The Top Five Risks of Perimeter Firewalls

and the One Way to Overcome Them All

RISK #1 Large attack surface

HOW ZERO TRUST CAN HELP:

Unlike firewalls that expose applications on the internet to make them easy to find, a zero trust architecture conceals source identities and obfuscates IP addresses to ensure that applications remain invisible and accessible only by authorized users.

RISK #2 Choking application performance

HOW ZERO TRUST CAN HELP:

An integrated zero trust approach enables direct, secure, and fast connections to cloud applications, eliminating backhauling and data center choke points inherent to firewall-centric architectures.

RISK #3 High operational complexity and costs

HOW ZERO TRUST CAN HELP:

When using the internet as the corporate network, zero trust eliminates the need for costly and complex firewalls, MPLS networks, and VPNs by placing security controls in the cloud close to where users and applications are located.

RISK #4 Lateral threat movement

HOW ZERO TRUST CAN HELP:

A true zero trust architecture eliminates the lateral movement of threats and reduces risk by directly connecting authorized users only to authorized applications–unlike firewalls that put users on the corporate network to access applications.

RISK #5 Data loss

HOW ZERO TRUST CAN HELP:

Zero trust provides consistent, unified security at scale for data in motion and data at rest—including encrypted traffic—across SaaS and public cloud applications, which is a struggle for firewalls and virtual machines.

Want more details on overcoming the risks of perimeter firewalls with a modern zero trust approach?

Read the full guide

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com