Zero Trust:
A Business-First Approach to Security

—

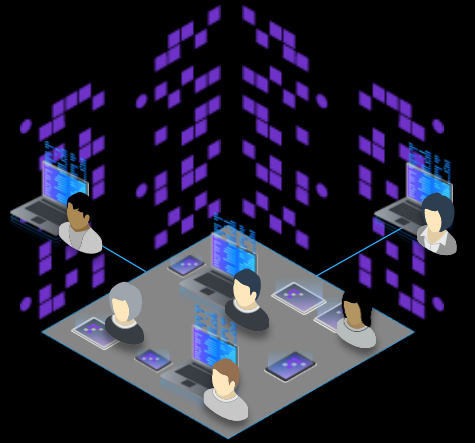
Partner Playbook

IBM **Security**

IBM

Contents

Digital transformation has changed the way businesses operate…



User and Endpoints

Accessing from anywhere
using any device

Applications and Data

Data is a shared resource
for users and applications

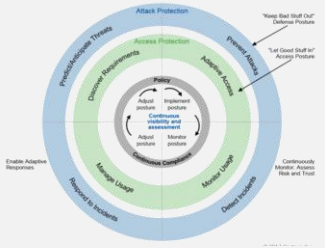
Infrastructure

Servers and networks distributed
across hybrid cloud environments

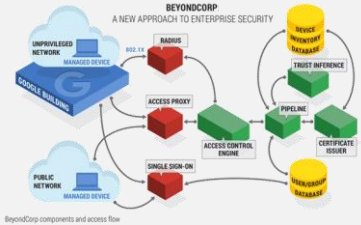
…this complexity is why organizations are turning to **zero trust.**

CISOs are looking to zero trust to manage their digital transformation

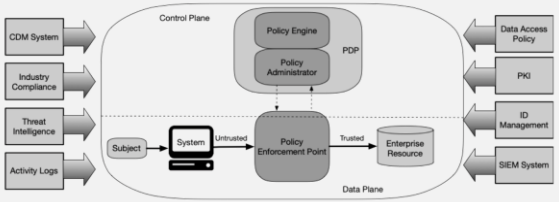
FORRESTER®
Zero Trust



Gartner
CARTA



Google
Beyondcorp



NIST
Framework

Principles of zero trust:

Never trust, always verify

Enable least privilege

Assume breach

Zero Trust is being touted as an approach to mitigate or even prevent the disruption caused by recent cyberattacks

"… Outdated security models and unencrypted data have led to compromises of systems in the public and private sectors. The Federal government must lead the way and increase its adoption of security best practices, including by employing a **zero-trust security model**…"

~ Executive Order on Improving the Nation's Cybersecurity

Colonial Pipeline Company

"… Every major infrastructure provider—from energy to transportation to water systems and healthcare and more—should be equipped or retrofitted with the **zero trust security controls** that […] provide much greater protection of critical infrastructure…"

~ Bert Rankin, Zentry Security COO

solarwinds

"…**Real-time authentication** tests users and looks to block suspicious activity and prevents adversaries from the kind of **privilege escalation** that was demonstrated in the SolarWinds attack…Many of the tools we need to implement this model already exist […] but successful implementation will require a shift in mindset and focus…"

~Chris DeRusha, Federal Chief Information Security Officer

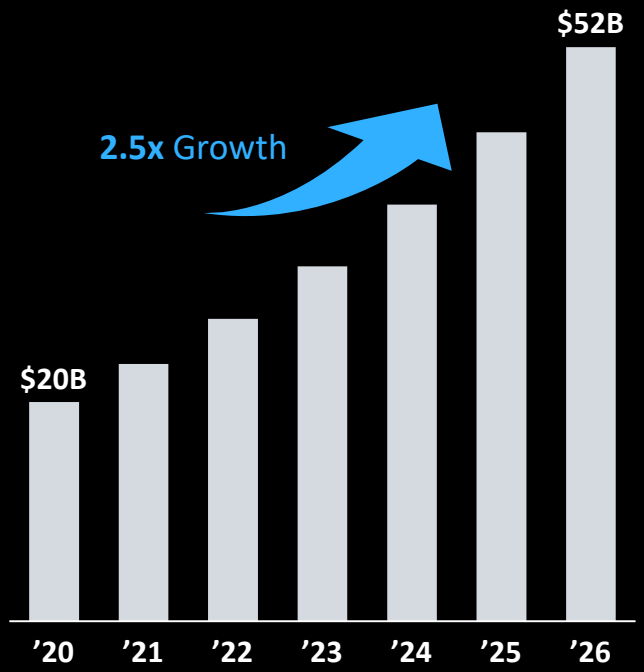
twitter

"…This incident [Twitter hack] is a great reminder of the importance of the principle of **least privilege**, sometimes referred to as **zero trust**. Least privilege means all employee access is considered privileged access, regardless of whether that access is at the authorization / administrative level or provides access to sensitive data…"

~ Joseph Carson, Thycotic Chief Security Scientist

The market opportunity for Zero Trust is expected to grow 2.5x by 2026 with Zero Trust use cases applicable across a range of industries

Zero Trust Market Opportunity



Industry Opportunities

Industry	Industry Drivers	Market Size 2020	CAGR 20 → 26
IT Services	Increased enterprise adoption of remote work and BYOD as well as a growing threat landscape	$6.5B	+18.0%
Financial Services	Growth of cloud banking and expansion of govt. regulatory standards (GDPR, PCI, Sarbanes Oxley, etc)	$3.8B	+17.6%
Healthcare	Accelerated digitization of health information and other PII data while maintaining HIPAA compliance	$2.5B	+18.4%
Retail	Growth of ecommerce channels and technologies such as location-based marketing increase vulnerability to threats	$0.8B	+17.1%
Utilities	Expansion of household IOT devices and increased targeting of large scale critical infrastructure (OT) by threat actors	$1.9B	+16.3%
Others	Growing frequency of target-based attacks, increased size of remote workforce, and accelerated migration to clou	$4.1B	+16.2%
Total		$20B	+17.3%

Source: Markets & Markets Zero Trust Market Forecast

Connect openly. Grow fearlessly. With Confidence.

Insights

Enable least privilege access by discovering and assessing risk across data, identity, endpoint, apps and infrastructure

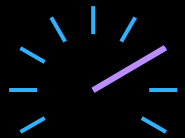
Enforcement

Never trust, always verify with context-aware access control to all apps, data, APIs, endpoints, and hybrid cloud resources

Detection and Response

Assume breach and identify threats and automate responses that not only stop the immediate attack, but dynamically adapt access controls

IBM's approach is best positioned to deliver on the Zero Trust value proposition

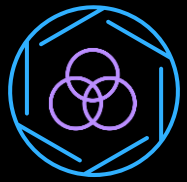


Industry Leading SW

- Industry leading Data Security, Threat Management and IAM tools
- Modern SW built for cloud-native and hybrid environments

Open Platform

- Cloud Pak for Security built on OpenShift
- Flexibility to deploy on-prem or across cloud environments
- Interoperability with existing security tools



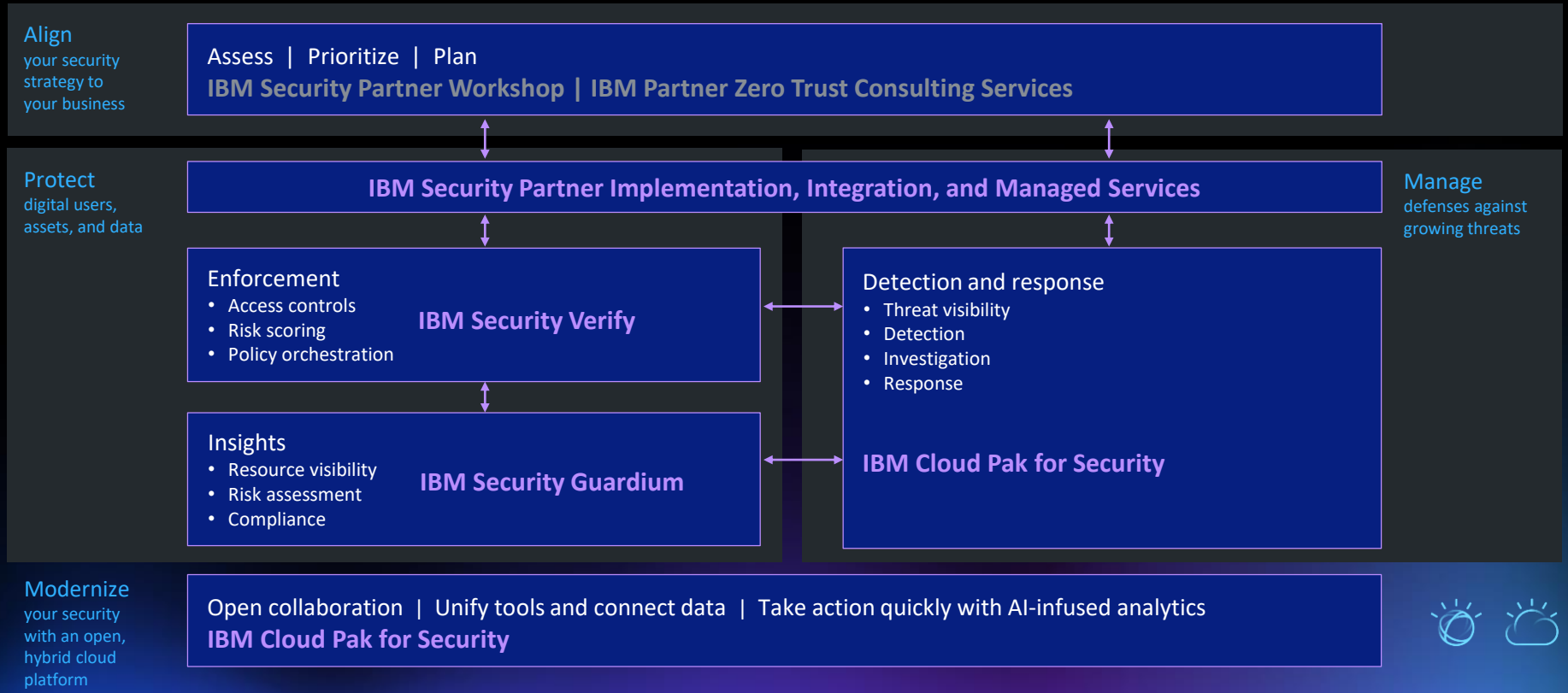
Technology Ecosystem

- Leverage strategic alliances and partnerships to complement IBM technology and enable zero-trust use cases

End to End Capability

- With the technology ecosystem, IBM offers an end-to-end security technology portfolio to enable a Zero Trust approach
- Integrated Zero Trust Framework

IBM is uniquely positioned to deliver end-to-end zero trust expertise, integrated across products and services



IBM’s business-first approach to zero trust is aligned to top business priorities

Hybrid Workforce

- Build an anywhere workforce with everywhere security

Insider Threat

- Limit business disruptions and improve security posture by quickly neutralizing insider threats

Consumer Privacy

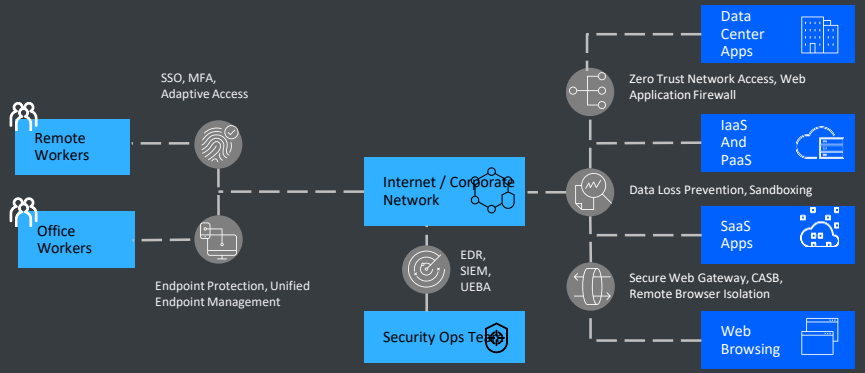
- Create and deliver customer experiences founded on privacy and security

Hybrid Cloud

- Move to cloud with confidence knowing security is in your control

Secure the Hybrid and Remote Workforce

Use Case and Solution Overview



Current Customer Challenges

- **Bypassed legacy network security controls** with direct internet access by remote users
- **Exposed internal network** to potential threats by relying on VPN connectivity to data center
- **Increased risk of phishing** and other credential theft scams
- **No protection for unmanaged devices** and riskier user behavior on managed devices

Outcomes Delivered

- **Reduced cost and improved security by** leveraging alternative solutions to VPNs for remote use access
- **Increased identity assurance of remote users without UX tradeoffs** to remove friction from authentication experience
- Enable **secure access from any device** for employees, contractors, and partners

Partner Playbook

Market Context and Opportunity

$11B
SASE Opportunity by 2024

82%
Of company leaders plan to allow remote work at least part time

90%
Of IT workers (managers through to C-Level) believe remote workers are not secure

Required Technical Solutions for Hybrid Workforce

SIEM / UEBA	SOAR	Data Protection	Identity & Access Mgt	Consent Mgmt.	Priv. Access Mgmt	Endpoint Protection	Third Party Partners
CP4S • Qradar + UEBA	**CP4S** • Resilient		**Verify** • SSO • MFA • Adaptive Access		**Verify** • Privilege Vault	**MaaS360** • UEM • Endpoint Threat Protection	zscaler

Partner ROI

SW Re-Sale

$175k
Average BP Deal Size

+

Services Multiplier

$90k - $700k
Consulting Services
Range: 0.5x - 4.0x

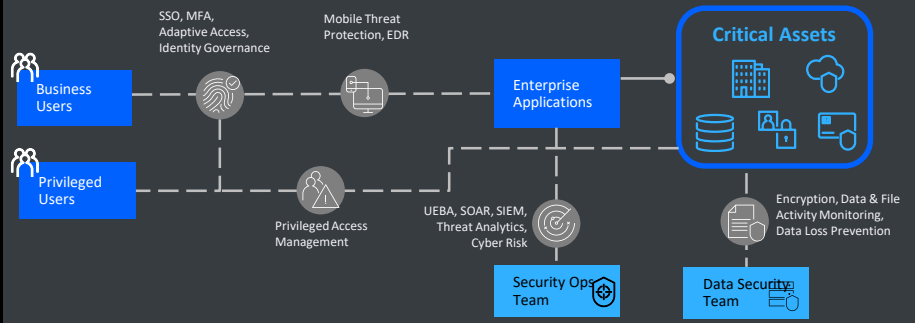
$525k
Managed Services
Up to 3.0x

Up to $1.4M
Total Opportunity

Note: Consulting Services Range (0.5x = Basic Training/Lab Services → 4.0x= Full Scale Transformation)

Reduce Risk of Insider Threat

Use Case and Solution Overview



Current Customer Challenges

- **Enforcement policies are fragmented** across different systems and tools
- **Intel limited to known bad actors,** limited visibility into user behavior patterns across devices, systems, and data sources
- **Manual and reactive response** to incidents leading to "too little, too late"
- **Static protection policies** become less effective over time

Outcomes Delivered

- **Proactively stop potential threats** faster and more accurately by leveraging **full context** available
- **Minimize manual response** processes and **dynamically adapt protections** to respond faster and prevent future threats

Partner Playbook

Insider Threat Demo

Market Context and Opportunity

$11.5M	77	62%
Average annual cost to respond to insider incidents	Average number of days to respond to each insider threat incident	Of insider threat incidents are due to negligence and not malicious actors

Required Technical Solutions for Insider Threat

SIEM / UEBA	SOAR	Data Protection	IAM SSO, MFA	Consent Mgmt.	Priv. Access Mgmt	Endpoint Protection	Third Party Partners
CP4S • Qradar + UEBA	**CP4S** • Resilient	**Guardium** • Data Prot.	**Verify** • MFA • Adaptive Access		**Verify** • Privilege Vault • Privilege Manager	**MaaS360** • Endpoint Threat Protection	zscaler

Partner Opportunity

SW Re-Sale

$185k
Average BP Deal Size

+

Services Multiplier

$90k - $750k
Consulting Services
Range: 0.5x - 4.0x

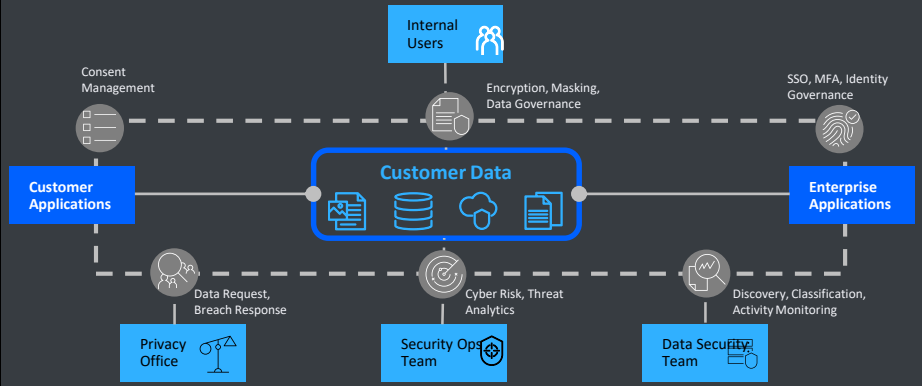
$550k
Managed Services
Up to 3.0x

Up to $1.5M
Total Opportunity

Note: Consulting Services Range (0.5x = Basic Training/Lab Services → 4.0x= Full Scale Transformation)

Preserve Customer Privacy

Use Case and Solution Overview



Current Customer Challenges

- **Lack of visibility** into where data resides and flows and whose data it is
- **Difficult to manage and enable secure data usage and sharing**, while conforming to purpose and consent of data subject
- **Heavy reliance on manual processes** for breach response, DSAR requests, and compliance reporting that are costly and not scalable

Outcomes Delivered

- **Gain a complete view of privacy risk** by tracking where personal data is stored, its lineage, and maintaining an audit trail
- **More effectively manage user consent** to deliver a better customer experience and ensure personal data use aligns with purpose
- **Reduce costs and improve response** by removing error prone manual processes with automated workflows, analytics, and simplified reporting

Partner Playbook

Market Context and Opportunity

$5.2B
Security buyer compliance tooling spend through '22

30%
Higher e-commerce profits for companies maintaining digital trust with customers

42%
Of customers protect their privacy online by avoiding organizations they don't trust

Required Technical Solutions for Customer Privacy

SIEM / UEBA	SOAR	Data Protection	IAM SSO, MFA	Consent Mgmt.	Priv. Access Mgmt	Endpoint Protection	Third Party Partners
	CP4S • Breach Response	Guardium • Data Prot. • Data Encryption • Insights	Verify • CIAM	Verify • Consent Mgmt.			1touch.io

Partner ROI

SW Re-Sale

$95k
Average BP Deal Size

+

Services Multiplier

$50k - $380k
Consulting Services
Range: 0.5x - 4.0x

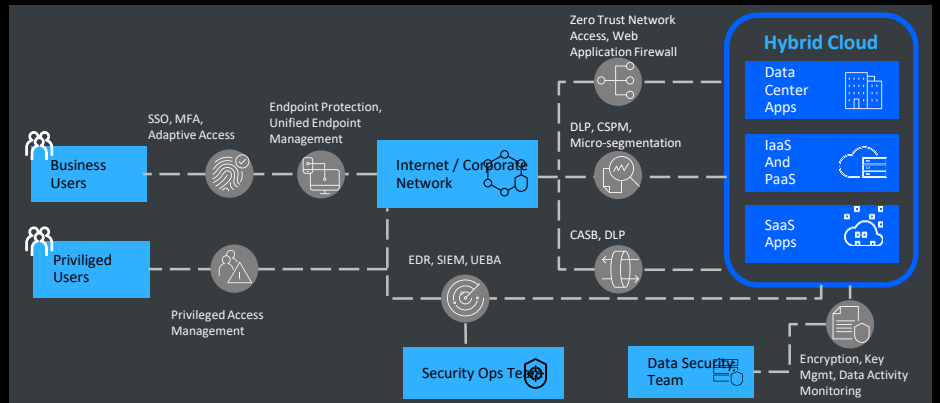
$285k
Managed Services
Up to 3.0x

Up to $750k
Total Opportunity

Note: Consulting Services Range (0.5x = Basic Training/Lab Services → 4.0x= Full Scale Transformation)

Protect the Hybrid Cloud

Use Case and Solution Overview



Current Customer Challenges

- **Increased risks** associated with Shadow IT, insufficient SaaS security controls
- **Visibility and consistent policy enforcement** of hybrid cloud infrastructure
- **Building secure apps** in the cloud from development through run time protection of cloud native workloads
- ~~**Securing data** in the cloud at rest, in transit,~~ and ensure regulatory compliance

Outcomes Delivered

- **Centralized visibility and policy mgmt** to enable continuous compliance, monitoring, reporting, and response
- More **efficiently monitor for cloud configuration drift** and ensure **consistency of security policies for all cloud workloads**
- ~~**Locate all assets** in the cloud to establish the~~ right **protections and access controls**

Partner Playbook

Market Context and Opportunity

$53B	94%	80%
Market opportunity for Cloud Security Services	Enterprises using multiple public clouds	Enterprise data still on-premises

Required Technical Solutions for Protecting the Hybrid Cloud

SIEM / UEBA	SOAR	Data Protection	IAM SSO, MFA	Consent Mgmt.	Priv. Access Mgmt	Endpoint Protection	Third Party Partners
CP4S • Qradar (w/ Cloud Connector)	**CP4S** • Resilient	**Guardium** • Insights • Data Encryption	**Verify** • SSO • MFA • Adaptive Access		**Verify** • Privilege Vault • Privilege DevOPS		aws Azure Google Cloud

Partner ROI

SW Re-Sale

$180k
Average BP Deal Size

+

Services Multiplier

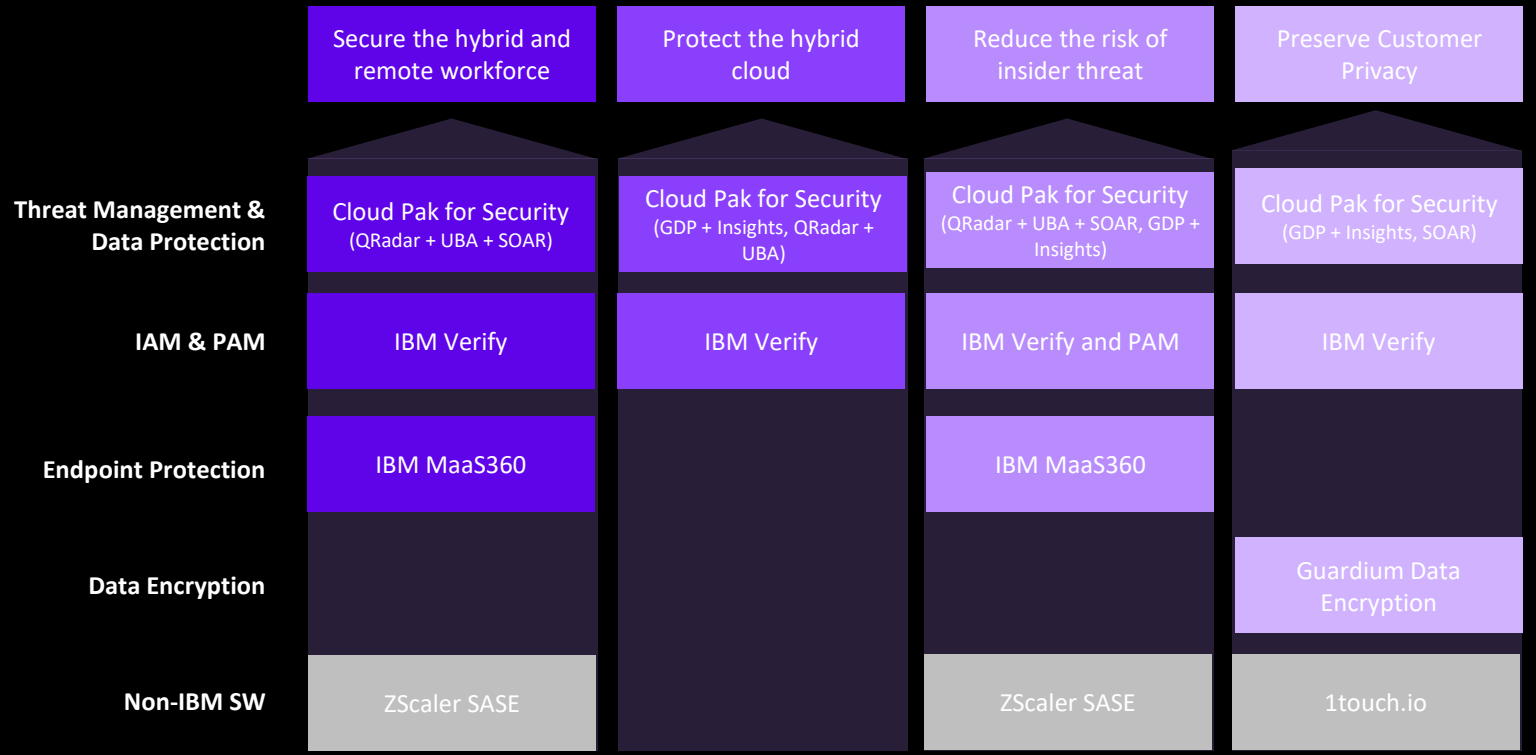
$90k - $720k
Consulting Services
Range: 0.5x - 4.0x

$540k
Managed Services
Up to 3.0x

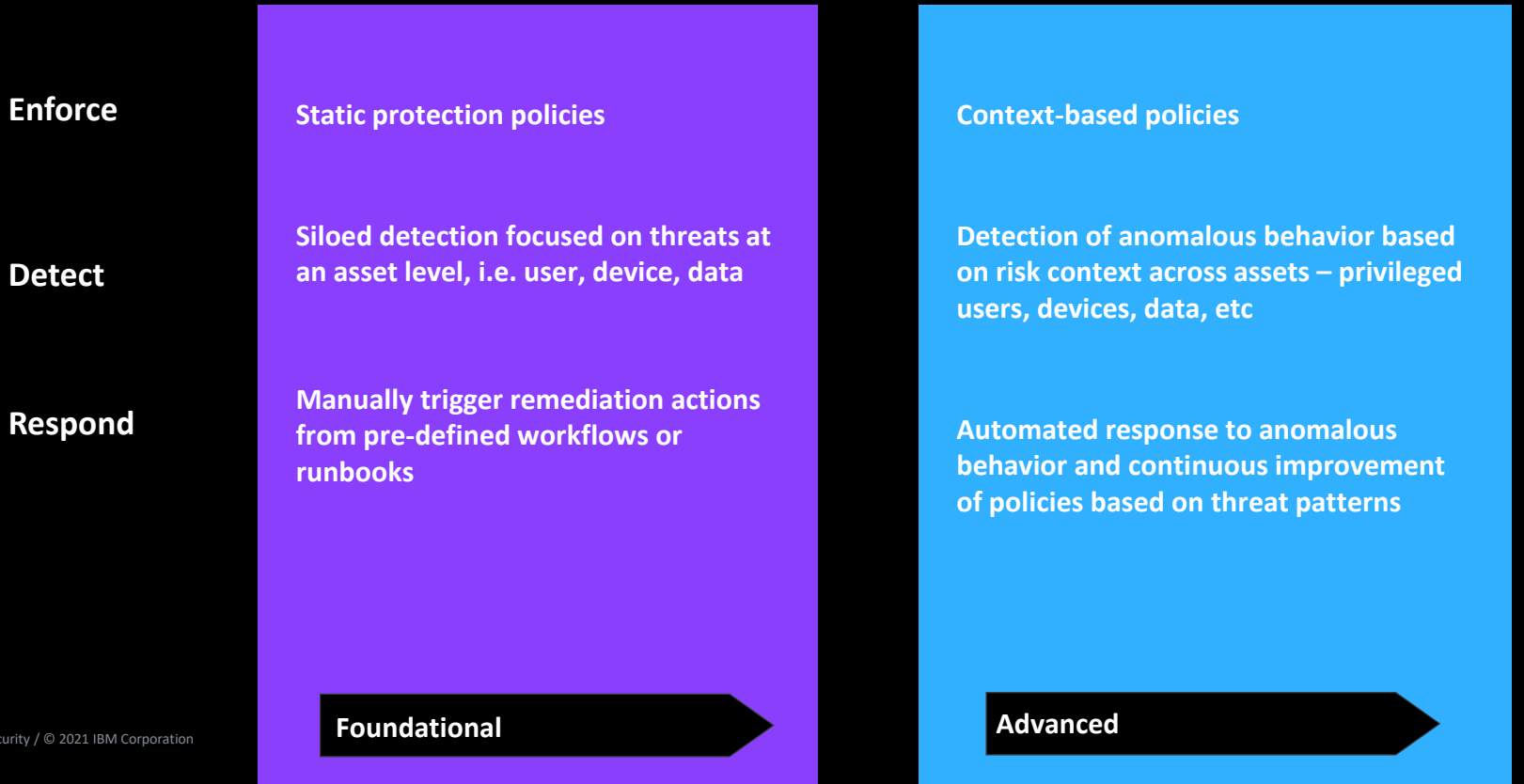
Up to $1.4M
Total Opportunity

Note: Consulting Services Range (0.5x = Basic Training/Lab Services → 4.0x= Full Scale Transformation)

IBM brings a complete set of technologies and strategic partnerships to deliver key Zero Trust use cases



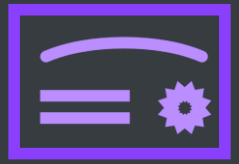
A Zero Trust engagement gives partners an opportunity to expand their relationship with a customers over time



How to Get Started? IBM has several assets and initiatives to help you get started with Zero Trust

Zero Trust Badges

- Foundational courses and training across a variety of skills (sales, solution domains, etc)



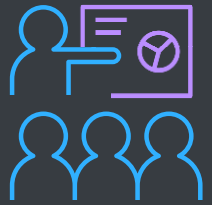
Zero Trust Certifications

- Official product administrator and specialist accreditation
- Demonstrate expertise in related IBM technologies and solutions

For Individuals

Zero Trust Competency

- Recognition for IBM partners who demonstrate technical proficiency and proven success in delivering zero trust value to customers



Zero Trust Workshop

- Workshop for BPs with IBM Security experts
- Prepare BPs to deliver a ZT engagement with customers

For Organizations

IBM Zero Trust Badges and Certifications

IBM Digital Badges

- Digital badges attest to an **individual's mastery** of a specified role
- Typically earned by **completing a course of self-study** and passing an online quiz
- Some badges require **participation in an instructor-led course**, either delivered by an authorized IBM Training Partner or at an IBM training event

IBM Security Certifications

- Worldwide industry program open to all technical professionals (IBM employees, Business Partners, Clients) to **demonstrate proficiency in the latest IBM technology and solutions**
- Establish **capability to perform job role related tasks and activities** at a specified level of competence.
- Certification **validates knowledge and technical skills** and served as a method for companies to ensure certain employee performance levels

IBM Zero Trust Competency

Recognizes IBM PartnerWorld members who demonstrate technical proficiency and proven success in delivering zero trust value to customers

Requirement to Earn Zero Trust Competency

- Set of zero trust services that leverage key IBM offerings
- Demonstrated thought leadership in zero trust implementation for hybrid cloud environments
- Achieved required skill validations in IBM technologies
- Meets threshold for minimum number of client engagements and IBM license revenue

Zero Trust Competency Benefits for Partner

- Technical validation of partner's zero trust capability by IBM Distinguished Engineer
- Solution/Service promotion through PartnerWorld spotlight
- Special designation and higher priority search results in Global Solutions Directory
- Access to Client Success Central team to produce client case studies
- Blog promotion with access to IBM Business Partner feature blog

IBM PartnerWorld

Program to become an "Official IBM Partner" and unlock additional benefits and support

- Competency certifications
- Training on IBM technology
- Go to market support
- Access to virtual client center
- Access to IBM Business Partner directory

How To Get Started: Zero Trust Framing & Discovery Workshop

An interactive virtual session that helps you to have a Zero Trust discussion with your clients

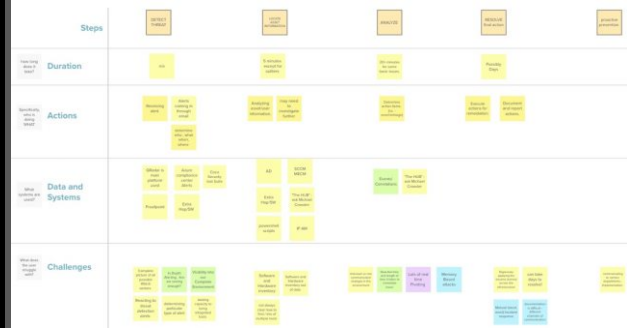
The details

IBM subject matter experts will help you prepare your business partners to deliver a zero-trust engagement. IBM will help partners modernize their customer's security program to uncover hidden threats faster, and make more informed, risk-based decisions

Obtain a strategic view of Zero Trust architectures

Gain insight on how to best apply a Zero Trust approach and communicate value to your customers

Identify zero trust initiatives based on client's business needs



Value of the workshop

Outcomes & Deliverables

Alignment on the definition of Zero Trust in the context of your business.

Clarity which Zero Trust initiatives would provide the most valuable results for your organization.

Outcomes deliverable with a recap of all workshop activities and actionable next steps towards a Zero Trust approach for your company.

IBM’s online partner tools

IBM PartnerWorld

Partner resources organized for the way you work

Getting started
Current incentives

Seismic@IBM

Key assets and collateral for IBM Security

IBM Security homepage
IBM Security content map

Security Learning Academy

Free technical training for IBM Security products

SLA homepage

Passport Advantage Online

Software entitlements, downloads, & order history

PAO for Customers
PAO for Business Partners

IBM Security Zero Trust Product Resources for Partners

		CP4S	QRadar	SOAR	Verify	Guardium	MaaS360
Security Software HOME Page	**START HERE** Find quick links to customer facing presentations/assets, demo assets, FAQs, sales plays, roadmaps, learning and more.	CloudPak for Security	Security Intelligence	SOAR	Verify	Guardium	MaaS360
Market Place Page	IBM customer facing site. Offering description and assets (whitepapers, data sheets).	< LINK >	< LINK >	< LINK >	< LINK >	< LINK >	< LINK >
Prospecting email templates	Pre-drafted email templates to be used for announcements, new logo and/or competitive prospecting.	< LINK >	<LINK>	<Privacy> <CP Upsell>	< LINK >	< GDP > < Insights >	
IBM Security Competitive Insights	Competitive battlecards, scorecards and analyst reports.	< LINK >			< Okta > < Forgerock > < CyberArk >	< LINK >	
IBM Security Demo Central	Use case based demos. scripts, click thru and video.	< LINK >					
Seismic assets for Partners	Additional marketing and technical resources	< LINK >	< LINK >	< LINK >	< LINK >	< GDP > < Insights >	< LINK >
Product Value Assessment	No cost workshop to assess state of customers deployment.		< LINK >	< LINK >			
IBM Global Customer References	Share win information and learn from others.	< LINK >					
IBM Security Customer References	Customer reference profiles and case studies.	< LINK >					
Enablement Talks and Replays	IBM Security Sales Enablement Talks, Events and Replays	2021 / 2020					

Always refer to the latest version of this document posted HERE.

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

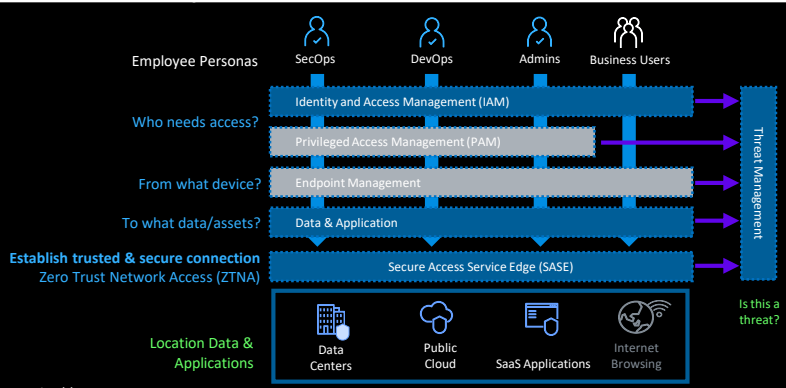
@ibmsecurity

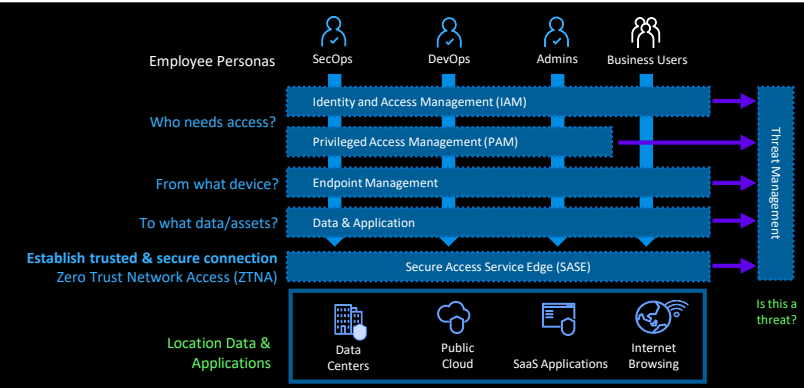
youtube/user/ibmsecuritysolutions

Backup / Reference

Hybrid Workforce: Simple client entry points provide a path to grow Zero Trust business over time and continue to deliver value to customers

		Zero Trust Entry Points		Additional Advanced Capabilities	
Compromised Credentials	**Insights**	**Application Discovery** by SASE			**IBM Verify**
	Enforce	**Zero Trust Network Access**	**ZScaler**	**Zero Trust Network Access with integrated Adaptive Access**	**Cloud Pak for Security**
	Detect & Respond	User & Entity **Behavior Anomaly Detection**	**QRadar UBA**	**Extended** Detection and Response	
Mobile Phishing	**Insights**	**Unified Endpoint Management**			**SASE Service**
	Enforce	**Adaptive access** using multi factor authentication	**Maas360** **IBM Verify**	**Data Loss Prevention** Remote **Browser Isolation**	**Cloud Pak for Security**
	Detect & Respond	User & Entity **Behavior Anomaly Detection**	**QRadar UBA**	**Extended** Detection and Response	
Data Exfiltration	**Insights**	SaaS **Application Discovery**			
	Enforce	**Secure Web Gateway**	**ZScaler**	**Data Loss Prevention** Remote **Browser Isolation**	**Cloud Pak for Security**
	Detect & Respond			**Extended** Detection and Response	





Note: Zscaler partnership required by BP

Insider Threat: Entry points with individual IBM Security SW products provide a path to grow Zero Trust business over time

		Zero Trust Entry Points		Additional Advanced Capabilities	
Compromised Credentials	**Enforce**	Secure **password & access policies** (MFA, etc.)	**IBM Security Verify**		
	Detect	**Audit & event logs** of user access		**Analyze user behavior** based on audit information	**Cloud Pak for Security** (QRadar + UEBA + Resilient)
	Respond			**Adaptively block access** at network layer	**ZScaler**
Mobile Phishing	**Enforce**	Define **device security policies**	**MaaS360**	**Establish trust dynamically** based on user and device risk	**Cloud Pak for Security** (QRadar + UEBA + Resilient)
	Detect	Detect **known threats**		**Anomaly-based detection** across all user devices	
	Respond	**Manually block access** based on threats on device		**Automatically enforce conditional access** based on threats detected **Dynamically improve protection policies** based on threat patterns	**ZScaler**
Data Exfiltration	**Enforce**	Monitor **sensitive data access**	**Guardium Data Protection**	**Define data and user level policies**	**Cloud Pak for Security** (Qradar + UEBA)
	Detect	**Detect policy violations** and unauthorized access		**Detect data leak** at the network layer and **analyze threats**	
	Respond	**Identify remediation** actions		Respond to incidents and **initiate remediation** **Dynamically update** data security based on threat patterns	**ZScaler**
Priviliged Account Misuse	**Enforce**	**Establish vault** & implement MFA	**IBM Security Verify Privilege**	**Governance via least privilege** and control of endpoint application rights	**Cloud Pak for Security** (QRadar + UEBA + Resilient)
	Detect	**Analyze privileged access** activities		**Detect anomalous behavior and threat patterns** for privileged accounts	
	Respond	**Manually identify remediation actions**		**Orchestrate remediation actions** based on privileged account access rights **Dynamically update privileged access policies** based on threat patterns	

Consumer Privacy: Foundational entry points with provide a path to grow Zero Trust customer privacy capabilities over time

Enforce

- Basic Data Discovery and Classification

Detect

- Data Activity Monitoring and Policy Management

Respond

- Compliance auditing and reporting

Strengthen your data privacy strategy by enhancing accountability and privacy values

Foundational

- Data discovery and classification for personal data with integrated data privacy risk dashboard
- Identity & access governance
- Encryption, masking and tokenization
- Consent management
- Data risk-based analytics and anomaly detection
- Real-time blocking and redaction
- Security orchestration, automation, and response with Open, connected security and privacy workflows

Privacy by design with improved data analytics and access governance. Deliver frictionless experiences through context-driven insights, advanced analytics, and automation.

Advanced

Journey to Cloud: Zero Trust provides easy entry points that align with a customer's cloud security strategy with a path to grow over time