

WHERE NETWORK SECURITY MEETS THE CLOUD

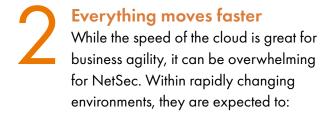




Security is more piecemeal

NetSec now has to operate and monitor
a range of tools, only to gain a blurry
picture of hybrid security. This leads to:

- Network blind spots.
- Slow mean time to repair.
- False positive security alerts.



- Manage more complex application connectivity requests.
- Continuously evaluate security policy and mitigate risks.
- Document changes for compliance in new areas.

App teams must cooperate
DevOps and CloudOps may unintentionally treat security as an afterthought while pushing innovation. That's why it's vital to achieve:

- Full on-premises and cross-cloud visibility.
- Close collaboration between NetSec and app teams.
- Security integration into DevOps tools and processes.

Misconfigurations are common
Misconfigurations are prevalent in the
cloud and frequently result in security
incidents. Common reasons for misconfigurations include:

- Skill shortage and poor understanding of network topology.
- Lack of effective security policy management.
- Overly permissive network access rules.

Compliance is elusive
Continuous compliance in the cloud is difficult to practice. Enterprises often struggle to accomplish:

- Centralized visibility into security and connectivity.
- A security posture that doesn't lapse into noncompliance.
- An adequate audit trail for compliance reporting.

IaC security is essential
Infrastructure as code (IaC) enables
cloud speed, but it can also introduce
security issues. Addressing these
concerns requires:

- Translation of security requirements into code.
- Careful evaluation of builds against security policies.
- Grasping the impact of changes before implementation.

