algosec | SECURELY ACCELERATE

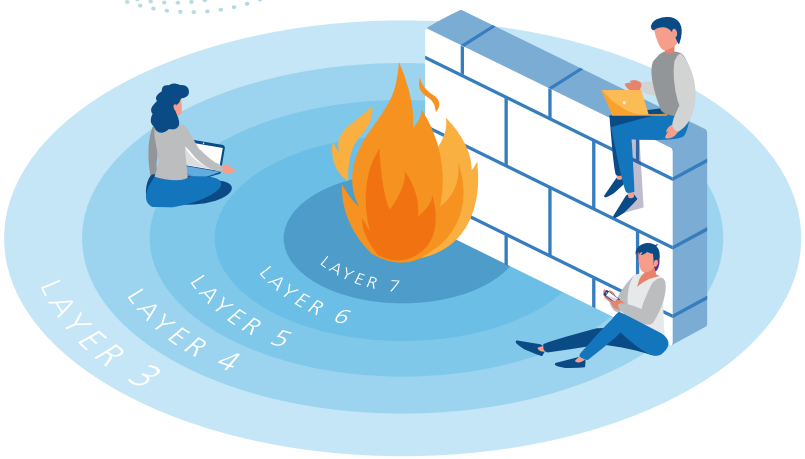
6 MUST DOS
TO SECURE THE HYBRID CLOUD

Managing security in a hybrid environment is complex. Follow these six best practices, and security management will be simpler.

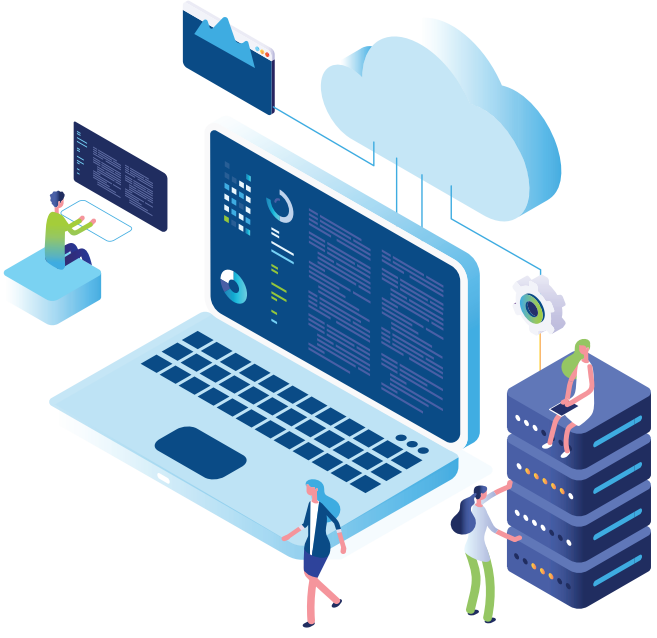
1 Use NGFWs in the cloud

Cloud providers' native security controls are not enough.

Next-Generation Firewalls (NGFWs) provide Layer 3 – Layer 7 protection capabilities.



49% of organizations report running virtual editions of traditional firewalls in the cloud.
(Source: CSA)



2 Use dynamic objects

On-premises, security policies are typically associated with static subnets or IP addresses. But in the cloud, workloads protected by traditional firewalls don't use static IP addresses. NGFW dynamic objects allow you to match a group of workloads using cloud-native categories.

3 Gain visibility over your entire hybrid network

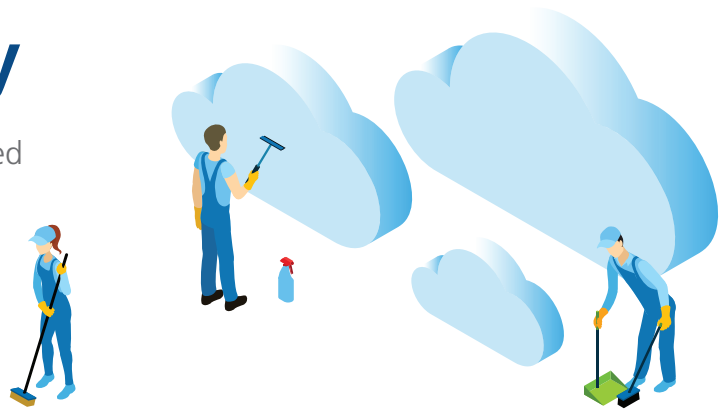
You can't protect what you can't see. Security should be evaluated in your cloud services AND in the path from the internet and data center clients.
It's important to have a single view over the entire network estate.

4 Evaluate risk over the entire hybrid network path

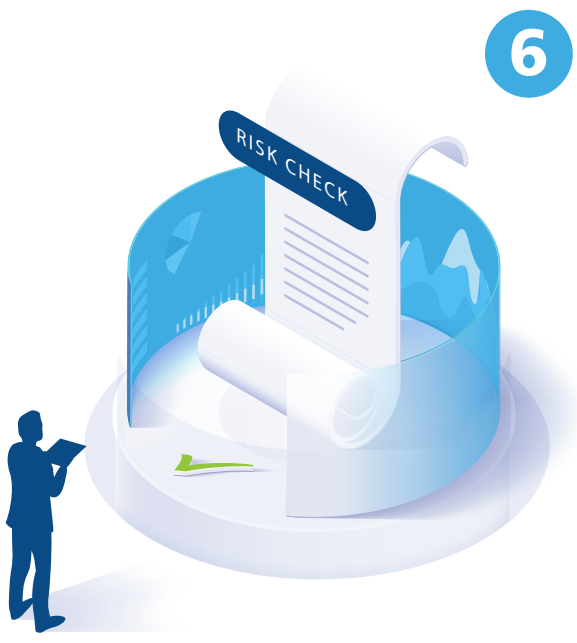
Consider risky traffic, not only in your cloud services, but also in the path from the internet and data centers.

5 Clean up cloud policies regularly

Cloud security groups are constantly adjusted so that they can rapidly bloat. This makes them hard to maintain and increases risk. Clean up your cloud security groups so that they are accurate, efficient, and avoid application outages.



6 Put "Sec" into DevOps: Maintain IaC security as part of the cloud change pipeline



Run a risk analysis and get detailed risk remediation recommendations that can be implemented using native DevOps methodology. Before a risk is introduced, run a what-if risk check as part of the code's pull request. Tighten the change to eliminate risk and only then push to production.

Find out how to keep your hybrid cloud secure and turn these best practices into action with the AlgoSec solution. Get a demo | Read the eBook | Watch the webinar