7 Symptoms Your Legacy Firewall Isn’t Fit for Zero Trust

Decades ago, hub-and-spoke network designs and perimeter firewalls were spry and healthy, and they served a purpose. In the modern cloud computing era, they’re showing signs of aging—not as quick as they used to be, using outdated firewall rules, and unable to offer inline, real-time protection against malware or protect SaaS apps from lateral movement.

In a world where 85% of IT professionals say firewalls are best delivered from the cloud, they’re proving that next-generation firewalls are last generation, and that data center-centric architectures are fundamentally incompatible with the zero-trust paradigm.

In this ebook, we’ve outlined symptoms that show how your firewall might not be fit for today’s zero trust security world, including:

- Congestion and lack of real-time visibility when inspecting traffic at scale
- High risk of internet-borne infections spreading across your hybrid cloud
- “Policy inflammation” from too many rules slowing you down
- Inability to see or stop lateral movement or ransomware

If your firewall is showing any of these symptoms, you might need a cloud firewall cure. *Read 7 Symptoms That Tell You Your Legacy Firewall Isn’t Fit for Zero Trust to find out more.*