IBM Security Verify, First Step to Zero Trust

Whether preserving client privacy, protecting a hybrid cloud, reducing the risk of insider threats, or securing a hybrid workforce, identity and access management is your first line of defense…start there

Charles H. Green, renowned trust expert and author likes to say, "I trust my dog with my life, but not with my ham sandwich." Sounds like he's drawing a thick red line there. Where do you draw the thick red line regarding digital trust for your company, your organization? We're guessing it's closer to the life end of the spectrum than the ham sandwich end. Today, lives, livelihoods, and privacy all depend on the establishment and maintenance of digital trust. As security, privacy, IT, development, even LOB leaders, we pledge to protect our workforce, customers, and constituents, and the data and applications they depend on.

And yet, we are challenged every day with new attacks on the very people and valuables that we've pledged to protect. What's the answer? At IBM Security, our recommendation is a Zero Trust approach, and the first step is to focus on identity and access management (IAM.) In this paper, we'll examine the specific IAM capabilities in the *IBM Security Verify* family that support a Zero Trust approach.

Highlights

- First: establish identity and access governance policy
- Next: balance between security and ease-of-use
- Fight the favorite inside hack: privileged access
- Look after your workforce, consumers, and bottom line

First: establish identity and access governance policy

Many businesses and organizations are operating at scary heights regarding identity and access. According to the Verizon 2021 Data Breach Investigations Report[1] credentials are the primary means by which a bad actor hacks into an organization, and 70% of users have more access privileges than are required. They are over-entitled. This can open organizations up to compliance failures as well.

Today's hybrid IT environments can make it challenging to enforce consistent Zero Trust identity governance policies across the enterprise. IBM Security Verify Governance solutions enable risk-aware, extensible identity and access governance across on-premises and hybrid cloud environments.

IBM's Security Verify Governance solutions manage a user identity throughout the workforce lifecycle, and establish and enforce rules for access, to ensure the right person has the right access at the right time. Plus, the IBM solution differs from other offerings.

The big difference is in how IBM approaches separation-of-duties (SoD) using business-activity modeling instead of the inflexible role-based modeling that others use. SoD helps prevent conflicts of interest, wrongful acts, fraud, abuse, and errors. It's designed to ensure that individuals don't have conflicting responsibilities. Most vendors model SoD through a role-based approach. This older, role-based approach only tells us that where the access comes from determines the risk. The problem with that is the impermanent nature of roles makes it extremely difficult to model risk policies and specifically SoD.

[1] Verizon 2021 Data Breach Investigations Report

Another unique feature are the advanced provisioning policies, fine grained at the attribute level for maximum flexibility. There is also advanced role-mining and SoD analysis capabilities with visualization and change control, that can help organizations to improve operational efficiency.

There are several deployment choices with on-prem, private cloud, public cloud, hybrid, or delivered from cloud. And finally, Verify Governance is part of the larger IBM Verify ecosystem.

Next: balance between security and ease-of-use

What does modern, effective access management look like? The answer shouldn't surprise you. Access management is a strategy, almost a philosophy, that's always seeking a balance between security and ease-of-use. Today, that depends on requisite technologies:

- *Single Sign On* - authentication that enables a log in with a single ID and password to any of several independent software systems
- *Advanced Authentication* - using real-world identity signals to provide significantly stronger verification for information and system security
- *Adaptive Access* - context-aware access control that balances the level of trust against risk

Avoid multiple IDs and passwords: single sign on

IBM Security Verify provides several capabilities around single sign on (SSO) including most of the common authentication languages, protocols, standards and technology, the ability to support multiple user scenarios, bridging to on-prem access and directories, and integrating with various endpoint management solutions.

IBM Security Verify provides SSO and access management for cloud and on-prem apps, including:

- Legacy and modern authentication languages, protocols, and standards
- HTTP headers and cookies
- User launchpads, registration, and profile management
- Attribute management
- Bridge-services for on-prem directories
- On-prem app access with a lightweight app gateway
- Endpoint management integration
- Delegate app administration to line of business
- Data privacy and consent management

Make “stronger” easier: advanced authentication

For more advanced authentication capabilities, IBM Security Verify provides support for multi-factor authentication (MFA) the ability to utilize QR codes and FIDO2 authentication, authenticating from email, SMS, voice, TOTP, push, face, and fingerprint, and several passwordless methods.

IBM Security Verify provides additional security for cloud and on-prem apps including developer-focused APIs and a resource portal for identity and authentication. Plus, you can enforce access policies to require MFA based on how the app is accessed (mobile, desktop, or new device.) Or extend MFA to VPN RADIUS, Linux, Windows RDP.

Authorize based on context: adaptive access

Our adaptive access capability is based on machine-learning, taking multiple context inputs, and providing a confidence score for whether an individual should be authenticated.

Context, in this case, could include real-time adjustments to access based on risk level, biometrics, keyboard and mouse movements, travel patterns, or enhanced device fingerprinting.

Once you've implemented adaptive access, IBM Security Verify provides continuous evaluation of user risk, applying machine learning for higher accuracy.

Fight the favorite inside hack: privileged access

Privileged users have complete access to your IT infrastructure. This unrestricted access makes privileged accounts extremely sought-after. Privilege misuse is the top category of security incidents and the third most common method used in data breaches. Through phishing scams or malware, hackers will steal privileged credentials and gain entry to the infrastructure completely undetected, wreaking havoc on the most critical systems and data.

Controlling and monitoring privileged user access is the best way to prevent attacks. First, you need to know who and where the privileged accounts are. *IBM Security Verify Privilege Vault* enables you to discover, manage, protect, and audit privileged accounts across your organization.

In a Zero Trust approach, you need to adopt a "least privilege" posture, enabling the exact access required only to who needs it when they need it. *IBM Security Verify Privilege Manager* enables you to enforce least privilege and application rights on all endpoints.

Look after your workforce, consumers, and bottom line

Overall, both workforce and consumer identity and access management have quite different frameworks, yet a shared technology solution like IBM Security Verify can help accelerate progress toward both implementations. For example, traditional

identity and access management (IAM) product development brings with it a swath of protections, including the integration of advanced fraud detection capabilities and risk-based authentication that fuels zero trust initiatives.

These same capabilities can be applied in a different way to verify the identities of genuine consumers and keep MFA rates as low as possible to preserve a simple user experience. Meanwhile, Consumer Identity and Access Management (CIAM) use-cases inspire broad authentication options, and developer-centric workflows that can still be applied toward workforce identity use cases to modernize employee experiences and increase time-to-value for developers who are focused on custom internal apps.

In addition, organizations can experience licensing efficiencies when consolidating to a single solution for both internal and external users, while only being charged for actual usage.

And why drive your access management in the cloud? There are several advantages.

Here are a few: it’s more agile, faster, and usually lower in cost, which paves the way for going-to-market faster. It’s scalable, enabling expansion, and reduction as you need it. It’s easier to protect your technology investments by letting someone else go through the update cycles, and if you're currently working from an on-prem model, you don’t have to lift and shift everything to the cloud at once. You can transition in phases, and we can help.

Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit www.ibm.com/security.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

For more information

To learn more about IBM Zero Trust, please contact your IBM representative or IBM Business Partner, or visit the following websites: https://www.ibm.com/security/zero-trust or, https://www.ibm.com/security/services/zero-trust-acceleration