

Partner acceleration guide for IBM Security Verify

April 2021

Dear business partner,

Whether organizations are modernizing internal infrastructure or consumer-facing websites and mobile apps, IBM Security Verify helps them navigate their digital transformation.

To accelerate your sales and marketing efforts, we have created the partner acceleration guide. This guide was expressly developed to help you to build a successful identity and access management business with Verify.

This simple, easy-to-follow guide provides the full value proposition for our partners to add Verify into their portfolios, including market opportunity; solution description; client challenges and use cases; your investment required to build a practice; how to make money; and key enablement resources.

Here's to great outcomes and explosive growth throughout the year! Please let us know if there is anything else we can do to support your success.

We thank you for your partnership with IBM.



Mary O'Brien
General Manager, IBM Security



David La Rose
General Manager, IBM Partner Ecosystem



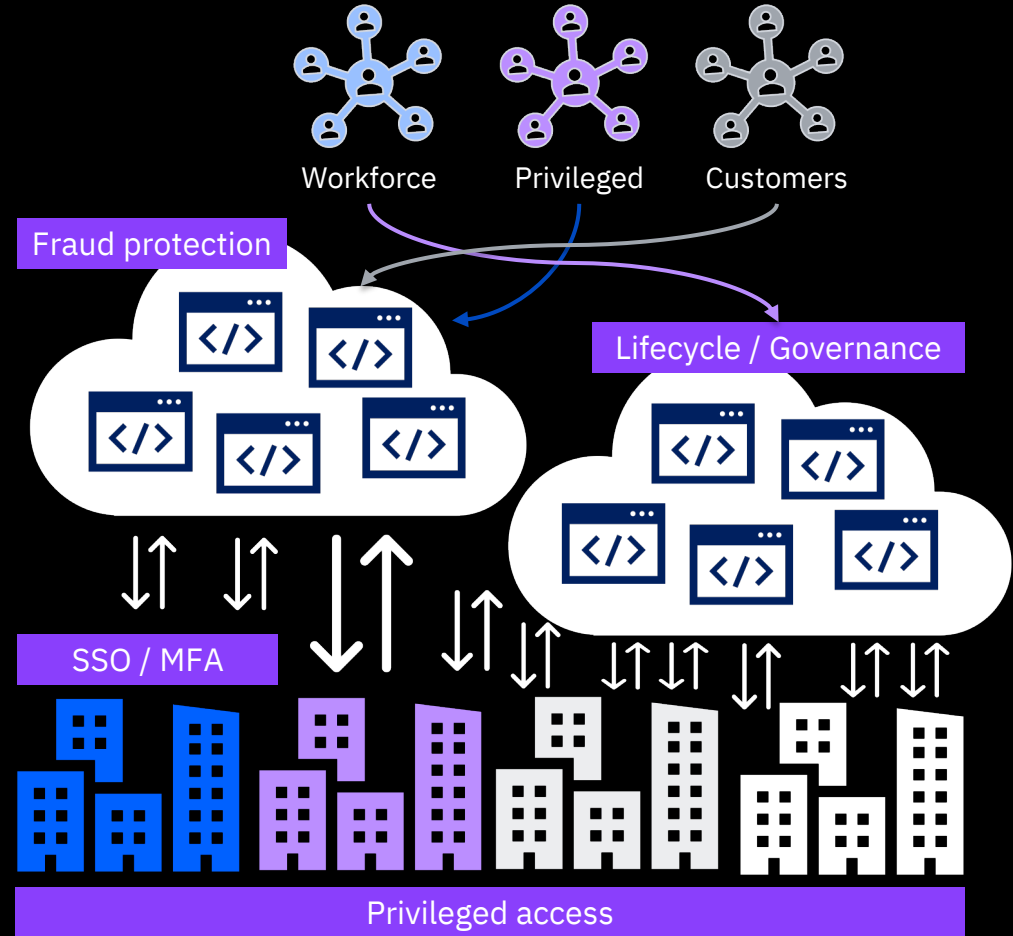
Table of contents

<u>Market landscape</u>	04
<u>Client challenges and solutions</u>	07
<u>What is IBM Security Verify?</u>	10
<u>Verify differentiators</u>	17
<u>Verify free edition</u>	18
<u>Demand generation for Verify</u>	19
<u>Your investment</u>	20
<u>ROI examples</u>	21
<u>Go-to-market resources</u>	23
<u>Demand generation tools</u>	24
<u>External client references</u>	25

Market landscape

Fragmented experiences and solutions across organizations

Different vendors,
different use cases,
different skill sets



Market landscape

21.1%

CAGR is expected for the identity-as-a-service (IDaaS) market, growing from \$2.5B in 2019 to \$6.5B in 2024.

Market landscape

Pillars of smart access management



Contextual for Zero Trust

Full user, device, and environmental context



Consumable for any use case

Securely connect any user to any resource



Comprehensive portfolio

Maintain existing infrastructure while scaling for the future



Client pain point #1

Problem

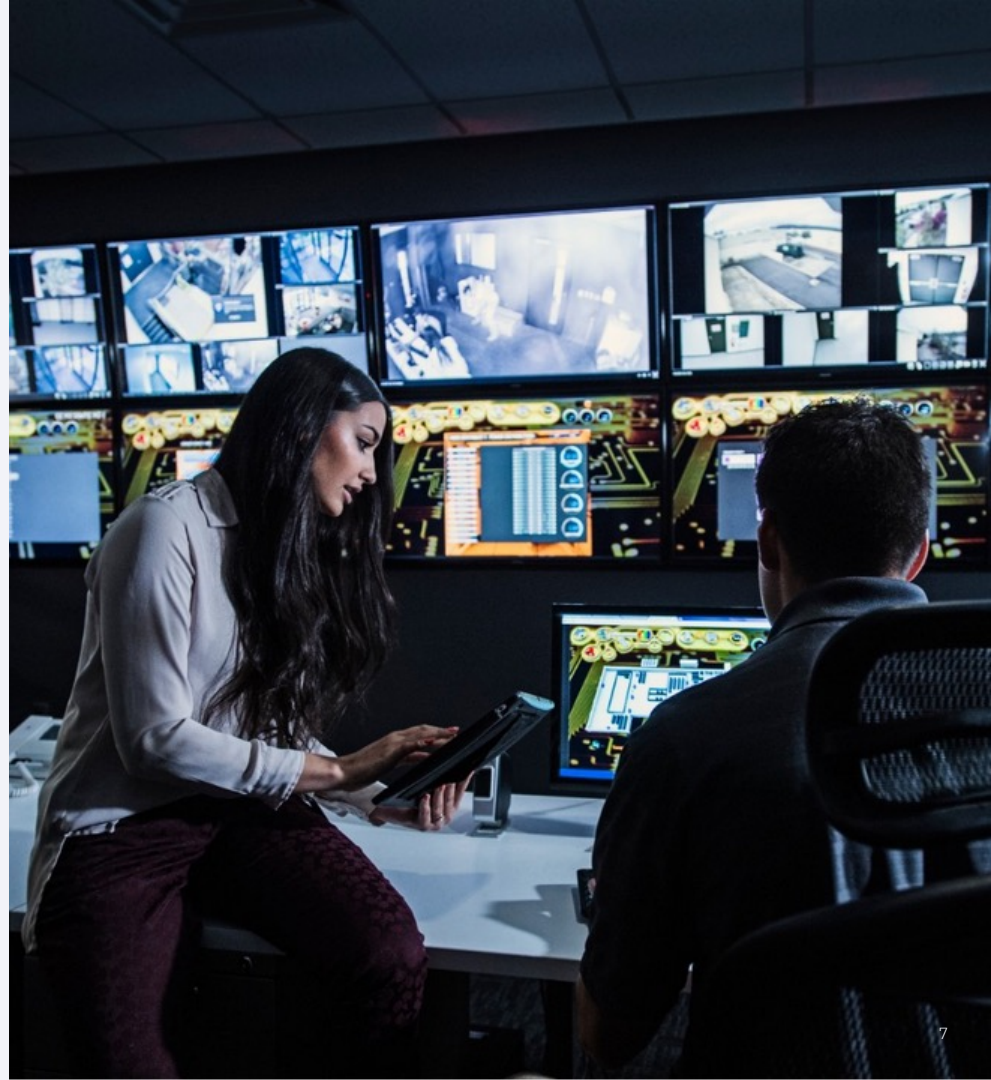
I can't move to cloud all at once

- Need to keep legacy on-premises infrastructure live for foreseeable future
- Getting pressure for digital transformation and journey to cloud initiatives

Solution

Hybrid identity and access management

- Cost-effective deployment strategy to modernize legacy apps
- Use on-prem and cloud IAM solutions simultaneously
- SaaS connects to on-prem to enable a gradual migration at a comfortable pace



Client pain point #2

Problem

Security and user experience are a tradeoff

- Inability to ensure easy access to valid users
- Still need to challenge access with suspicious users
- At all costs, must prevent a data breach

Solution

Make access adaptive

- Allow frictionless access to low-risk users while protecting against higher risk scenarios
- Continuously evaluate holistic risk context across user, device, activity, behavior and environment
- Leverage purpose-built fraud detection engine maintained by IBM Security



Client pain point #3

Problem

My access management solutions are siloed

- Multiple systems and directories that don't "talk"
- Don't know how to approach custom integrations
- IAM separate from other security systems

Solution

Integrated by design

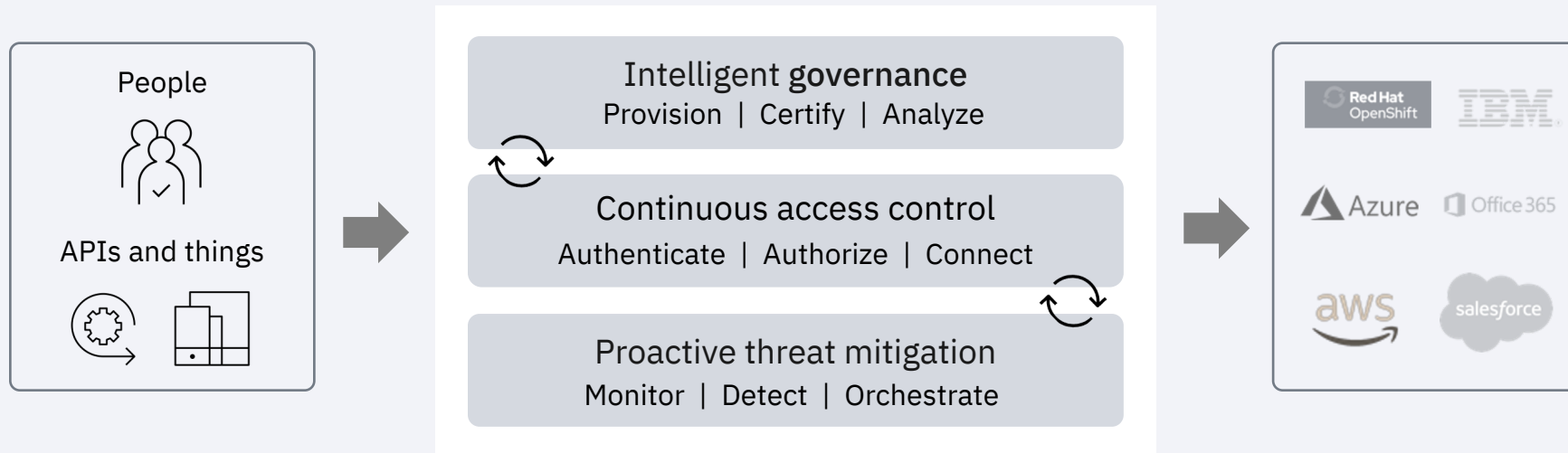
- Use a universal directory to consolidate historical info
- Maintain a centralized management system
- Integrate natively with unified endpoint management, threat management and incident response systems



What is IBM Security Verify?

Our vision: smart identity for the hybrid multicloud world

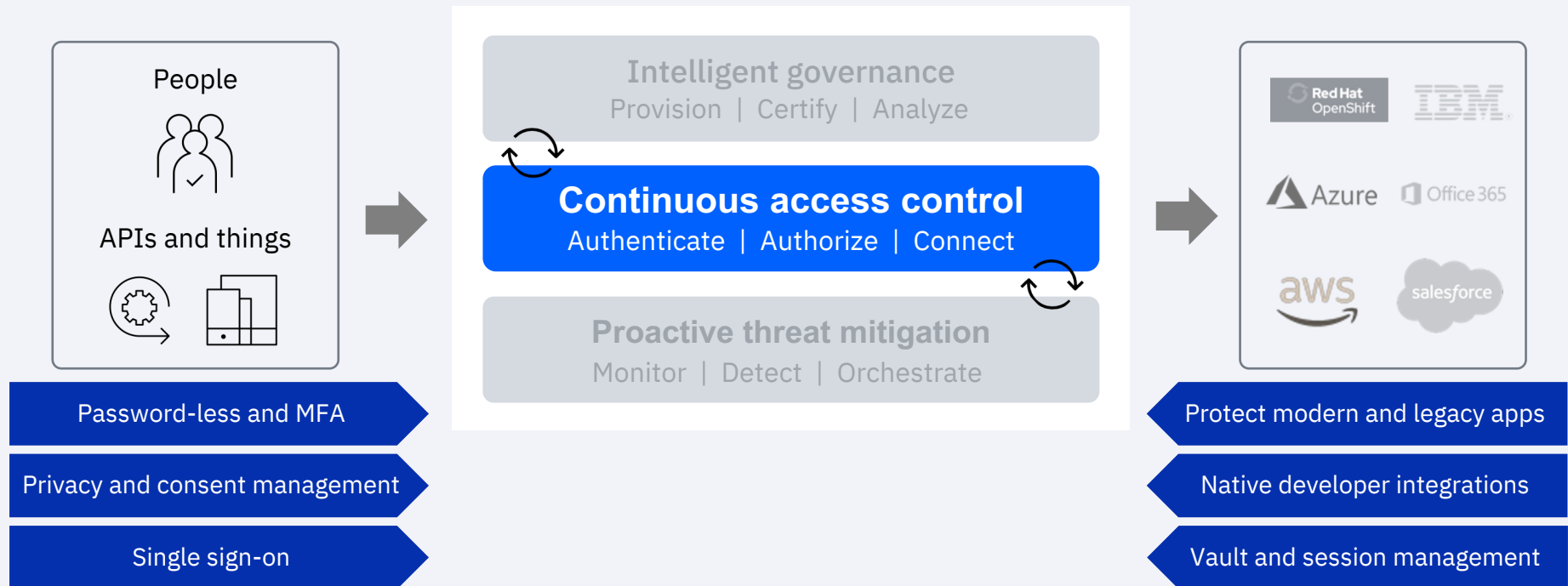
Modular identity platform that runs anywhere, and adaptively governs and connects all users, APIs, and devices to any application or service running inside or outside of the enterprise



What is IBM Security Verify?

Continuous access control

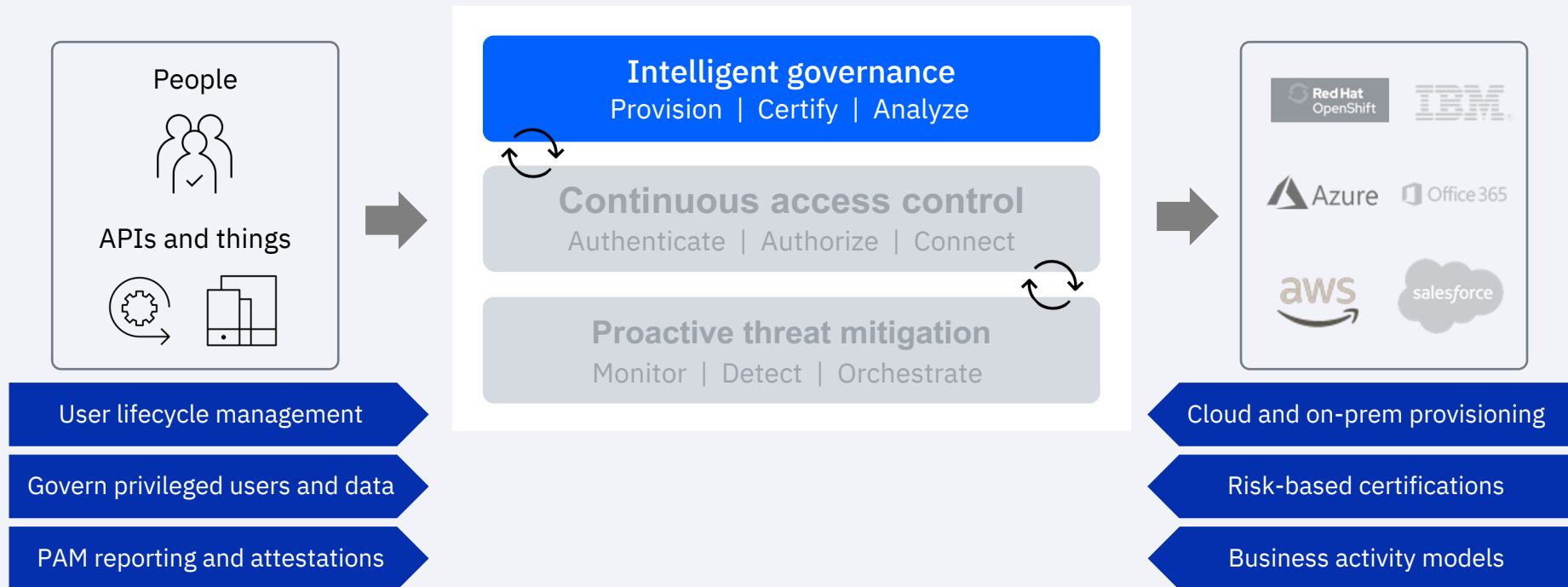
Adaptively enforce authentication and authorization policies, while delivering a frictionless experience for consumers, workforce, and privileged users



What is IBM Security Verify?

Intelligent governance

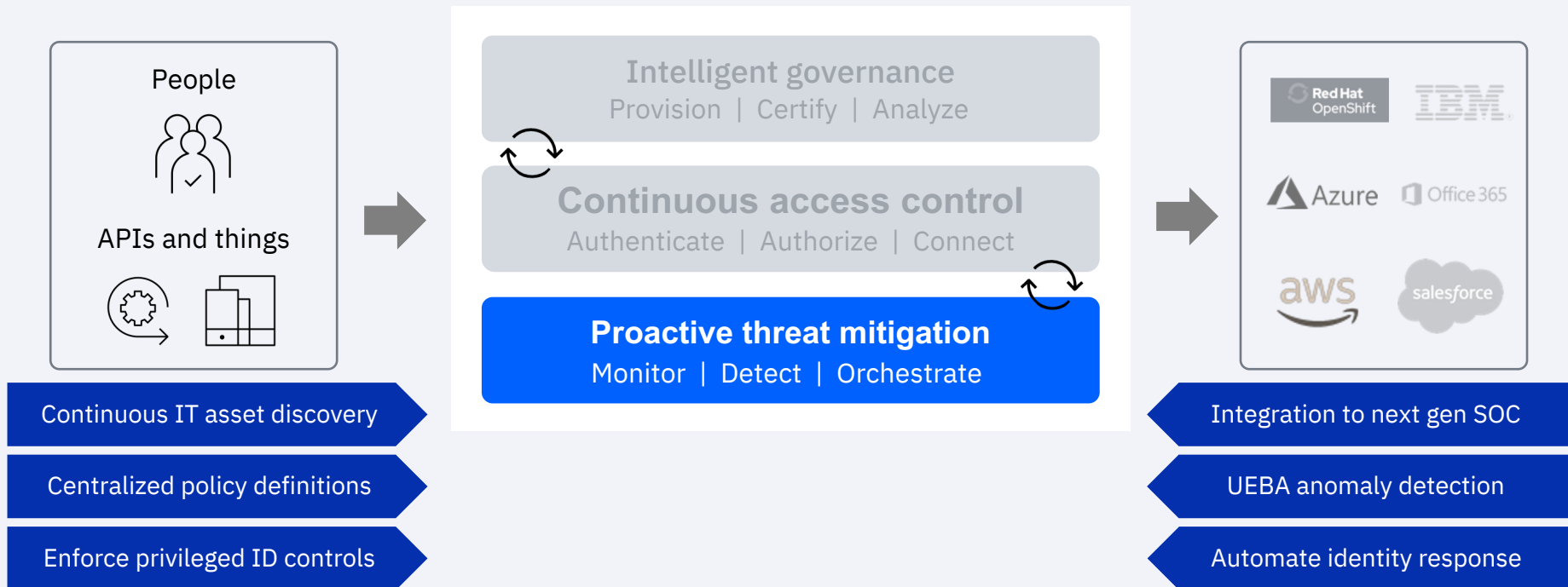
Govern all digital identities, from business to privileged users, with risk-aware compliance and actionable intelligence



What is IBM Security Verify?

Proactive threat mitigation

Integrate identity into the broader security ecosystem in order to more effectively adapt to emerging internal and external threats

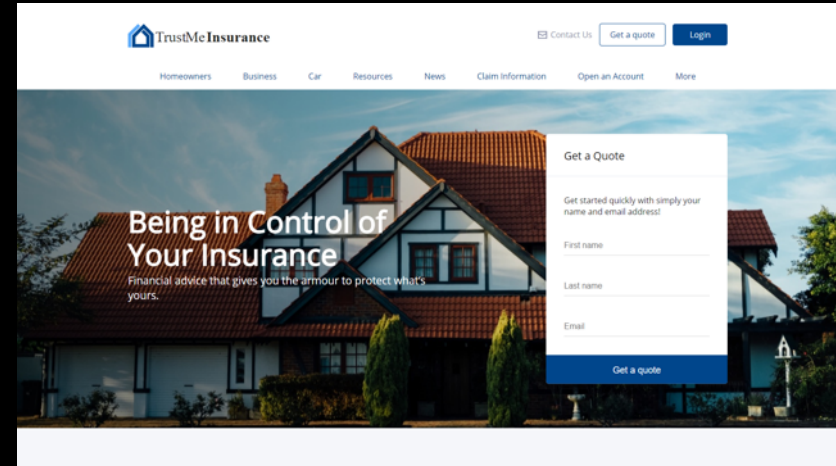
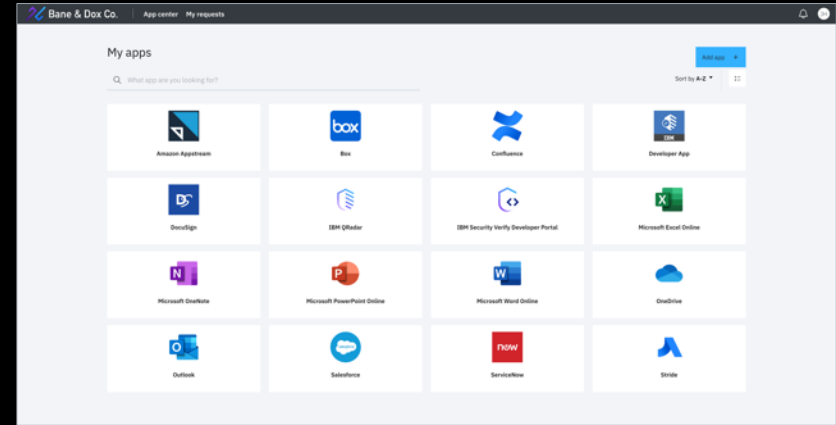


What is IBM Security Verify?

Client value

Digital Transformation for workforce and consumers—provides identity-as-a-service that scales for external users, including SSO, risk-based MFA and adaptive access, and privacy and consent management.

- Enable business agility and operational efficiencies; organizations have seen **619% ROI and payback in <6 months***
- Infuse identity as a central pillar of a zero trust strategy
- Modernized, modular IAM platform with AI-powered and risk-based authentication
- Help organizations establish and maintain trust with their customers by supporting the delivery of seamless omnichannel experiences



What is IBM Security Verify?

2021 Strategy

Smart identity for the hybrid multi-cloud world

Consumers are demanding frictionless experiences, where security is assumed

Cloud has changed how enterprises must think about security

Consumer digital transformation



- Enable business growth through easily integrated **secure but seamless** user experiences while giving end users more control

Workforce modernization

- Modernize workforce IAM solutions with improved security, addressing identity risks, governing data and privileged user accounts and mainframe across **hybrid multi-cloud infrastructures**

What is IBM Security Verify?

IBM Security Verify SaaS—IBM IDaaS platform

Single sign-on (SSO)	Advanced authentication	Adaptive access	Identity governance	Identity analytics
SSO and access management for cloud and on-prem apps	Additional security for cloud and on-prem apps	Continuous evaluation of user risk applying ML for high accuracy	User lifecycle management and governance	IAM analytics providing 360° access risk view
<ul style="list-style-type: none">– Modern authentication<ul style="list-style-type: none">• SAML, OIDC, OAuth2– Legacy authentication– HTTP headers, cookies, LTPA– Easy application management– User launchpad– User profile management– Attribute management– Bridge services for on-prem directories– Maintain on-prem app access with lightweight app gateway– Endpoint management integration– Delegate app administration to line of business	<ul style="list-style-type: none">– Passwordless methods<ul style="list-style-type: none">• QR code and FIDO2– Multi-factor everywhere<ul style="list-style-type: none">• Email, SMS, voice, TOTP, push, face, fingerprint– Adaptive MFA and conditional access– Developer-focused APIs and resource portal for identity and authentication– Enforce access policies to require MFA based on how the app is accessed (mobile, desktop, new device)– Extend MFA to VPN RADIUS, Linux, Windows RDP	<ul style="list-style-type: none">– Realtime adjustment of risk level– Biometric analysis– Keyboard / mouse movements– Travel patterns– Enhanced device fingerprinting– Advanced policy editing	<ul style="list-style-type: none">– Request access to applications– OOTB SaaS applications for provisioning– On-premise provisioning bridge and active directory provisioning– SCIM 2.0 based custom provisioning adapter– Access Certification– Account Lifecycle management– Role based fine-grain entitlements– Audit events– Provisioning and governance reports– Hybrid IGA for Verify Governance	<ul style="list-style-type: none">– 360-degree view of access risks– User entitlements risk scores– OOTB support with Verify Governance– OOTB Risk policies– Help me decide to make approvals, recertification access easier for Verify Governance– External data sources integration– Custom risk policies– External remediations <div> OpenID </div>

Verify differentiators

Adaptive access

- AI-powered fraud engine evaluates deeper risk context than other vendors for risk-based authentication
- Brings digital identity trust and access management together for true adaptive access

Identity analytics

- Empowers predictive and autonomous risk mitigation with decision support
- Trend in IGA market; included in same SaaS environment as access management

Access recertification

- Only tool to offer automated campaigns for recertification to mitigate manual spreadsheet reviews and rubberstamp approvals
- Helps limit human error as organizations prioritize compliance initiatives

Application modernization

- Preserve SSO experiences to legacy and new applications via single IAM framework to reduce user experience disruption
- No cost, modern deployment options as clients move to cloud and protect on-prem applications for true hybrid cloud use cases

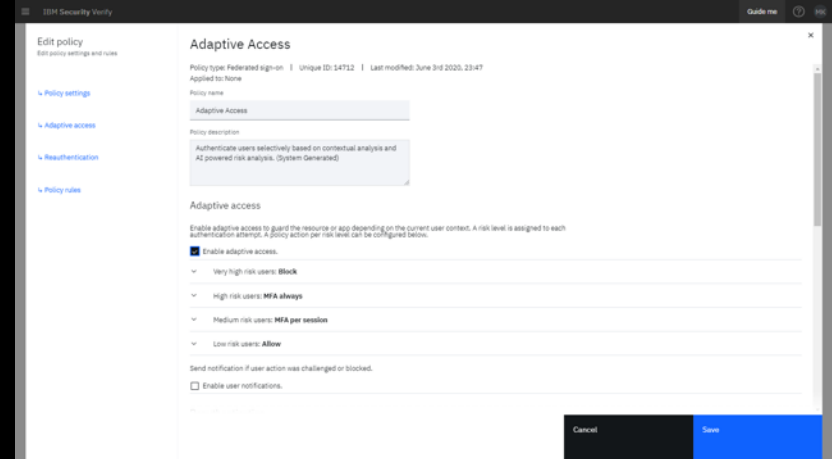
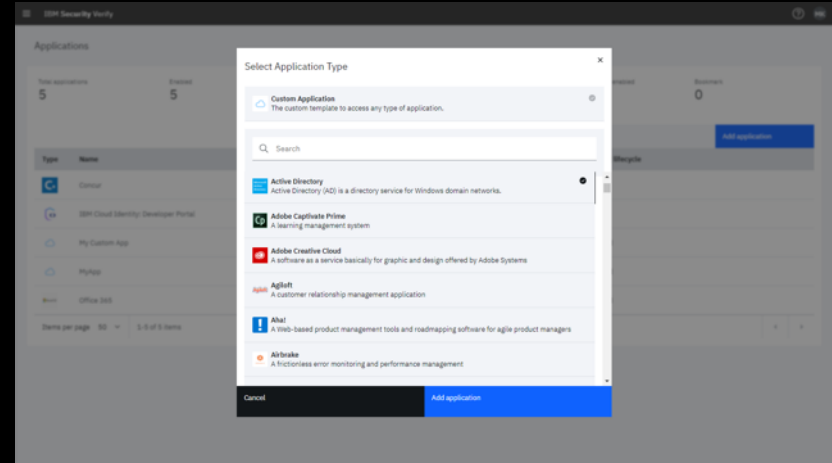


Sign up now Try free edition for yourself

Explore a trial of IBM Security Verify and get started in under 10 minutes:

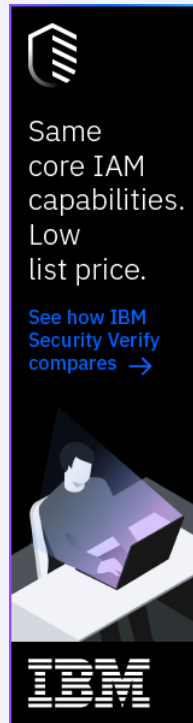
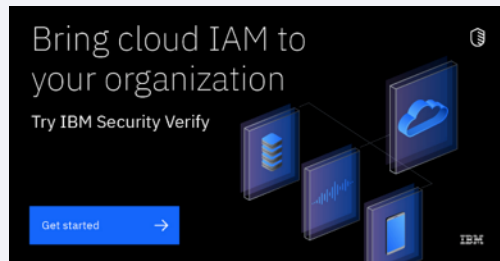
- Add apps to single sign-on
- Connect to a directory or add new users
- Try out MFA and adaptive access

Get started [here](#)



Demand generation for Verify

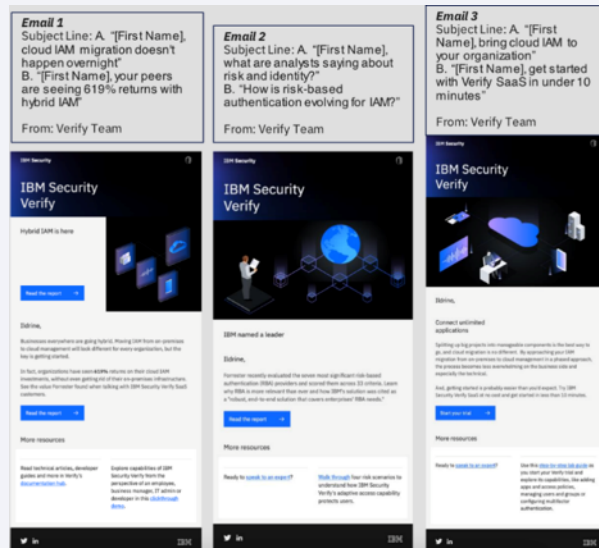
Paid social, paid search, competitive targeting, email nurture streams



Ad · https://www.ibm.com/ibm_ciam/solutions ▾

IBM CIAM - IBM CIAM Solutions

IBM Access Management Solutions & Services Protect and Secure Consumer Data. Explore now. Explore IBM Security Verify for Consumer IAM & Learn to Implement Core **CIAM** Capabilities. Engage Users with Trust. **CIAM** for Dummies eBook. Modernize User Journey.



Your investment

Get started quickly and grow as fast as your time investments allow

Sign-up, start learning, start selling

- Register for IBM PartnerWorld
- Sign-up for Seismic
- Sign-up for Verify SaaS free trial
- Review interactive demos and tutorials

Build employee skills in as little as 3 weeks

- 2 technical credentials
- 1 sales credential
- Required to earn channel incentive
- Time cost

Create your own Verify SaaS instance

- Verify tenant for up to 10 apps
- Never expires
- Build your own demos and reusable content
- No cost but requires approval

Increase your rewards

- Complete advanced technical certifications
- Demonstrate sales success
- Achieve customer satisfaction targets

Can be accomplished concurrently

Verify Access —new license example

Co-Led/BP-Led segment
incentive rates

Partner incentive
potential*

*Average sale cycle:
6 to 9 months*

*Timing for initial deployment:
4 to 6 months*

Incentive type	Incentive rates	Comments
Estimated average deal size for Verify – \$100,000 for on-prem. Typical deals range from \$75K – 100K		
Sales incentive	10%	Sales incentive rewards Business Partners for the opportunities they generate and the value they bring through the different stages in the sales cycle which result in the sale of IBM New License software to the End user
Focus offering incentive	10%	Focus offering incentive rewards Business Partners for selling eligible IBM product offerings which are core to IBM's strategy with value (applicable when transaction also received sales incentive or engagement incentive)
Growth client accelerator incentive (BP Led only)	15%	Growth client accelerator rewards Business Partner for selling in the BP-Led (Growth) customer segment with value (applicable when transaction also received sales incentive or engagement incentive)
Engagement incentive	10%	Engagement incentive rewards Business Partners for their role and post-sales value-add activities they bring which result in the sale of IBM New License software to the End User and implementation and usage of the newly acquired IBM licenses.
Value-add distributor channel margin	Contact VAD	IBM Distributors have sole discretion to determine the amount (if any) of channel margin shared with the reseller. Resellers should discuss the channel margin with their distributors
Additional BP-provided services revenue	2x deal size	Potential additional BP services negotiated and provided by BP to clients
Maximum potential margin	30% (Co-Led) 45% (BP-Led) +VAD margin	Earnings on your first deal may defray the cost of your time investment.

*For planning purposes only, incentives for GOE clients and VAD margin paid at time of transaction; incentives for non-GOE clients are paid back-end. Incentives above are worldwide rates; some Geos or Markets may vary. Refer to <https://www.ibm.com/partnerworld/program/compliance/ibm-product-groups-exhibits> for parts eligibility and <https://www.ibm.com/partnerworld/incentives/ipe-software-new-license> for detailed incentive descriptions

Verify SaaS — example

Co-Led/BP-Led segment incentive rates

Partner incentive potential*

*Average sale cycle:
3 to 6 months*

*Timing for initial deployment:
30 to 60 days*

Incentive type	Initial Subscription rates	Contract extension rate	Comments
Estimated Average Deal Size for SaaS- \$50,000; 1200 employees / SSO / MFA = \$50K ACV			
Land incentive	10%		Rewards Business Partner who acquires a new customer or move clients to IBM-hosted SaaS offerings.
Deal registration	5%	5%	Incentive protection when BP registers SaaS deals in MySA and becomes the IBM Business Partner of Record for SaaS
Stay engaged		10%	Receive recognition for staying engaged and ensuring clients extend or renew eligible SaaS subscriptions
Long-term commitment	5%	5%	Rewards when Business Partner resells to extend IBM-hosted SaaS offerings for qualifying items for a coverage term of 24 months or longer
Additional BP-provided services revenue	1x - 5x deal size		Potential additional BP services negotiated and provided by BP to clients (examples - Migrating on-prem to SaaS, consumer digital transformation, workforce modernization)
Maximum potential margin	20% + VAD margin	20% + VAD margin	Earnings on your first deal may defray the cost of your time investment.

*For planning purposes only, all SaaS incentives and VAD margin are paid at time of transaction. Refer to <https://www.ibm.com/partnerworld/program/compliance/ibm-product-groups-exhibits> for parts eligibility and <https://www.ibm.com/partnerworld/incentives/ipe-software-saas> for incentive descriptions. Incentives above are worldwide rates; some Geos or Markets may vary.

Verify go-to-market resources

Develop your strategy for
delivering Verify to your clients
and/or prospects

[Product overview](#)

Review the latest about the solution

[Demo](#)

Explore the demo and learn how to
**securely connect any user to any
resource**

[Calculator](#)

Try the unit resource calculator to
easily estimate cost of Verify

[Free edition](#)

Try Verify and quickly add applications
to SSO, try out adaptive MFA across
resources

[Enablement](#)

Build your sales and technical
knowledge with a comprehensive
roadmap

[Competencies](#)

Earn solution competencies to
differentiate your skills in the
marketplace

[Community](#)

Join our community to interact with
IBM, clients and peers

[IBM Services](#)

An available option to offer clients, if
needed

Verify demand generation tools

Drive demand and engage with your clients and/or prospects about Verify

Co-Marketing Funding

Leverage IBM co-marketing funding to enhance your marketing plans

[Learn more](#)

Digital Campaign

Drive leads through customized content throughout all stages of the buyer journey

[Learn more](#)

Client facing assets and messaging

All content available to business partners

[Learn more](#)

External client reference

How can you boost business agility with cloud-based identity management?

In its move to hybrid cloud computing, a US boutique asset management firm sought a robust identity and access management (IAM) solution for its digital wealth management platform. It engaged IBM Business Partner [Pontis Research, Inc.](#) to deploy and manage the IBM Security Verify Access offering hosted by Amazon Web Services, helping drive growth through greater IT flexibility. By teaming with an experienced security services provider, the firm can also increase productivity and minimize IT costs.

[Read the full story](#)

Simplifies web and mobile experiences using single sign-on and multifactor authentication across applications and devices

Solution component:
[IBM® Security Verify Access](#)



External client reference

How do you grant system access to thousands of users and comply with hundreds of regulations?

Logistics is a complex business. But the challenges extend far beyond moving products from Point A to Point B. As an owner and operator of an integrated system of rails and ports, [VLI](#) must comply with hundreds of government regulations. Its 9,000 workers also need access to just the right systems at the right time to do their jobs.

By deploying solutions from the [IBM Security](#) portfolio of products, VLI better managed compliance and identity governance and administration, and realized gains across the business.

[Read the full story](#)

Grants user access to necessary systems 99% faster than before, from five days to just seconds

Solution component:

- IBM® Security™
- IBM Security Directory Suite
- IBM Security Verify



Contact Us!

Worldwide

Guy Fries, WW Channel Sales Leader
guyfries@us.ibm.com

Traci Romero, WW Business Partner Marketing
traciromero@us.ibm.com

Prasad S Raman, WW Ecosystem Offering Management
Digital Trust
Prasad.S.Raman@ibm.com

Geo

North America
Randy Long, Security SW Sales Leader - Business
Partner Ecosystem
randy.long@us.ibm.com

EMEA
Patrik Horemans, Subject Matter Expert IAM IBM Global
Markets
patrik.horemans@be.ibm.com

APAC
Kittipong Asawapichayon, IBM Security, Ecosystem &
Channels Lead
kittipon@th.ibm.com

Thank you!

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

© Copyright IBM Corporation 2021. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty, of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.



Appendix

Market landscape

Serve both workforce and consumer populations

Workforce IAM

Accelerate workforce productivity. Leverage unparalleled context and intelligence for access decisions and integrate IAM with threat management and incident response for comprehensive enterprise coverage.

Consumer IAM

Protect and maintain brand trust. Deliver a seamless omnichannel experience with progressive profiling, strong privacy and consent tracking, and frictionless access for low-risk users.



Recent Forrester reports for IBM Security Verify

The Forrester Wave:
Risk-Based Authentication,
Q2 2020



"The solution is a great fit for firms that need access policy enforcement in addition to login activity risk scoring."

The Forrester Wave:
Customer Identity and Access
Management, Q4 2020



"The solution is a great fit for firms that need to combine risk-based authentication with CIAM or revamp an existing IAM or web fraud management portfolio from IBM."

The Forrester Total Economic
Impact of IBM Security Verify,
Q3 2020



ROI
619%



Payback
<6 months

"The (organization) benefits from a lower cost cloud model and the ability to do things faster, such as adding multifactor authentication to applications; this had taken 30 days to do with the on-premises solutions but takes only a few hours with IBM Security Verify."

2020 modernization of IAM brand

