



ZERO TRUST SECURITY



IDENTITY



ENDPOINTS



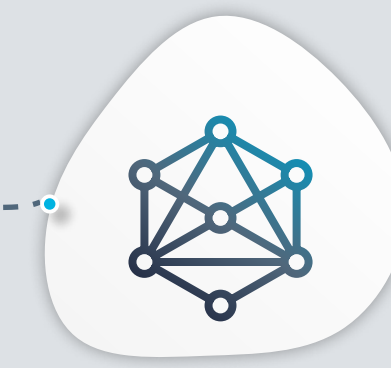
DATA



APPS

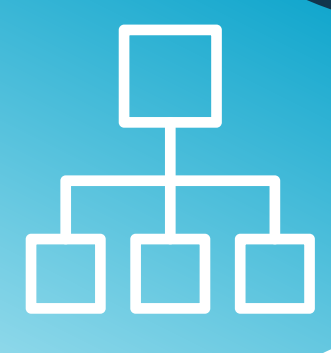


INFRASTRUCTURE

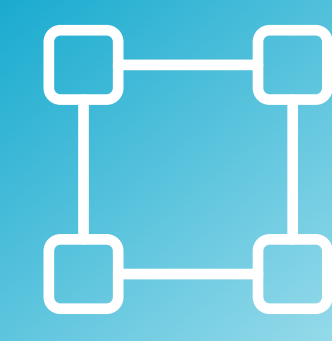


NETWORK

# ZERO TRUST | IN 2023 APPS



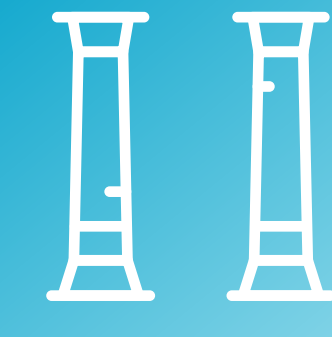
**Application access** in the context of Zero Trust is based on the security model used to manage access to an **organisations applications** at the application level.



When a user, regardless of if they are inside or outside the **network perimeter** wants to access an application, the access request is valuated based on **access controls**.



Additionally, with application access requests being justified on a case by case basis provides **enhanced visibility** into how those applications are being used, as well as reducing the **attack surface area** by only providing the minimum amount of access needed.



Application access links closely with the **Identity, Network and Visibility & Analytics** pillars of Zero Trust.

[LEARN MORE](#)

To prevent **lost productivity** and downtime, security, IT, and governance professionals must better secure and manage messaging and collaboration tools. Mimecast delivers a set of solutions that help organizations **better manage risk** through fast and accurate threat detection and remediation, as well as enhanced visibility into conversation topics and sentiments.

Mimecast solutions also diminish the risk of **shadow IT** by providing visibility beyond email to modern messaging and collaboration channels.