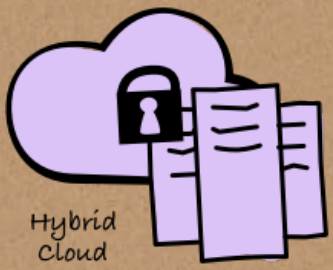
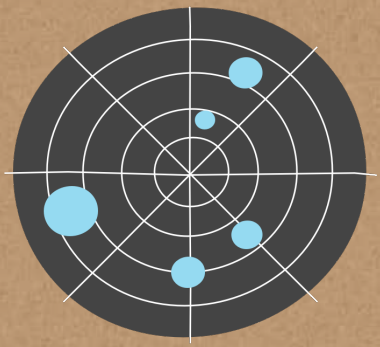
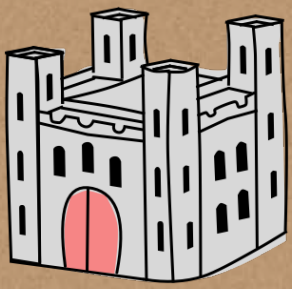

Risk
score


Hybrid
Cloud





Download the current version of the
IBM Zero Trust Security Field Guide

https://ibm.biz/zero-trust-field-guide

What is zero trust?

Imagine a castle surrounded by a series of walls and moats that establish a perimeter to protect the crown jewels. Legacy cybersecurity architectures protect IT resources with a set of perimeter-based controls. Once inside the perimeter, an entity is considered trusted, able to traverse the network and access everything within the zone. As digital transformation has accelerated, perimeter-based controls no longer work because your workforce has become more distributed and your data and applications more decentralized.

IT'S TIME FOR A NEW APPROACH

Zero trust. A security framework founded on the idea that security controls must not rely on implicit trust. That means no user or entity should be trusted based solely on its location (e.g., inside the corporate network), the device being used, or any other singular attribute.

Implement least privilege. Grant entities the minimum level of access required to get their job done. Limit entities access to applications, data, systems, and workloads to reduce the overall attack surface.

Continuous verification. Do not grant an entity access to a resource solely based on a past authentication or other single trust indicators. Always perform verification to ensure that risk factors have not changed.

Assume breach. Run security operations anticipating that security controls have been penetrated. This approach favors a preparedness and proactive nature to threat hunting and breach response.

What's inside?

This field guide provides a high-level overview of zero trust security.

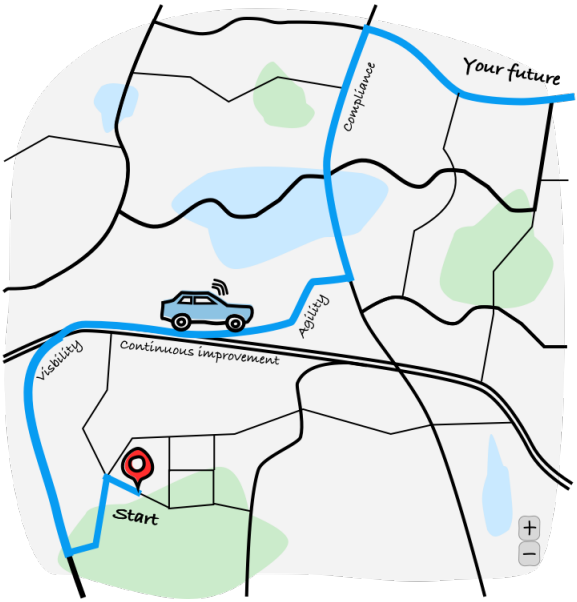
LEARN IT
A summary of the concepts.

GET STARTED
Considerations for implementing zero trust security.

The value of zero trust

When organizations evolve their security programs to adopt a zero trust framework, they become more proactive and less reactive. No security program can provide a 100% guarantee that there will not be a breach or a security incident. However, by applying the core principles of zero trust, organizations can severely limit their attack surface and ensure they have the proper controls and countermeasures in place to reduce the impact and more quickly respond in the event of an attack.

ZERO TRUST IS A JOURNEY, NOT A DESTINATION



Learn more

Applying a zero trust framework can reduce the average cost of a data breach.
https://www.ibm.com/security/data-breach

Visibility is essential. You can't protect what you don't know about. Being able to have clear visibility into all of your assets – data, users, endpoints, workloads, infrastructure – is the first part of any zero trust journey. Discovery and classification are critical first steps on the journey, but you must also ensure that you have that same visibility for activity that is happening across these assets.

Security that is as agile as the business. IT environments are constantly evolving and changing. Developers are discovering new tools. Third parties are onboarded. Devices come and go. As security controls become more adaptive and contextually aware, business changes can continue at speed without introducing new risks.

Continuous improvement is part of the culture. A zero trust framework provides the technical foundation that enables security programs to be more agile. People and processes must commit to ongoing analysis and improvement. Increase business resiliency by learning from past experiences, continuously evaluating efficacy and adjusting policies.

Compliance is a byproduct of secure by design. Compliance is a major priority for any security program. With a zero trust framework that is based on the principles of least privilege and continuous verification, demonstrating compliance is a natural outcome from security activities. There is a level of confidence that the right visibility, controls, and response processes are in place.

Zero trust ≠ don't trust

The term zero trust is often misunderstood. It appears to be in contrast with cultivating trust with customers, partners, and employees. Zero trust is not about removing trust in individuals. In a complex and at times dangerous digital world, adversaries are well organized, innovative, and persistent. Zero trust enables you to have more confidence and actually build trust with all your users.

ENGAGE WITH CONFIDENCE AND BUILD TRUST

Empower your users to engage with confidence. Today, most users are aware of cybersecurity. Multifactor authentication is not only for internal enterprises. It protects our personal banking, email, and social accounts. Implementing visible security controls builds trust and demonstrates that organizations are focused on protecting the organization and their users.

Work with anyone, anywhere. Organizations are no longer restricted to the local geographic talent pool and can now tap into a broad and diverse set of skills and resources worldwide. With zero trust in place, organizations can more confidently open their businesses to customers, partners, and employees wherever they are located.

Be prepared for the unknown. The attack techniques carried out by adversaries include spear phishing, social engineering, business email compromise, malware, and ransomware. A zero trust framework enables organizations to protect themselves, have more dynamic controls, and respond to zero-day vulnerabilities.

Check out how zero trust can help your business grow.
https://securityintelligence.com/posts/confidently-secure-business-grow-fearlessly-zero-trust

The global pandemic of 2020 forced organizations to rethink how they conduct business. An overwhelming majority of the workforce began working remotely, seemingly overnight. Those who have adopted a zero trust framework recognize that it has opened up new business opportunities.

Strike the balance between security and user experience

With a zero trust approach, continuous verification validates that entities are who, or what, they claim to be using challenges such as a second factor authentication (2FA) request. Organizations focused on delivering best-in-class user experiences hesitate to disrupt the user with unnecessary 2FA requests; however, this level of identity assurance is critical for zero trust. New technologies are more convenient than legacy 2FA techniques.

HAVE YOUR CAKE AND EAT IT, TOO!

Personalize the security experience. Most access management and authentication solutions provide a wide range of 2FA options. Modern options, mobile push and OTP generators, take advantage of mobile devices. Users might also choose the 2FA option that is best for them.

Eliminate passwords once and for all. It is accepted that passwords are inherently insecure. Passwordless authentication options include biometrics (fingerprint, face, voice), QR code, FIDO tokens, & behavioral biometrics (keyboard dynamics, mouse movements, screen swipes).

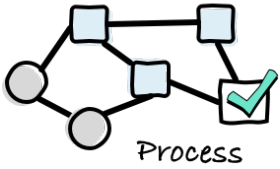
Adaptive access provides transparent security. Adaptive access allows for more dynamic and contextually aware access decisions to be made and is a critical technology for getting to zero trust. For example, it is important to ensure the device being used is not compromised and that the activity being performed is within policy.

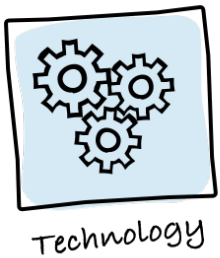
Check out how adaptive access can power a frictionless user experience.
https://www.ibm.com/security/digital-assets/iam/verify-adaptive-access-demo

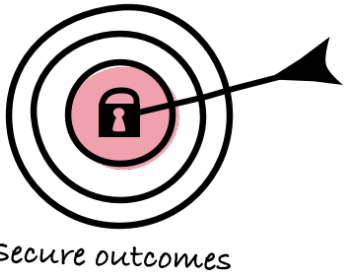

Code
2576
Enter Code
2 Factor authentication
Biometrics
Behavioral biometrics
QR codes
FIDO tokens

Architect security controls for zero trust

You cannot achieve zero trust by using a single technology, product, or vendor. In fact, you might already have many of the key security capabilities core to a zero trust architecture. But are you using them in the right way to get the outcomes that you need? Like many things in the IT world, implementing zero trust is a combination of people, process, and technology.







Learn more

Check out the IBM CISO's perspective on how to approach zero trust. https://securityintelligence.com/posts/ibm-ciso-perspective-zero-trust-changes-security

FORGET WHAT YOU THINK YOU KNOW ABOUT SECURITY CONTROLS

Identity is the new perimeter...again. In the context of zero trust, identities are the new perimeter. The principles of least privilege and continuous verification are applied at the identity layer. A strong and dynamic Identity and Access Management (IAM program is foundational to any zero trust journey. Identity governance, MFA, SSO, and privileged access management are all key capabilities for implementing zero trust.

The network isn't gone, but it has changed. For many cloud-first organizations, the internet has become the corporate network causing the dissolution of the traditional internal network. Network security is critical. Technologies like Secure Access Service Edge (SASE) are replacing traditional firewalls, intrusion prevention systems, and web application firewalls (WAF).

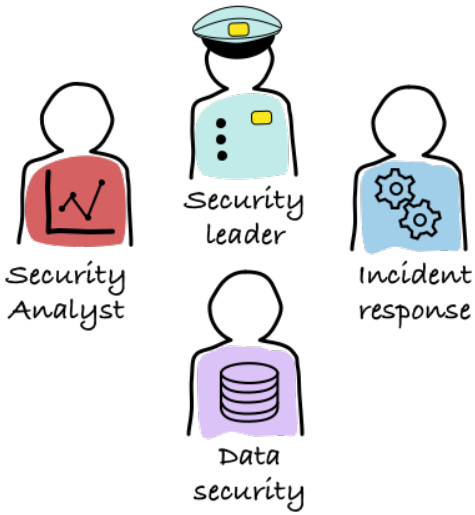
Endpoints are a valuable source of telemetry and control. Dissolving the internal network has removed a critical source of telemetry and visibility for security operations centers (SOC). Security teams are turning to endpoints as an important source of telemetry to understand what is happening both on and off the corporate network. Tools like endpoint detection and response (EDR) and unified endpoint management (UEM) are growing in importance. Combining this endpoint context with cloud and workload context is leading to new solutions like extended detection and response (XDR).

Data is at the heart of what you are trying to protect. Data has become the currency of business and is the target of most cyberattacks. It requires controls not only at the edges, but as close as possible to the data itself. Start with discovery and classification of data for both security and compliance. A zero trust approach requires additional controls like activity monitoring, encryption, and behavioral-based anomaly detection.

Break down the security silos

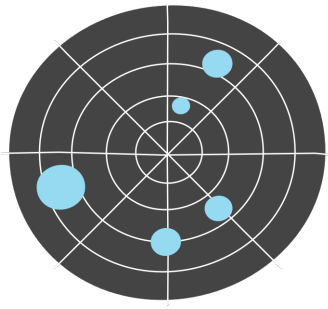
A zero trust framework emphasizes security controls like identity, network, endpoint, and data. Security tools and security teams frequently operate within silos and have different skill sets and priorities, which creates a challenge to align on a common objective. Technical integrations are often complex to manage, time consuming to implement, and costly to maintain. When technical and organizational silos are broken down, it paves the way for zero trust.

WITH ZERO TRUST, 1 + 1 = ∞



Learn more

Streamline the SOC analyst workflow and unify disparate security silos.
https://www.ibm.com/products/cloud-pak-for-security/demos/use-cases



Focus on security outcomes. Security domains share a set of common goals centered around three key areas: insights, enforcement, and detection & response. Insights provides visibility into assets and risk. Enforcement is about controlling access to resources. And detection and response are focused on finding and stopping potential threats.

Share more, detect more, stop more. When context is shared across security domains, opportunities are unlocked for advanced analytics to improve detection rates, reduce false positives, and reduce recovery times through automation. Identity context can help the SOC analyst determine if a particular threat is from a malicious insider or a victim of credential theft. Data context can help the IAM administrator set the proper entitlements for accessing sensitive customer data.

A zero trust platform approach. To be successful, zero trust requires a security platform founded on open standards that works across a heterogeneous environment of vendors and technologies. By unifying multiple technologies into an open platform, you can unlock new insights, ensure a consistent access policy, and more rapidly detect and respond to threats.

Insights: Identify your biggest risks and enable least privilege

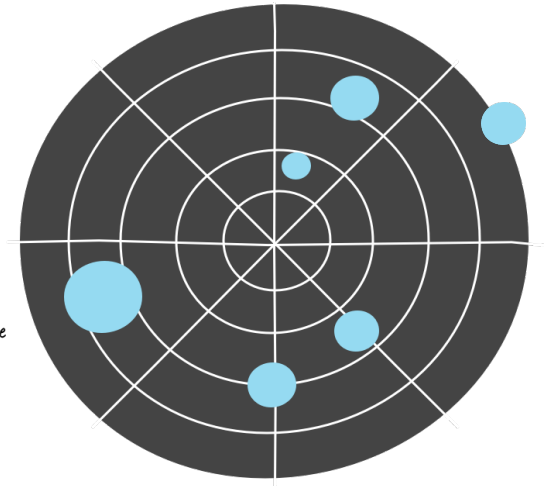
To implement the principle of least privilege, you must understand the assets in your dynamic IT environment. Privileged access is not just a people problem; you need to know what applications have access to what data. The process of discovery, classification, and risk assessment is continuous. Bring together risk data from your digital assets to uncover new business level risk insights to help you establish the right policies.

Who are your users?

Where is your data and who has access to it?

Where are your workloads running?

What endpoints and hosts are connected to your networks?



Learn more

Check out how to prioritize security investments and address potential threats.
https://www.ibm.com/products/cloud-pak-for-security/risk-manager

THE NEXT BIG BREACH COULD BE LURKING AROUND THE CORNER

Customer data fuels your business, but also puts it at risk. Data exists in the data center, in the cloud, and at the edge. Fragmented visibility puts privacy, security, and compliance at risk. You need a single view of where data is, how it traverses your enterprise, and who has access to it. A data security platform automates the process of data discovery, classification, lineage, and uncovers potential risks through analytics.

Identify your riskiest users. Users acquire access to more applications and more data over time. Dormant accounts and excess privileges increase the attack surface. Having strong identity governance and certification processes is not enough. AI can identify your riskiest users based on what they have access to and what they are doing with that access. It can also help approvers make better decisions to reduce risk.

Patching vulnerabilities is never ending. Identifying, prioritizing, and remediating the endless number of vulnerabilities within your IT infrastructure is an overwhelming, yet essential task. If you spend time on the wrong vulnerabilities, you might miss the one that lets criminals into your network. AI can help prioritize findings based on weaponized exploits and key risk factors such as asset value and exposure. This minimizes false positives and ensures a better return on investment.

Bringing it all together to have a single view of cyber risk. Normalized and correlated risk data from across the enterprise and all security domains provides a more complete view of an organization's security risk landscape. This helps you identify and manage macro level risks like credential compromise, data exfiltration, and network intrusion.

Enforcement: Continuously verify users and context

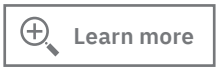
Traditional access policies focus on one time authentication with optional authorization checks based on static attributes or roles. The principle of continuous verification requires dynamic access control policies that make use of context from multiple different sources that can be applied at login and during high risk operations or sensitive data accesses.

YOU MAY BE YOU, BUT SHOULD YOU HAVE ACCESS?

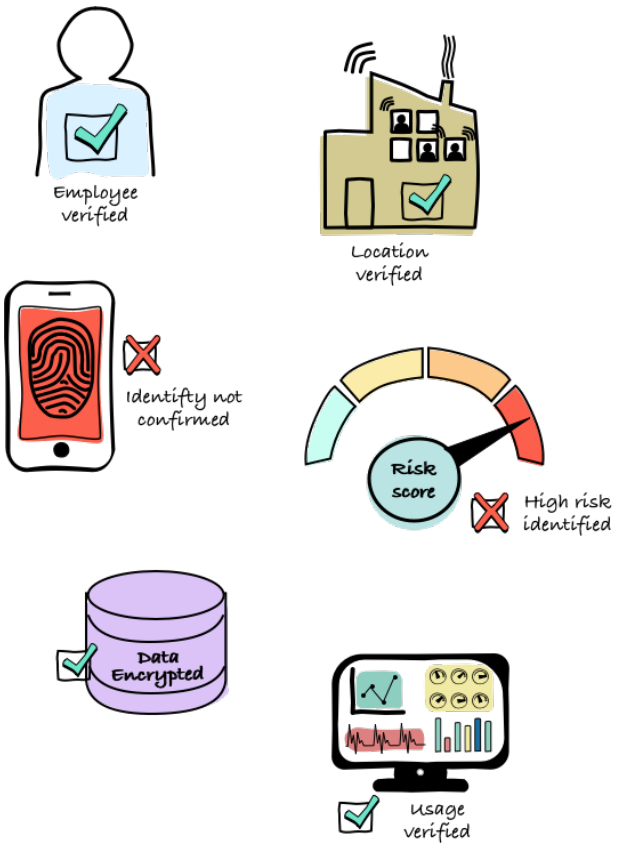
One time verification is not enough. When authentication and authorization checks occur only during the login phase, it creates an opportunity for attacks like malware, remote access trojans, and session hijacking to go undetected. Before any high value or sensitive operation is performed, verify the authenticity of the user and the validity of the action.

Context is king for building trust. Simple attribute and role-based access policies are not enough. A combination of positive and negative signals is required to determine the true risk of allowing access to a given resource. A policy engine can combine signals from an assortment of sources into a single risk score used to control access or take a remediating action.

Enforce consistent policies for all types of resources. There is no single policy management tool today that can work across identity, data, networking, workloads, and endpoints to achieve a consistent continuous verification. However, there are techniques that allow risk context to be shared between components to facilitate better decisions.



Check out how to verify sessions across the entire digital journey.
https://www.ibm.com/security/digital-assets/trusteer/digital-identity-trust-demo



For example, risk scores produced during a risk-based authentication step can be passed to a SASE or a CASB solution as part of a conditional access decision. Over time, expect more standardized approaches to policy definitions to emerge and be applied to zero trust [for example, see open policy agent (OPA)].

Detection & Response: Assume breach and adapt policies

Run your security operations with an “assume breach” mindset, anticipating that your defenses have been penetrated. This shifts the focus to proactive detections, early warning signs, threat hunting, and use of proven runbooks. Detection and response must be tightly integrated with the insights and enforcement layers, sharing context and dynamically adjusting access control policies in response to identified threats.

YOU FOUND THE NEEDLE IN THE HAYSTACK, NOW WHAT?

Telemetry comes from the IT and security environment. The IT environment is complex, resulting in specialized detection and response capabilities: endpoint, network, cloud, and SIEM. Although it is inefficient to maintain specialized solutions, it is required to identify more sophisticated attacks that cross the layers.

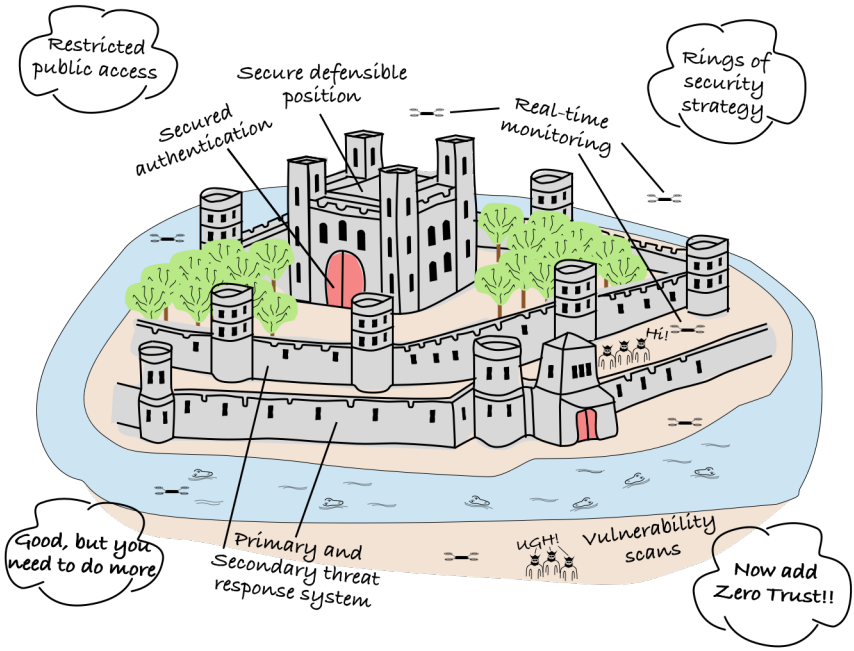
Identify hidden threats using AI & analytics. XDR solutions are important for naturally bringing together telemetry from multiple layers and leveraging AI to quickly identify potential threats by correlating data from all sources.

Prioritize SOC analyst work. AI aids the process of detection and threat hunting. With the increased availability of telemetry and context, use AI to identify and prioritize incidents that have the highest potential impact and to recommend remediating actions.

Learn more

Check out how to reduce remediation time and improve SOC effectiveness.
https://www.ibm.com/products/cloud-pak-for-security/soar

Automation and orchestration are critical for zero trust. To support a swift response after an incident and remediating actions have been identified, XDR solutions must have connectors to the security and IT environment. A simple one-click remediation operation can be the difference between containment and a catastrophic impact. Focus on continued improvement and not only stopping immediate attacks. Use automation to stop the next potential attack before it happens.



Apply a zero trust architecture to top business initiatives

You can use the desired outcomes for your business as a guide for your zero trust journey. By applying a zero trust approach to a specific business initiative, you not only get a faster return on investment, but measurable results that demonstrate value to the organization.

ZERO TRUST IS A BUSINESS ENABLER, NOT AN END GOAL

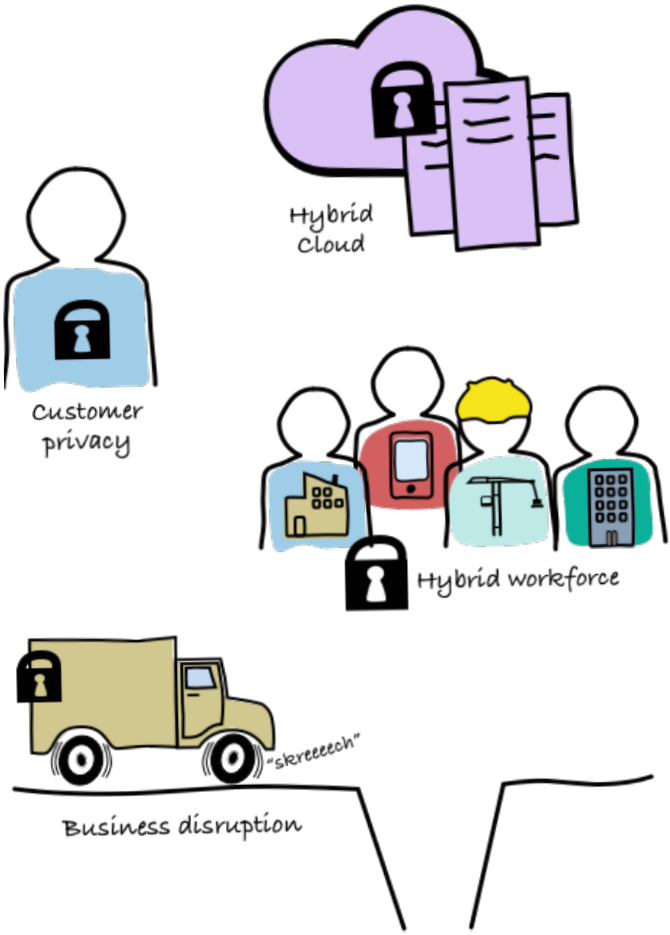
Zero trust is a security, business, and IT strategy. To properly implement zero trust requires buy-in and collaboration from stakeholders throughout the organization: security, IT operations, network, line of business, digital office, privacy office, and more.

Four common business initiatives drive zero trust adoption. A focused approach that applies the principles of zero trust in the context of strategic initiatives limits a typical "boil the ocean" approach and focuses on quick wins. Most organizations have initiatives in one or more of the following areas: preserving customer privacy; protecting the hybrid cloud; securing the hybrid workforce; and reducing the risk of business disruption.

Lay the foundation for securing additional business initiatives. Think of the four business initiatives as a potential starting point with a set of overlapping security requirements. Each initiative requires multiple capabilities that holistically address security challenges.

Learn more

Check out how Dow Chemical is applying a zero trust framework.
https://www.ibm.com/thought-leadership/think-essentials/playlist/security?video=rfv1n8l0


Hybrid
Cloud
Customer
privacy
Hybrid workforce
"skreeeech"
Business disruption

Preserve customer privacy

Ensuring privacy is an essential element for demonstrating the transparency and accountability that fuels brand trust. A zero trust approach can help organizations protect customer privacy with access controls based on least privilege, giving access to only those with a legitimate need and for the agreed upon purpose.

BUILD REGULATORY COMPLIANCE INTO YOUR SECURITY DNA

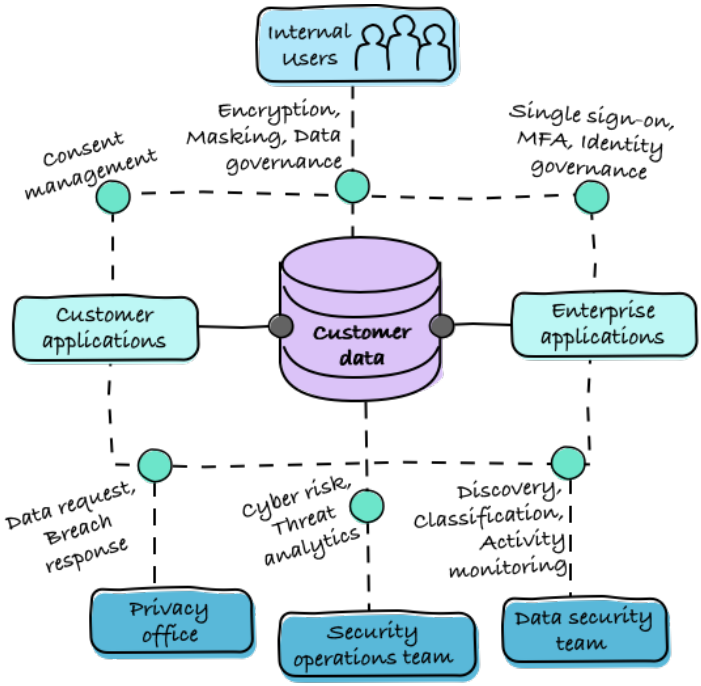
Understand your personal data landscape. Increase visibility to repositories containing personal data, access, and other details to generate contextual insight. Consider integrating tools for data discovery and classification, identity and data access governance, and data and file activity monitoring.

Enable secure data usage and sharing. To achieve business outcomes, your employees might need to access customer data. You need to carefully manage access to personal data within and beyond the organization. Consider integrating tools for consent management, data masking and tokenization, and authentication.

Automate and streamline response. Reduce the inefficiencies of costly and error prone manual processes with automated workflows, analytics, and simplified reporting. Automation enables teams to collaborate in response to data privacy incidents, using shared insights to inform actions. Consider integrating tools for risk-based analytics, anomaly detection, data classification, and orchestrated and automated response.

Learn more

Check out how to preserve customer privacy.
https://ibm.biz/zt-preserve-customer-privacy



Uncover risky user behavior, find security gaps, align to customer consent, chart a path to data privacy maturity, and prepare for audits and regulatory compliance.

Protect the hybrid cloud

Digital transformation relies on the hybrid cloud. Deploying security consistently across all cloud environments helps instill confidence and resilience in business operations. A zero trust approach can help organizations modernize operations and allow security to become a business enabler by dynamically adapting to users, datasets, and workloads throughout the business, no matter where they are.

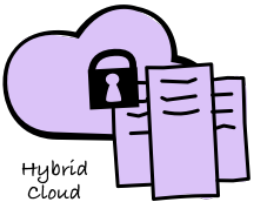
OPTIMAL CLOUD SECURITY COMES IN MANY SHAPES AND SIZES

Adopt SaaS applications. Cloud-delivered applications and services provide tremendous benefits and business agility. With increased visibility and in-line security controls, increase your productivity, remain agile, and limit your exposure to new security risks. Consider integrating tools for adaptive access, data loss prevention, and cloud access security brokers (CASB).

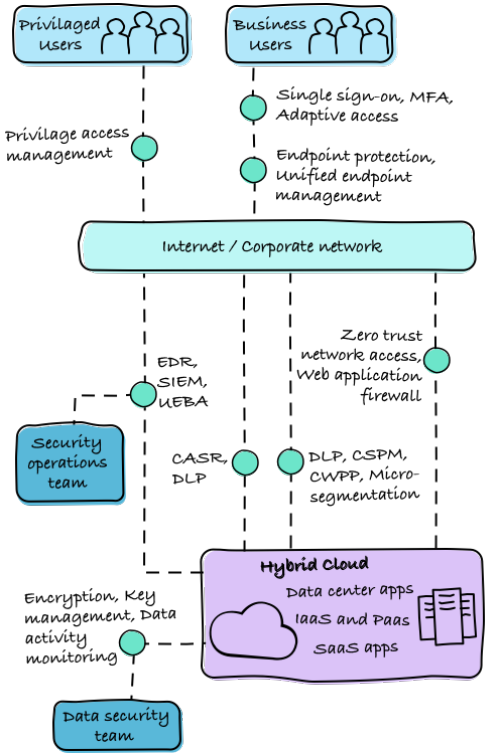
Migrate data and workloads to cloud. Most enterprise workloads currently running in public clouds are the result of lift-and-shift of existing apps and data to achieve cost reductions and IT efficiencies. However, the security controls in this environment are significantly different than traditional data centers. A zero trust framework can provide more consistent policy enforcement and reduce the potential attack surface that often arises from adopting new cloud platforms. Consider integrating tools for cloud infrastructure and entitlement management, multicloud key management, and privileged access management.

Learn more

Check out how to help protect the hybrid cloud.
https://www.ibm.com/security/zero-trust/cloud



Modernize enterprise applications. As new applications are built using cloud-native technologies like containers, service meshes, APIs, and Kubernetes, security needs to shift left and become embedded in the development cycle, and become more consumable for developers who are not security experts. Security teams maintain oversight and visibility into the security of the hybrid cloud environment without restricting innovation or the progress of the business. Consider integrating tools for cloud security posture management, cloud and container workload protection, API security, and DevSecOps.



Protect the hybrid cloud with zero trust to bring centralized visibility, context, and management that consistently enforces security policies and helps your organization innovate quickly without delays.

Secure the hybrid workforce

Businesses support their workforce from any location on any device connected to resources in multiple environments. Organizations empower their workforce by correlating security information across all domains to quickly enforce conditional access based on a model of least privilege. This reduces barriers to access resources without sacrificing security.

IN THE OFFICE OR AT HOME, USERS ARE THE BIGGEST RISK

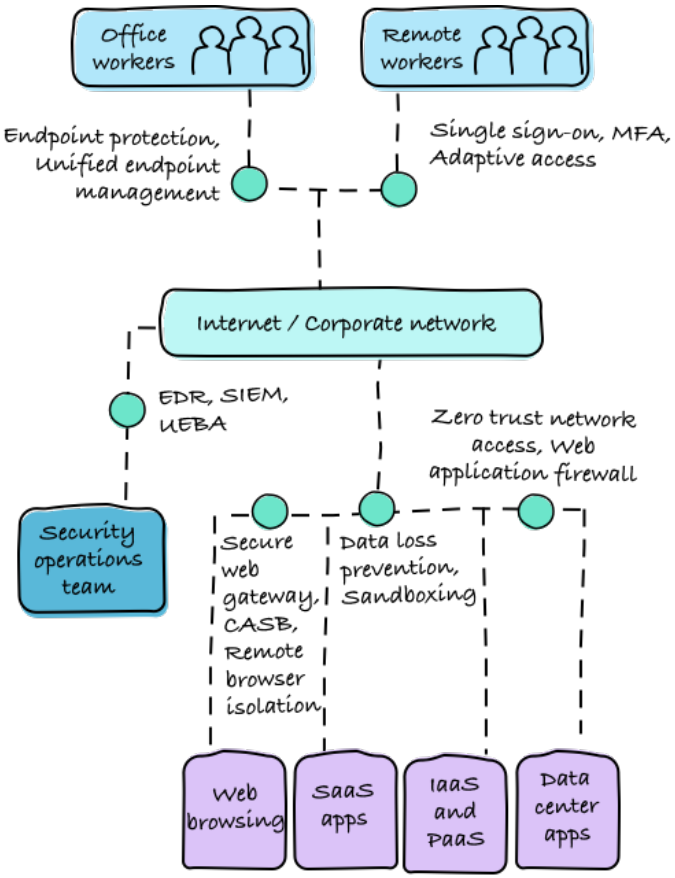
Replace VPNs to reduce network access risk. With virtual private networks (VPNs), users have access to an entire network or segment of a network. Alternatively, users should be given access only to required applications. This reduces the attack surface and can provide an improved and more consistent user experience as users move between remote and in-office interactions. Consider integrating tools for adaptive access, zero trust network access, and micro-segmentation.

Protect employees from phishing attacks. It only takes one mistake to lead to a security incident. The ability to block or quickly remediate a phishing attack is crucial. Consider integrating tools for email filtering, mobile threat management, and multifactor authentication (MFA).

Secure risky Internet behavior by end users. Users frequently combine their digital private life with their digital work life. Protecting users and their devices as they navigate the Internet helps reduce the risk of spreading malware infections throughout the organization. Consider integrating tools for DNS security, remote browser isolation, sandboxing, and endpoint detection and response (EDR).

Learn more

Check out how to to help secure the hybrid workforce.
https://www.ibm.com/downloads/cas/ZY8GN1NZ


Office workers
Remote workers
Endpoint protection, Unified endpoint management
Single sign-on, MFA, Adaptive access
Internet / Corporate network
EDR, SIEM, UEBA
Zero trust network access, Web application firewall
Security operations team
Secure web gateway, CASB, Remote browser isolation
Data loss prevention, Sandboxing
Web browsing
SaaS apps
IaaS and PaaS
Data center apps

Reduce the risk of business disruption

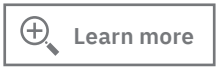
Persistent attacks like ransomware can be costly and disruptive to the business. Proactively isolate threats, insulate your most valuable resources, dynamically enforce security controls, and automate responses to threats targeting your business with a zero trust approach.

RANSOMWARE, MALWARE, AND INSIDERS! OH MY!

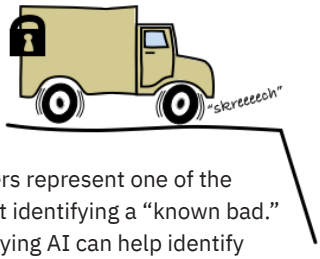
Proactively protect against ransomware. The first goal is to prevent an infection. When prevention is not feasible, reduce the attack surface. It is important to identify your high value assets, methodically enforce the principle of least privilege, and limit the ability for ransomware to move laterally through your environment. Consider integrating tools for data discovery and classification, adaptive access, and microsegmentation.

Respond quickly to ransomware. Detect and respond to ransomware quickly to reduce the risk of business disruption. Rehearse incident response through adversarial simulation and pen testing, and ensure you have a well-defined backup and recovery plan. Consider integrating tools for vulnerability management, endpoint detection and response, and SOAR.

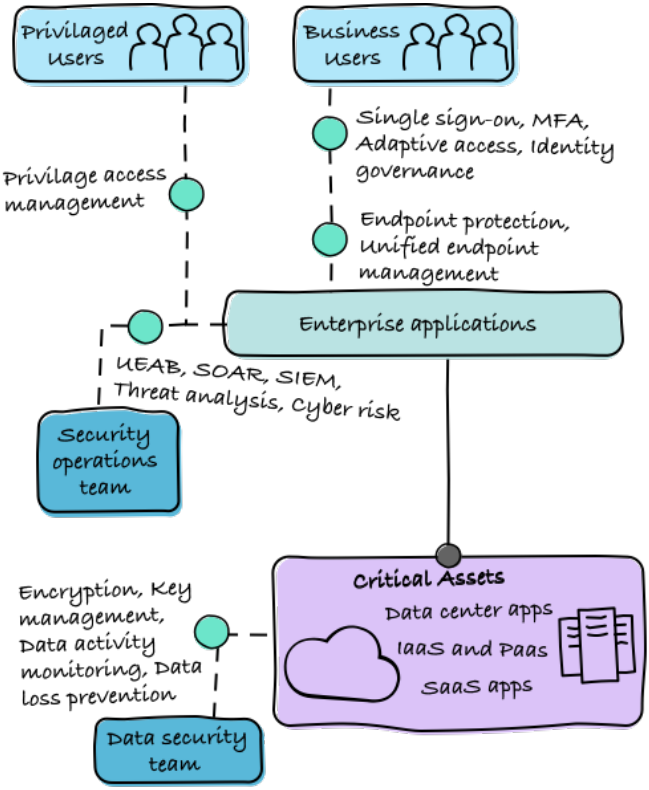
Protect user credentials. Insider threats are most frequently the result of user negligence or stolen credentials. Proactive protections that restrict access and focus on increasing the level of identity assurance can help prevent data breaches. Consider integrating tools for multi-factor authentication, privileged access management, and endpoint protection.



Check out how to reduce the risk of business disruption.
https://ibm.biz/zt-address-insider-threat



Stop malicious insiders. Malicious insiders represent one of the biggest challenges because it is not about identifying a "known bad." Sharing context across domains and applying AI can help identify insider threats and dramatically reduce response time. Consider integrating tools for user and entity behavior analytics (UEBA), data activity monitoring, and SOAR.



Infuse zero trust into the hybrid cloud infrastructure

A true defense-in-depth zero trust approach requires security embedded at all layers of the IT stack, including the cloud service and hardware. This extra level of hardware security is especially relevant in government or highly regulated industries like financial services, healthcare, and energy.

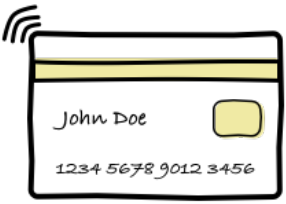
ZERO TRUST WOVEN INTO THE FABRIC OF CLOUD & DATA CENTER

Cloud infrastructure must be secure-by-design. Whether public or private, hybrid multicloud environments must have embedded security controls for identity, data, network, and workloads. Additionally, hybrid cloud platforms must have out-of-the-box integration with existing threat management and SOC tools like an XDR.

Encrypt data at rest, in transit, & in use. For sensitive data, and highly regulated industries, encrypting data at rest and in transit is not enough. Confidential computing isolates sensitive data during processing making it accessible only to authorized programming code, and invisible and unknowable to anything or anyone else. In a hybrid cloud environment, you can apply confidential computing from public cloud to mainframes.

Keep your data safe in an air-gapped backup. Having a backup and recovery plan is essential. Backups connected to your active systems are as susceptible to ransomware as your production copies. More advanced storage systems with logical airgap, enhanced security, and rapid restores can help recover from attacks.

Check out how confidential computing enables least privilege for sensitive data.
https://www.ibm.com/cloud/learn/confidential-computing

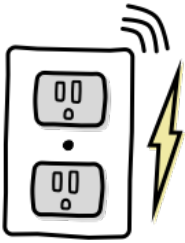


Banking and Financial

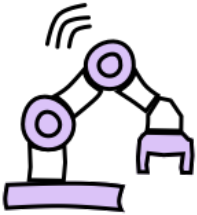
Insurance

Utilities

Healthcare



Energy



Manufacturing

Adapt zero trust to the NIST Cybersecurity Framework

The US National Institute of Standards and Technology (NIST) published the Cybersecurity Framework, which is used by many security practitioners both in the public and private sectors for guidance on how organizations can manage and reduce cybersecurity risk. One approach to adapting zero trust to the NIST Cybersecurity Framework is to think about the functions of the framework in the context of zero trust components that would fulfill those capabilities.

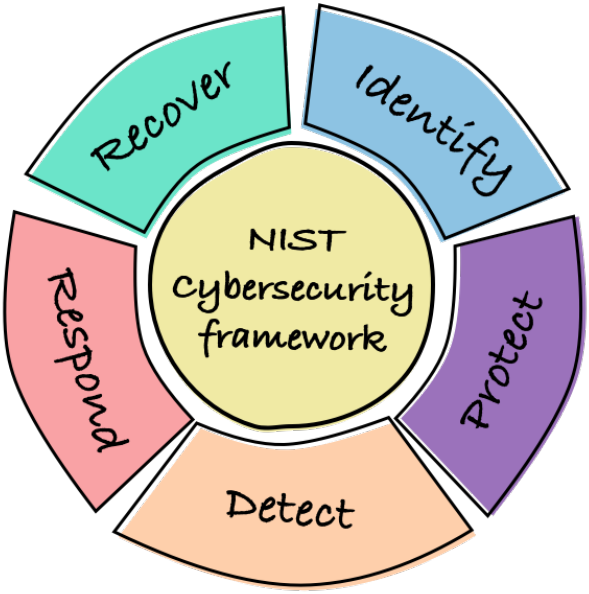
CYBERSECURITY FRAMEWORK TO ZERO TRUST MAPPING

The current NIST publication (NIST.SP.800-207) distinguishes between zero trust and a zero trust architecture.

Zero trust. "Zero trust (ZT) provides a collection of concepts and ideas designed to reduce the uncertainty in enforcing accurate, per-request access decisions in information systems and services in the face of a network viewed as compromised."

Zero trust architecture. A zero trust architecture (ZTA) is defined as "an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies."

Check out IBM resources on how to adopt the NIST Cybersecurity Framework.
https://www.ibm.com/cloud/learn/nist-cybersecurity-framework



A mapping of components that are categorized based on the NIST cybersecurity framework and how they are used in the context of a zero trust architecture.

A practical approach for the ongoing zero trust journey

Implementing zero trust renovates cybersecurity in a way that involves more “request for permission” than users are accustomed to. However, when it is implemented, it becomes routine and integrated with your current security policies and practices.

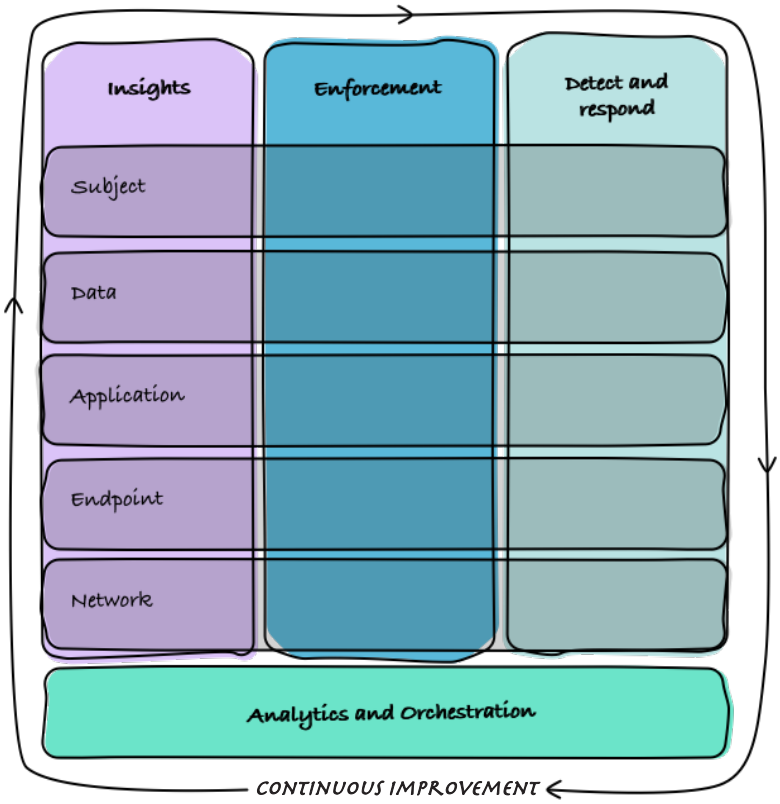
EVOLUTION NOT REVOLUTION!

Organizations should strive to evolve towards zero trust principles, processes, and technology solutions to secure highest value and risk data assets versus overhauling the entire cybersecurity approach all at once. Many companies continue to operate in a mode where zero trust and more classic perimeter-based security models coexist for a period of time while evolving their security architectures.

A practical approach to moving to an architecture based on zero trust principles involves using a framework that encourages continuous growth and road-mapping while providing an entry point for progress. IBM Security’s Zero Trust Framework focuses on turning a philosophy into action.

Continually repeating this framework in the context of your prioritized use cases across your organization’s identified subjects (users and systems), data, applications, endpoints, and networks will enable the evolution of zero trust for your enterprise.

Check out how to get started and succeed on your zero trust journey.
https://www.ibm.com/security/zero-trust



A zero trust approach aims to wrap security around every user, every device, every connection — every time.

IBM can help

IBM Security experts can guide you to identify the right use cases and initiatives to get started now. Align your stakeholders with the right goals, model your outcomes with the right architecture, and build the right solutions.

YOU BRING YOUR FRIENDS AND WE'LL BRING OURS

The IBM Security Framing and Discovery workshop is the first step to deliver accelerated zero trust results for your business. In this engaging, highly interactive, and collaborative working session, we work together to identify existing capabilities and gaps across the zero trust framework and develop it into an actionable use case (or use cases) that can be prioritized.

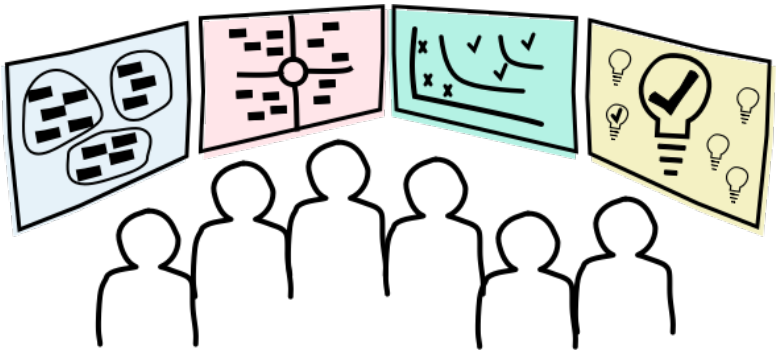
You can plan to bring 5 to 7 participants from your organization that include security executives, security leaders, architects, engineers, and operations. Diversity makes for unique solutions; however, participants should be familiar with your technical landscape and cybersecurity goals.

The workshop leverages tools to ensure and facilitate effective collaboration - virtually or physically.

The work session includes open discussions, cognitive thinking, and interactive exercises to drive towards actionable outcomes.

Learn more

Check out how to sign up for a no-cost Security Framing and Discovery workshop.
https://www.ibm.com/garage/services#2901281



YOUR LAUNCHPAD: SECURITY FRAMING AND DISCOVERY WORKSHOP

Focus. Align stakeholders around the most urgent and impactful zero trust goals for your business.

Collaborate. Gain insight on your critical subjects and how to best apply a zero trust approach.

Plan. Identify zero trust initiatives based on your desired security outcomes.

Let IBM help you create a unified view of business risk and prioritize your security investment!
https://www.ibm.com/security/services/security-governance/risk-management

Check out the National Institute of Standards and Technology (NIST) publication on zero trust architecture.
https://csrc.nist.gov/publications/detail/sp/800-207/final

Get involved with Open Cybersecurity Alliance (OCA) to contribute to new standards for zero trust interoperability.
https://opencybersecurityalliance.org

Notices

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the products and/or the programs described in this publication at any time without notice.

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

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

IBM ZERO TRUST