THE CISO PERSPECTIVE

TECH INSIGHT. NO HYPE.

VIDEO CHEAT SHEET

On-Prem vs SASE

What Should Stay Local (and What Moves to the Cloud)

cisoperspective.com

Watch the video

TL;DR

Moving security inspection to the cloud doesn't automatically make it better, and keeping everything on-premises doesn't necessarily provide every capability you need. Here are 13 capabilities, placed where each works best.

70%
Percent of SD-WAN purchases will be single-vendor SASE by 2028
Gartner, Magic Quadrant for SASE Platforms · 2025

13
Security capabilities compared, from antivirus to SSPM and DSPM
The video's three parts: A, B and C

5
Decision factors: effectiveness, performance, cost, complexity and resilience
The video's comparison criteria

THE VERDICT MAP

A = Network security · B = Secure access & data protection · C = SaaS & cloud posture

ON-PREMISES 5

- **A** Antivirus & Malware — Local inspection, if detection matches
- **A** Application Control — Sees traffic that stays local
- **A** Network Firewall — Full NGFW + local segmentation
- **A** Intrusion Prevention — Inspects inbound + internal traffic
- **A** IoT & OT Security — Can't run agents: protect locally

HYBRID 3

- **A** Web Filtering — Both work; depends on PoP proximity
- **A** DNS Security — Lightweight: both models work together
- **B** Zero Trust Network Access — Depends where users and apps live

Why hybrid? Both approaches work well. The better fit depends on where your users, apps and data are located.

CLOUD-DELIVERED 5

- **B** CASB — SaaS APIs see off-network activity
- **B** Data Loss Prevention — Classification, context + SaaS
- **B** Remote Browser Isolation — Provider runs isolation at scale
- **C** SSPM — Risky SaaS settings + permissions
- **C** DSPM — Finds sensitive data exposure

KEY TERMS

PoP	Cloud point of presence where corporate traffic is tunneled for inspection.
Thin edge / CPE	Branch device that connects to the PoP. May offer only basic firewalling.
NGFW	Next-generation firewall: application inspection, segmentation, advanced security.
ZTNA	App-specific access by user identity, device posture and context. No traditional VPN.
SSPM / DSPM	Find risky SaaS settings and permissions / sensitive data and its exposure in the cloud.

DECISION CHECKLIST

Ask for each capability

- ☑ Where do the users, apps and data actually live?
- ☑ Does this traffic ever leave the local network?
- ☑ Can the device run an agent? If not, protect it locally
- ☑ Is detection really equal? Don't assume it is

Then weigh

- ☑ Security effectiveness first, then performance where it matters
- ☑ PoP proximity and connectivity
- ☑ Cost, operational complexity and resilience
- ☑ Can the thin edge give full NGFW and segmentation?

CISO TAKEAWAY — **Place each capability where it provides the greatest benefit. For many enterprises, that means combining local and cloud-delivered security.**

JUMP TO A CHAPTER

Each one opens the video at that moment

- 0:00 Why on-prem vs cloud security
- 0:53 Two architectures
- 2:08 Antivirus
- 3:34 Web filtering/DNS
- 4:56 Application control
- 6:23 IPS
- 7:00 IoT/OT
- 7:54 ZTNA, CASB, DLP
- 9:50 RBI
- 10:24 SSPM/DSPM
- 10:58 Conclusion

TCP MEDIA

© 2026 TCP Media · Share with attribution · @cisoperspective

Watch the full video: youtu.be/qi-rZz7GMu4