E-book Series

Microsoft Security

Meet regulatory and compliance requirements

Meet your current regulations and better adapt to new or future requirements

Keeping up with evolving regulatory requirements is challenging

Regardless of the complexity of your organization's IT environment, new regulatory requirements are continually adding up and you need to ensure your IT systems keep pace. Regulations such as the European Union's General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and data residency requirements necessitate strict data privacy and management controls. These processes can be long, complex, and tedious when not managed appropriately. This challenge has massively increased the workload of security, compliance, and regulations teams to achieve and prove compliance, prepare for an audit, and put practices into place.

While many organizations use various legacy solutions to stitch together to serve this purpose, these solutions often don't work together seamlessly, thus exposing infrastructure gaps and increasing operational costs. Relying on traditional virtual private networks (VPNs) leaves you with outdated identity management solutions, ineffectual device management controls, or governance policies. It further increases the risk of security breaches, and restricting access policies creates gaps in the employee experience. At the same time, lack of adherence can also lead to significant drops in revenue and decrease customer employee and partner confidence.

A survey of US-based decision makers showed that to meet their compliance and data-protection needs, almost 80 percent had purchased multiple products, and a majority had purchased three or more.

Source: February 2022 survey, commissioned by Microsoft with MDC Research.

Zero Trust strategy to accelerate and ease your journey

Implementing a Zero Trust architecture helps you meet regulatory and compliance requirements with a comprehensive strategy. Govern, protect, and manage your organization's entire data estate while providing unified data governance and risk management. Zero Trust strategies often exceed other regulatory requirements and perform fewer system-wide changes to adhere to new regulatory requirements.

An effective Zero Trust architecture helps to meet and accelerate your regulation and compliance journey by adhering to the following principles:

Verify explicitly

Always make security decisions using all available data points, including verifying every identity, location, resource, and data classification while identifying device health and anomalies.

Use least-privilege access

Limit access with just-in-time/just-enough-access (JIT/JEA) and risk-based adaptive policies. Capture and analyze telemetry to better understand and secure your digital environment, ensuring you can discover and secure unmanaged endpoints and network devices.

Assume breach

Minimize blast radius with micro-segmentation, end-to-end encryption, continuous monitoring, and automated threat detection and response

Implementing compliance and regulatory requirement with Zero Trust principles

Visibility matters in a Zero Trust approach, and effective endpoint management is a significant factor in delivering it. Improve the effectiveness of regulatory and compliance programs by providing:

End-to-end visibility and discovery of critical assets

Unifying your security strategy and policy with a Zero Trust approach breaks down siloes between IT teams and systems, enabling better visibility and protection across the IT stack. A real-time level of visibility allows automatic discovery of assets, including critical assets and workloads, while compliance mandates can be applied to these assets through classification and sensitivity labeling.

A Zero Trust model is a proactive, integrated approach to security across all layers of the digital estate that explicitly and continuously verifies every transaction; asserts least-privilege access; and relies on intelligence, advanced detection, and real-time response to threats.

Rules and policy enforcement

Complete visibility allows you to intercept data requests and explicitly verify signals, while applying and automating Zero Trust security policies across your entire data estate. Analyzing productivity and security signals also helps you to evaluate your security culture, identifying areas for improvement or best practices for compliance and regulatory requirements.

Network segmentation

Visibility also helps you at a granular level when you segment compliance-critical workflows. Network segmentation reduces risk, helping prevent attackers from moving laterally across your network, and ensures compliance. With an audit trail, you can also make incident response and documentation more straightforward in case of a breach.

Least-privilege access and device compliance

By following least-privilege access principles and verifying every access with strong authentication, you're making sure access is compliant and typical for that identity. Once access has been granted, Zero Trust security ensures continuous monitoring while enforcing device health and compliance checks for secure access to reduce any threat issue or risk.

How a Zero Trust approach benefits businesses security and compliance agility

A Zero Trust approach not only helps you solves security problems and addresses evolving regulatory requirements—it also helps your business grow with increased agility and efficiency.

Enhanced audit and compliance management.

A Zero Trust approach makes it easier for your security and compliance personnel to audit their environment and understand the policies they need to implement to comply with internal and external governance requirements. Enable continuous assessments—from taking inventory of data risks to implementing controls, staying current with regulations and certifications, and reporting to auditors. With ongoing assessments and monitoring, audits are streamlined; therefore, you're minimizing the effort required to support compliance faster and more efficiently. Your compliance personnel can retain and easily recall necessary documentation, improving accuracy and reducing time when conducting audits.

Increase compliance agility and adaptation

A Zero Trust approach often exceeds compliance requirements; organizations may find that they already meet a new condition or need to do additional work to be compliant. It enables teams to simplify ongoing and upcoming compliance requirements and eases the journey to achieve new regulatory compliance certificates.

Increase business reliability and integrity

Implementing Zero Trust principles enables you to protect the reliability and integrity of critical business processes. It ensures privacy, integrity, and availability guarantees for data and applications. By integrating robust security controls and architectures, you're able to restrict the impact of threat events and support greater resiliency and efficiency. Integrating a Zero Trust model into your culture also helps you embrace new security standards and guidance. By removing artificial constraints to operating workflows, you can operate processes effectively in a compliant and regulated manner and enable organizational agility and entrance into new markets and territories.

A Zero Trust approach from Microsoft helps reduce resources required for audit and compliance management by

Source: The Total Economic Impact™ Of Zero Trust Solutions from Microsoft, December 2021.

Start your journey with Zero Trust security

With a Zero Trust strategy, you can deliver on improved and modernized security while driving tangible business results.

To learn more, visit aka.ms/zerotrust