An open and unified approach to Zero Trust that puts security everywhere, so your business can thrive anywhere

Today, organizations must adapt to a rapidly expanding and complex security landscape. They must protect infrastructures distributed across hybrid cloud, edge, IoT and OT environments. They must secure the future of work as employees, customers, suppliers and partners are accessing data from anywhere, using any device. They must stay vigilant against today's evolving threat landscape as ransomware and other sophisticated attacks continue to disrupt the business. All of this while maintaining regulatory compliance and privacy demands as more and more data is being shared.

Despite all this complexity, security must somehow accelerate with the speed of business. This is why security leaders are looking to adopt a zero trust strategy that instructs security to:

1. Establish a state of least privilege, so no user or app has any more access than what's needed
2. Verify continuously, as apps and users access data and tools
3. Always assume there's a breach

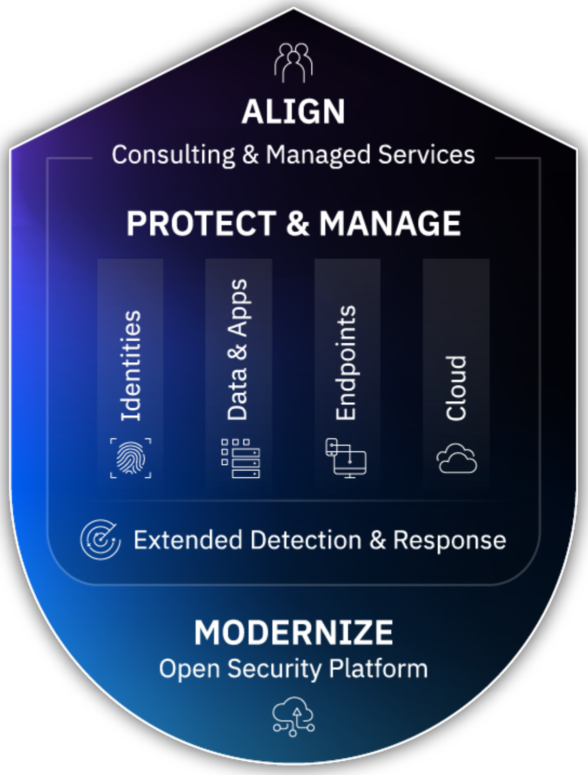
Zero trust can do more than just prevent bad things from happening – if done right, it can enable real business outcomes:

- Reduce security risks associated with hybrid cloud modernization, which enables faster adoption.
- Allow seamless user authentication, from any device, so employees can be more productive.
- Improve business continuity through reducing attack risks.
- Enable organizations to build trust and improve customer experiences by maintaining compliance and privacy mandates.

Adopting a Zero Trust approach will accelerate security maturity so it shifts from...

- Static network-based to dynamic perimeter-less security
- From manual to automated security with the help of AI and machine-learning
- From reactive threat management to a proactive XDR approach
- From siloed bolted on security, to continuous security spanning multiple cross-disciplines like DevSecOps
- And finally, shift from using proprietary and disparate tools to open and connected solutions

IBM **Security**



IBM Security offers an open and unified approach to Zero Trust that puts security everywhere, so your business can thrive anywhere.

ALIGN
Your security strategy to your business with the help of our consulting and managed services

PROTECT
Identities, data, apps and infrastructure whether in the cloud, on mobile devices or on-prem to establish least privilege and verify access continuously.

MANAGE
Defenses against growing threats in an assumed breach with open XDR solutions and services to manage threats across the entire lifecycle.

MODERNIZE
Your security architecture with an open platform that connects to your ecosystem of vendor tools.

IBM Security solutions are backed by decades of investment and differentiated by our leadership and expertise across 15 leading security segments. AI and machine-learning technology is embedded across our entire portfolio. Our open security platform is built on a foundation of Linux and Kubernetes which enables it to run anywhere. And because building a zero trust strategy involves leveraging your existing and future investments, we have built one of the largest ecosystems in the world which includes thousands of open integrations.

IBM