Business at the Speed of Trust

How identity and access management drives innovation, agility, and security

There are many barriers to business innovation. One that is often overlooked is the lack of trust between new and old parts of the IT ecosystem. To drive agility and reduce costs, a framework of trust is an essential element of every digital transformation.

The Hidden Constraint

Our entire social fabric is built on trust. Where there is trust in character and competence, progress is accelerated. Where there is lack of trust, progress is slow, expensive, unreliable, and frustrating. Just as a chain is only as strong as its weakest link, a business process is only as fast as its slowest step. The lack of trust among different parts of a business process can create bottlenecks, slowing progress and innovation.

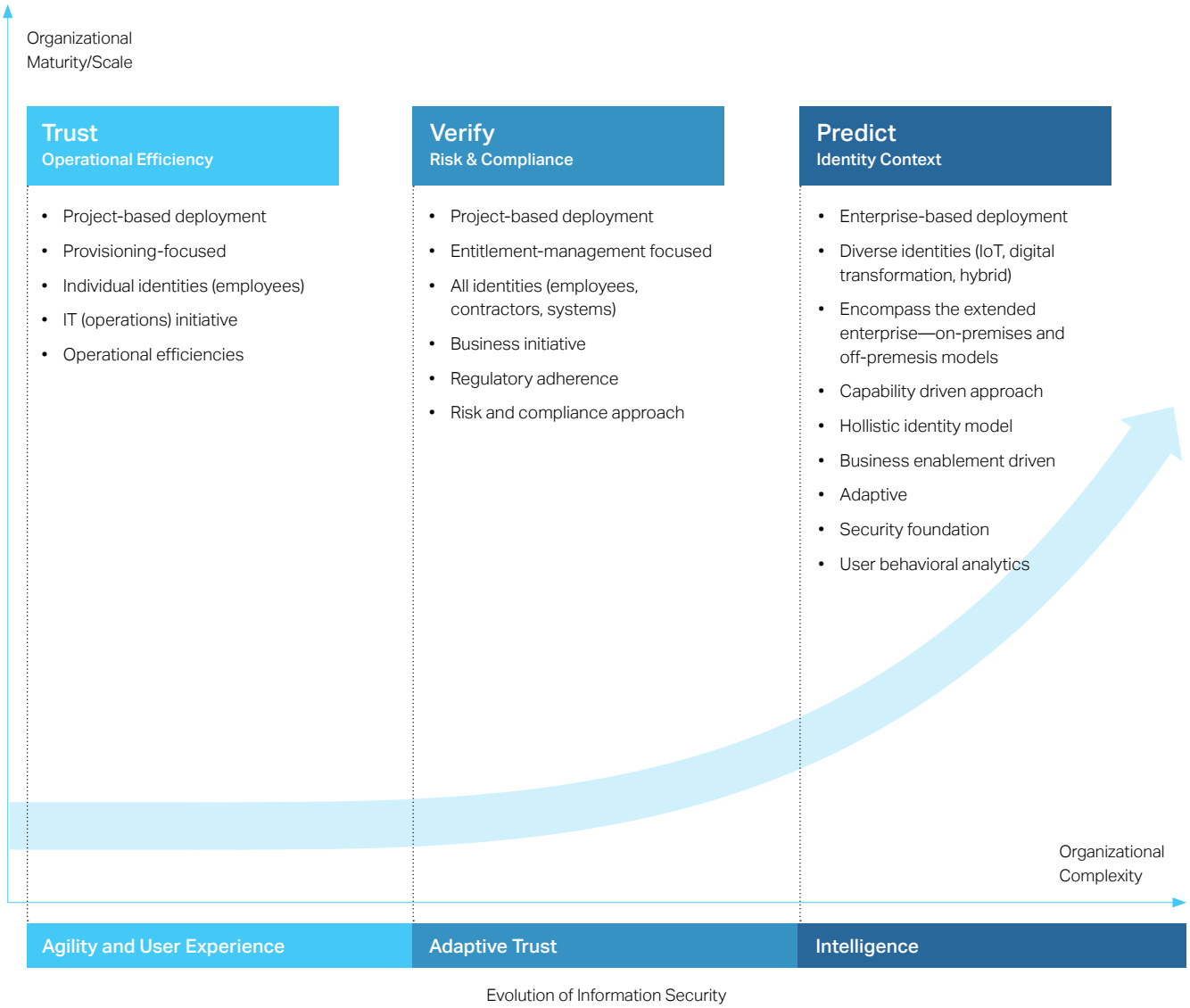
This situation also occurs in IT. The misalignment and lack of connection between the islands of systems in an IT landscape can cause extra work for the users and custodians of these systems. This slows the pace of innovation and increases the risk of innovation failure. A great example of this is the lack of trust between islands of identity data. Not only is this expensive, but it denies business and IT operations teams the ability to scale up and increase agility through policy (or automation) tools. This lack of identity trust is a key hidden constraint to innovation.

Businesses typically respond to these problems by creating "shadow IT." To deal with these islands of shadow IT, many organizations create simple, script-based provisioning actions to keep them in sync. These solutions offer short-term, local benefits, but they magnify the problem in the long-term by introducing greater complexity. Point solutions typically fail to handle multiple sources of truth and handle failures poorly. De-provisioning of identities and consent is also usually forgotten. The results are orphaned accounts and access creep. Inaccurate identity data causes user frustration, policy violations, and even fines that can result in lost sales, rework, and complaints.

Lack of identity trust is a key hidden constraint to innovation.

Building Digital Trust

A key step to resolving the challenge of complexity and lack of trust is to centrally manage identities and access. Implementing a common, synchronized identity and access model across the landscape of applications and data—or IT



Evolution of Information Security

islands—creates a framework of digital trust. This identity-powered framework is the foundation for improved user experiences, security, and analytics.

An essential part of implementing a central identity and access model is the inclusion of verification. The proverb "Trust, but verify" offers a reliable approach. Until recently, the expense and friction of effective verification has been prohibitive. However, the proliferation of sophisticated cyberthreats and affordable technology has led to the rise of adaptive trust models such as "Zero Trust." The aim of these models is to deliver the right amount of verified trust through event-driven, policy-based risk scoring and controls.

A powerful benefit of a centralized identity and access model is the ability to deliver adaptive experiences. Adaptive experiences—based on identity attributes and context—are at the heart of an effective digital transformation program. They are also a powerful tool to eliminate the duplication that arises from shadow IT. The adoption of federation protocols (SAML), which allow for identity and context attributes to be passed seamlessly to applications, is accelerating the adoption of adaptive experiences.

The centralized identity and access model also allows for an identity-centric event stream that can be mined for value. For example, it can be used for risk avoidance through behavioral analytics or for opportunity mining through data mining. There are many use cases that can take advantage of this: information theft, fraud, affinity or loyalty programs, and others.

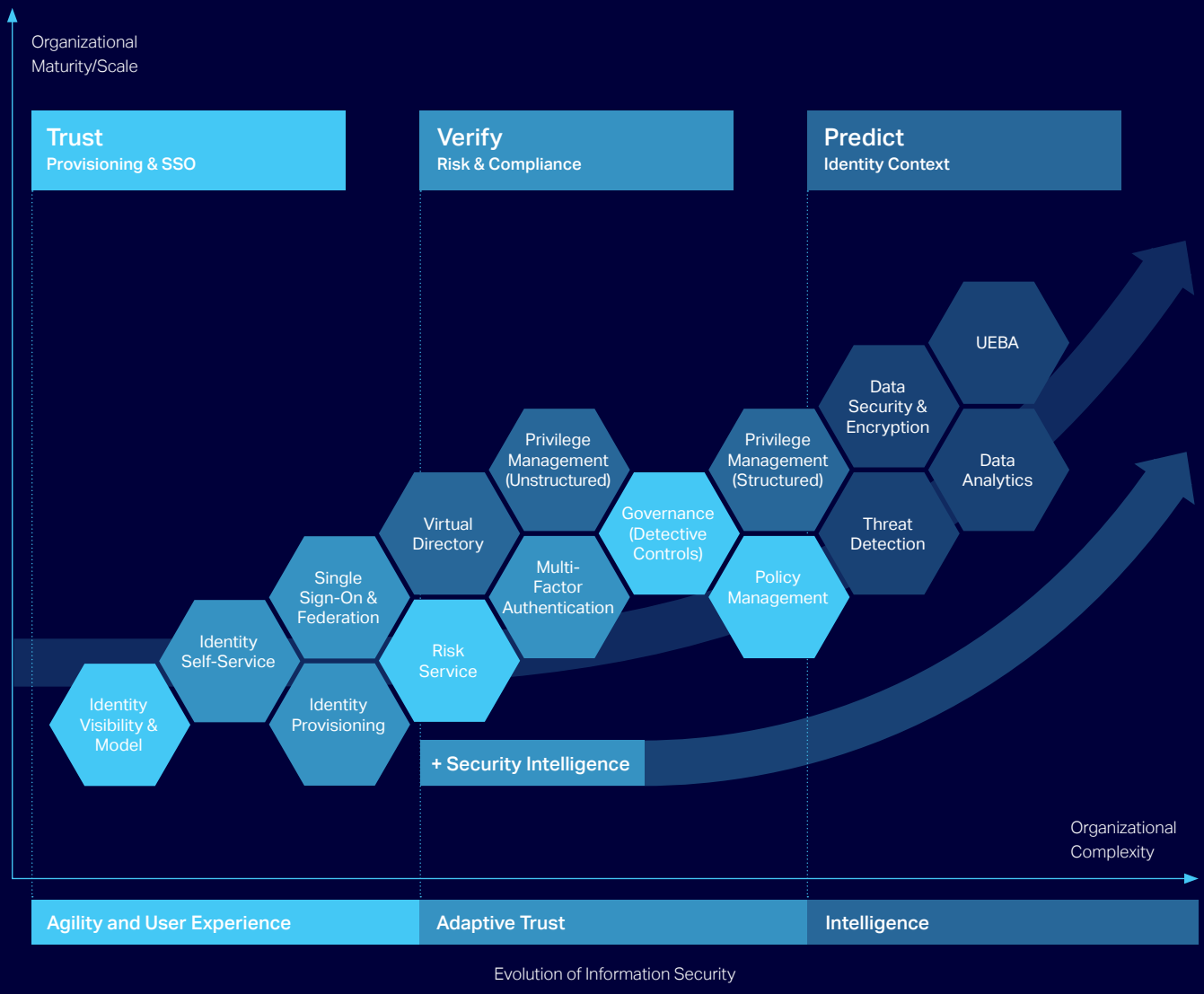
Implementing a Central Identity Model

The journey to a central identity and access model is typically triggered by a failure, large or small. It often starts in the operations side of the business. Due to legislation, it might also be motivated by risk or compliance issues. The diagram above shows where to look for initiatives so that they can be knit together into a cohesive strategy, as opposed to using point solutions.

Steps to a Central Identity Model

Often the challenges of creating a central identity and access model is considered too big and confusing to solve. Sometimes organizations play "pass the parcel" because nobody wants to accept the risk of owning the overwhelming identity challenge.

Breaking down the process into smaller, more manageable chunks enables organizations to start realizing the benefits that align with immediate business objectives, while setting the stage for long-term IT agility, security, and analytics. The diagram below shows the fundamental building blocks of a typical journey toward establishing a central identity and access model.



Learn More

Learn more about how a central identity and access model can increase trust in your business at **microfocus.com.**

© 2020 Micro Focus