the biggest barrier to effective identity security. A heavy reliance



Unified identity security allows businesses to remain **protected** and **compliant** while building confidence to **adopt new technologies**.

on IT—with its accompanying glut of manual processes, tribal knowledge, and doing the best you can with what you have, can derail even the most well-meaning identity security project. But often decisions are forced on us by the technologies we choose.

One Identity solutions are designed to eliminate manual processes, which frees up your IT staff to focus on more critical tasks. Our unified identity security platform delivers visibility and puts decision-making power in the hands of the right people – not just the people that know how to use the tools. That means that provisioning can be run by the line-of-business personnel that know who should access what. This capability extends to governance activities, which suddenly become quick and easy exercises for the line-of business, not time-consuming requests between an overworked IT staff and the rest of an organization.

Learn more

For more information visit www.oneidentity.com

Remember:

1.
INVEST
in simplicity

2.
EMBRACE
open standards

3.
THINK
software first

4.
BUILD
end-to-end security
(or identity security)

5.
MODERNIZE
and AUTOMATE

About One Identity

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Our Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Identity and Access Management (IAM), Privileged Access Management (PAM) and Active Directory Management and Security (ADMS) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale – managing more than 250 million identities for more than 5,000 organizations worldwide. For more information, visit www.oneidentity.com.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

ONE IDENTITY
by Quest