Four SD-WAN security hurdles to overcome

The biggest challenge for SD-WAN is that traditional security solutions are not enough

Let's examine four hurdles to overcome on your SD-WAN journey, as well as the most effective way to secure your deployment.

Hurdle 1 Relying on the firewall in your SD-WAN edge device

Only using native SD-WAN security leaves significant blind spots.

Most don't have advanced threat protections, such as NGFW, sandboxing, advanced threat prevention, IPS and DNS security.

What to look for in a solution?

- An application-, protocol-, and context-aware cloud-based firewall.
- Inspection of traffic on and off-network for all users, apps, devices, and locations.
- The ability to make access decisions based upon request contents, not just destination.

Hurdle 2 Abandon the idea that traditional security approaches are up to the task

Cutting corners kills efficiency.

Deploying appliances at every branch is prohibitively expensive and leads to comprises in security or performance.

Backhauling traffic to regional hubs is also not the answer as it leads to latency and increased cost.

What to look for in a solution?

- Identical protection for all users with comprehensive, cloud-delivered security.
- The breakout and inspection of all ports and protocols, including SSL-encrypted traffic.

Hurdle 3 Don't count on existing security architectures to handle encrypted traffic

Inspecting encrypted traffic is critical.

Traditional firewalls do not natively inspect SSL traffic.

Turning on inspection typically degrades performance, which leads to some companies bypassing SSL inspection, putting them at greater risk.

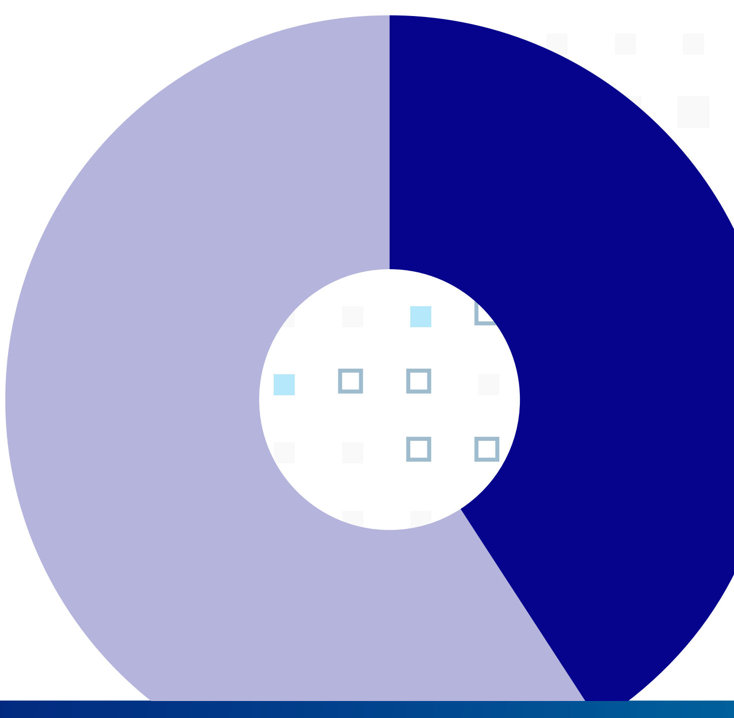
What to look for in a solution?

- A proxy-based architecture that natively inspects SSL-encrypted traffic.
- Inspection of all traffic without degrading performance.
- Elastic scalability as traffic and the number of users grow.

More than

41%

of network attacks today use encryption to evade detection[1].



Hurdle 4 Avoid the trap of multiple security management platforms

Legacy technologies are challenging.

Collecting and correlating activity is difficult.

Implementing policy changes typically requires individual management interfaces or manual deployment.

Providing timely visibility and reporting is complicated with appliances scattered across every branch.

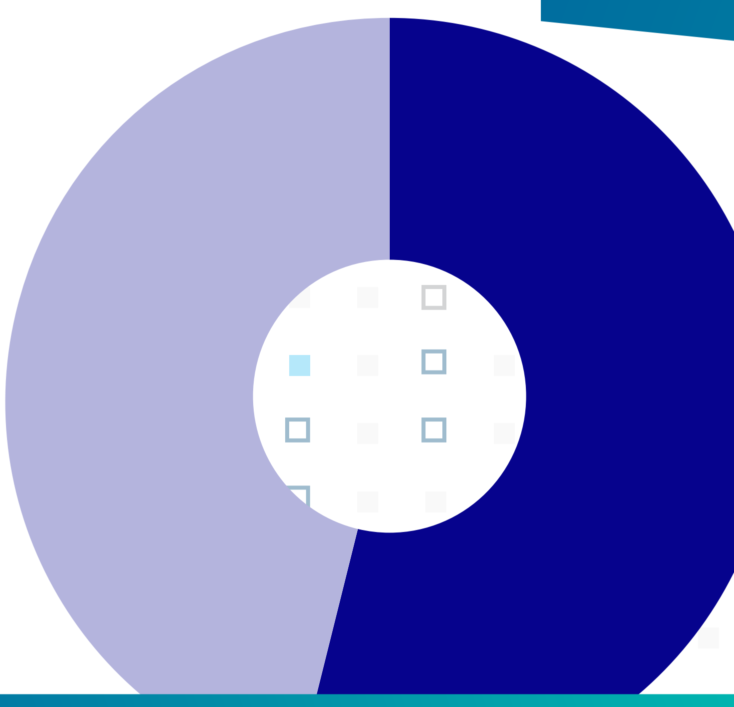
What to look for in a solution?

- A flexible framework that provides actionable insights.
- A single platform to correlate and view logs.
- The ability to centrally define and immediately deploy policies to all locations.

54%

of organizations

reported increased technology complexity as the top concern regarding current methods for securing internet connections across locations[2].



Want to learn more?

Read the Full Whitepaper

zscaler

[1] Ponemon Institute, "Hidden Threats in Encrypted Traffic: A Study of North America and EMEA." 2016
[2] Network World, Inc. survey of IT Directors across 100 organizations

zscaler.com