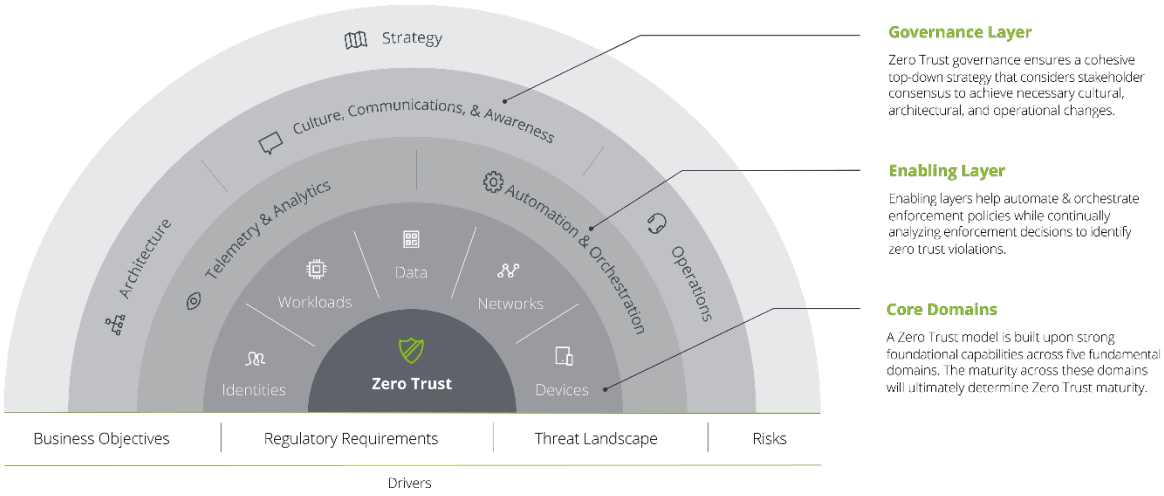
Deloitte.

Zero Trust Framework



Core domains: Identities, Workloads, Data, Networks, and Devices

Identities are the new "perimeter"—a core component of a Zero Trust network is shifting to identity and contextual risk-based access control decisions based on user profile, entitlements, authorization, and acceptable usage patterns.

Workloads are applications or services people use, either on legacy infrastructure or in cloud environments and containers. They may be hardened, segmented, and monitored at a granular level with adaptive actions, such as limiting access or blocking uploads to specific applications.

Data lies at the heart of an effective Zero Trust framework. Organizations need to understand what data they have, where that data is stored, as well as who and what should be able to access that data, and under what conditions. Data should also be protected through obfuscation, encryption, and advanced data loss prevention mechanisms.

Networks establish communication between identities, devices, and workloads. A Zero Trust Architecture begins with the assumption that network connection requests are inherently untrustworthy.

Devices include both known and managed endpoints, unmanaged ones, and smart devices that connect to an organization's network and enterprise assets. Devices should be subject to continuous assessment for risks and threats and to evaluate their compliance with the defined security policies.

Deloitte.

Enabling Layer: Telemetry & Analytics; Automation & Orchestration

The next ring encompasses what we consider the Enabling Layer. We consider these horizontals because we see them as the stitching that holds the Core Domains and their respective capabilities together. Telemetry & analytics systems collect data and threat intelligence from relevant security controls into a centralized platform for event correlation and advanced analysis that may help detect suspicious and potentially malicious behaviors. As modernized controls are implemented, the associated telemetry should be ingested to help enhance situational awareness of network and user access patterns.

Automation & orchestration capabilities help empower a more proactive security posture by automating detection, prevention, and response actions through integrated security controls, leading to more productive security operations which may become even more productive when investigative tasks are automated.

Governance Layer: Architecture, Culture Communications & Awareness; Operations

The governance layer encompasses Architecture principles that should be defined and aligned to in a Zero Trust model. Culture Communications and Awareness socialize the potential impact on the end-user experience and the associated organizational change management updates to IT and security. The Operations team could also require alignment to manage new or modernized security controls.

Strategy Layer: Zero Trust Strategy

Finally, the outer ring encompasses the organization's Zero Trust Strategy, which should align with business drivers, making sure of the journey supporting the business and is not considered a science experiment or costly technology implementation.