IBM Security Zero Trust Acceleration Services

Highlights

- Align governance to zero trust
- Select a zero trust use case
- Reach higher levels of zero trust maturity
- Plan and strategize your zero trust roadmap

Accelerate zero trust adoption

IT ecosystems have evolved significantly over the last decade from traditional, perimeter-based monolithic structures to complex, perimeterless multicloud environments. These new complex ecosystems disperse data, users, and devices across applications, platforms and workloads. As organizations transform digitally and the diversity of the security environment expands, new security models like zero trust can help bring context and insight into a rapidly evolving attack surface.

While the philosophy of zero trust has matured in scope for nearly a decade, the fact remains that it is challenging to implement and integrate across multiple security domains. Rather than focus on one functional area of security, zero trust forces security and risk leaders to shift into a business outcomes mindset, rooted in a unified strategy that accelerates business and IT objectives.

IBM Security helps organizations accelerate their zero trust journey by defining an integrated, multi-disciplinary zero trust strategy and offering a prescriptive set of steps needed to make it actionable. Our in-house security professionals can help organizations verify that users, data and resources are securely connected through a deny-by-default policy and authorization.

IBM Security Zero Trust Acceleration Services can help clients assess their current security gaps for a specific use case scenario against IBM Security's zero trust governance model and align priorities while addressing the organization's unique security risks, industry compliance requirements, and investment strategy.

Aligning zero trust governance to your security strategy

The zero trust governance model developed exclusively by IBM Security can help an organization achieve actionable progress toward zero trust maturity. The four core tenets of this zero trust governance model include:

- **Define Context** – Discover and classify resources based on risk. Coordinate actions across the ecosystem for consistency and context.
- **Verify and Enforce** – Protect the organization by quickly and consistently validating, enforcing and implementing zero trust policies and controls.
- **Rapid Response** – Resolve and remediate security incidents with minimal impact to the business by taking targeted actions based on context.
- **Analyze and Improve** – Continually improve security posture by adjusting policies and practices to make faster more informed decisions to tighten security around each resource.

Selecting a multidisciplinary zero trust use case

IBM Security professionals recommend a phased, use case-based approach to mature zero trust capabilities and integration across multiple security disciplines. Selecting a use case can allow your organization to incrementally mature security controls across the major security domains impacted by a zero trust strategy.

In addition, IBM Security professionals can help align your new zero trust strategy to existing frameworks like NIST, Cloud Security Alliance Capability Maturity Model, and other proven security frameworks for a new target state, including technology architecture, processes, and policies. This approach allows the organization to integrate security domains for intelligent, context-driven decision making.

Guiding your organization to the next level of maturity

IBM Security professionals first focus on assessing your organization's current security posture for your chosen use case through the principles of its zero trust governance model. Various in-person or virtual workshops are conducted to provide prescriptive recommendations that guide the security team from its current state to a new target state.

The maturity assessment includes a broad review of current infrastructure, technologies and tools, workflows and business processes and individual roles and responsibilities of groups. The goal of the assessment is to understand the gaps that exist within your current security landscape. This information is then applied to the domains within the use case, including identity and access management, data security and privacy, network, device, endpoint and application security. Lastly, the output provides clients with a maturity rank against IBM

Security's Zero Trust Maturity Model.

Planning and strategizing your zero trust roadmap

Once the maturity assessment is complete, IBM Security professionals can help strategize a target or future state zero trust architecture and provide recommendations in a roadmap document. In addition, the target state architecture and roadmap can be leveraged as a reference model for planning future zero trust transformation projects.

The phased roadmap illustrates the target state zero trust capabilities and various points of integration across security domains. In addition, IBM Security professionals can prescribe which existing or new technology tools and technologies will be needed to support the execution and deployment of new zero trust capabilities. Finally, a formal project business case is developed to document the strategy and approach for the adoption of recommended zero trust capabilities.

Make zero trust actionable

Whether your organization is unsure of how to get started with zero trust or simply needs help maturing existing capabilities, IBM Security professionals can help organizations apply zero trust to the most relevant use case scenarios for your enterprise today.

IBM Security Zero Trust Acceleration Services was designed to help organizations:

- Identify security gaps against IBM Security’s zero trust governance model
- Build a detailed zero trust security roadmap aligned to your company’s unique security, industry compliance and investment strategy requirements
- Follow a use case-based approach to help mature new or existing zero trust capabilities across multiple security disciplines for faster zero trust adoption

Increase the effectiveness of your overall security program with the right business outcomes driven by zero trust. Contact an IBM Security expert today to schedule a zero trust strategy consultation:

Why IBM?

IBM Security Services professionals can offer helpful zero trust expertise, broadened by access to IBM's research and development team. Available worldwide, IBM experts can tailor recommendations to your organization's and region's unique circumstances. Our approach to consulting and managed services examines impact at every level of your organization—from business strategy to applications to IT infrastructure—to help you implement a zero trust strategy designed to meet your business and IT objectives.

Next steps

→ Talk to our specialists about Zero Trust Acceleration Services

For more information

To learn more about the IBM Security Zero Trust Acceleration Services, please contact your IBM representative or visit the following website: https://www.ibm.com/security/services/zero-trust

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: ibm.com/financing

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:
IBM Security Zero Trust Acceleration Services™