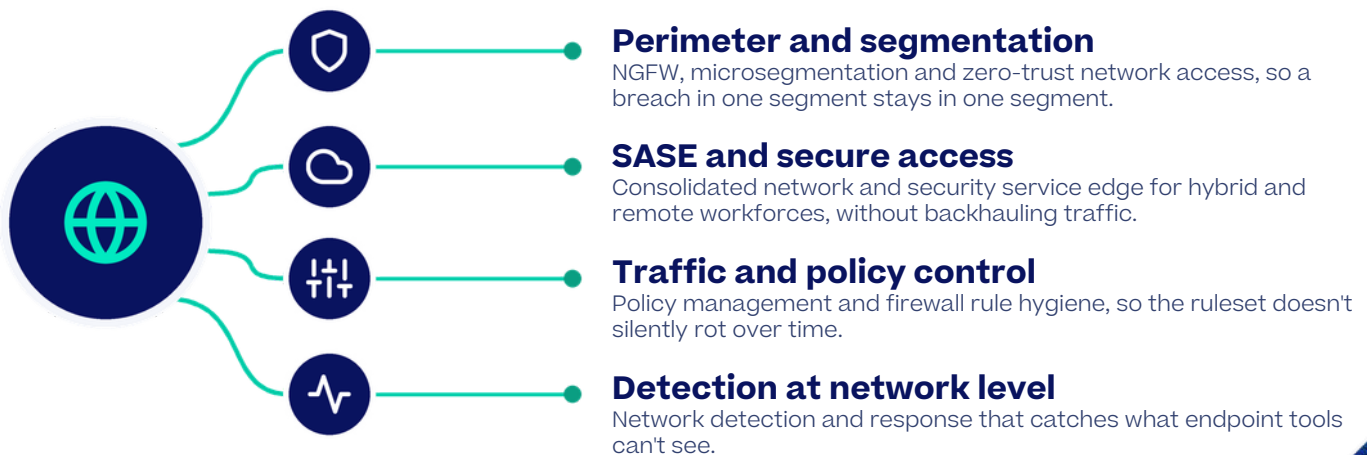


NETWORK SECURITY

NGFW, SASE, segmentation and zero trust, designed for your risk profile.

The network carries everything, which is why locking it down and keeping it fast keep colliding. We design and implement network security architecture against your actual risk and compliance profile, then run it so maintenance stays scheduled.

SECURE THE NETWORK WITHOUT SLOWING IT DOWN.



WHY DIGITALERA

Vendor-agnostic method

A documented 4-step method, so the shortlist fits your environment.

Deployed with tuning

Professional Services stays through the tuning period after go-live.

NOC-backed operation

Managed Networking keeps the architecture holding, 24/7.

No lock-in

Exit at contract renewal, with no penalty for leaving.

HOW WE SELECT

- 1 Assess**
 Coverage gaps and ranked risk, before any product demo.
- 2 Shortlist**
 2 to 3 fits, scored on your environment and budget.
- 3 Deploy and integrate**
 Configure, integrate and tune, with support after go-live.
- 4 Run it or hand it back**
 Move into the matching managed service, or keep it in-house.

VENDOR ROSTER

Palo Alto Networks	Zscaler
Fortinet	Cloudflare
Darktrace	Cato Networks

+ 13 more, listed online

WHERE IT CONNECTS

Start here
Network Assessment

Runs with
Cloud Security

Feeds into
Managed Networking

Right fit if you need segmentation, NGFW or SASE designed against your actual risk and compliance profile.

Something else first if you haven't mapped what's exposed yet (start with Network Assessment) or you're mid-incident (call the emergency line).



Talk to an expert

digitaleragroup.com/contact/network-security

Active incident? Certified responders answer 24/7, no retainer required.

CALL US: 1-786-621-8600