SECURITY-THE HYBRID WAY

HYBRID CLOUD INFRASTRUCTURE IS THE TREND NOW. IN FACT, RESEARCH SHOWS THAT AROUND 40% OF BUSINESSES NOW USE HYBRID CLOUD AND THAT THIS FIGURE IS EXPECTED TO RISE BY THE END OF THE YEAR. THEREFORE, IT FOLLOWS THAT SECURING THE HYBRID CLOUD REQUIRES A HYBRID APPROACH, FOR MAXIMUM EFFECTIVENESS. SO, HOW DOES IT HAPPEN? WE SPEAK TO THE EXPERTS TO FIND OUT.

A hybrid approach to security is one that tightly integrates SaaS solutions with an enterprise's existing IT infrastructure. How will this approach ensure maximum security in a space where hacking is getting extremely sophisticated?

ACCELERATED MULTI-CLOUD ADOPTION IS RENDERING TRADITIONAL PRIVATE NETWORKS LESS RELEVANT AS THERE'S LESS NEED TO BACKHAUL TRAFFIC BACK TO CORPORATE DATA CENTERS.

Alain Penel
Regional Vice-President, Middle East & Pakistan at Fortinet

As organizations continue to accelerate their digital innovation initiatives, it is important to adopt an effective security design as new network edges are introduced to the security infrastructure – from data center, LAN, SASE and more.

One of the most profound changes lately has been the increased adoption of cloud-based infrastructures, SaaS applications and services, and the need to provide fast, flexible and secure connections to these resources to any user on any device in any location. We've seen a greater appreciation for a hybrid approach and we are now seeing companies creating a mix of on-prem and cloud environments. Accelerated multi-cloud adoption is rendering traditional private networks less relevant as there's less need to backhaul traffic back to corporate data centers. Indeed, remote workers, branch offices and headquarters locations are increasingly directly connecting to multiple clouds and SaaS providers.

This new distributed network, including the new home office and transformed branch office, has added another layer of complexity. The model moving forward focuses on the user or the entity sitting on some local area network (LAN), reaching across a wide area network

(WAN) to access resources from multiple clouds. As the platform, infrastructure and software become more distributed and disaggregated, it's clear that security and networking have to be integrated and automated across the LAN, WAN and cloud edges. In addition, security should come in multiple form factors and consumption models to suit an organization's unique requirements.

Amit Hooja, NetGraph
CEO, NetGraph

With digital transformation becoming the cornerstone of most organizations, increasing work from home environments, stupendous loads of data being transferred in today's world is also an environment where the number of data security attacks have not only increased, but have also become more advanced. This calls for an even greater need for organizations to ensure that their data is protected to ensure that they can run their businesses unhindered.

Although a lot of SaaS is being increasingly incorporated in most business processes, what we are seeing are increased specializations that are arising both as App based and or API, where certain business processes are better handled by specialized companies. However, both service providers as well as end-users must be able to understand the pros and cons of the vendors they work with.

One of the biggest challenges is integrating SaaS apps within existing IT infrastructure, as more often they are geared to be specialized problem solvers. Having said that, Most SaaS companies are better equipped to handle the security events and avert sophisticated hacks.

Integration across disparate platforms may require several protocol conversions at the data layer and hence opens up doors for hackers to get in. For SaaS integrations to be effective they must implement security at multiple layers including IP restrictions, API security keys, and must have the right processes to ensure that data flow needs are adequately monitored for proper usage, while any abnormal data selections must generate appropriate alerts.

Most SaaS platforms are web delivered and removes the need of installation of any client level software. It is however, very critical that organizations are aware of the need to have regular updates and patches.

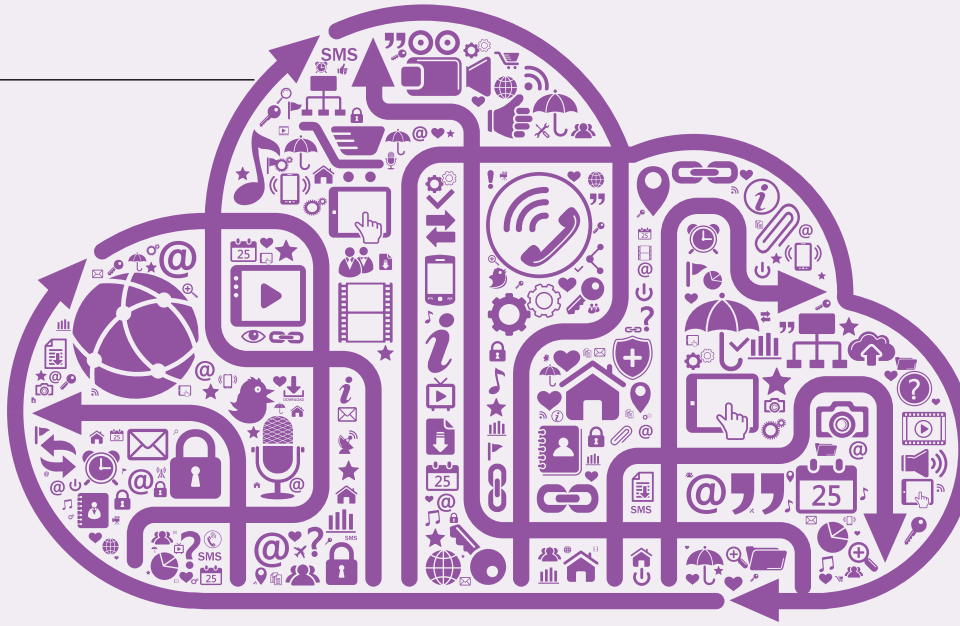
As a part of our Managed Security Service offerings at NetGraph, we constantly review the integration architectures for any security loop holes, provide SaaS vendor security audits and ensure that there are no leakages at the partner level. We also tackle monitoring for data access usages and build patterns on right use of data.

FOR SAAS INTEGRATIONS TO BE EFFECTIVE THEY MUST IMPLEMENT SECURITY AT MULTIPLE LAYERS INCLUDING IP RESTRICTIONS, API SECURITY KEYS AND MUST HAVE THE RIGHT PROCESSES TO ENSURE THAT DATA FLOW NEEDS ARE ADEQUATELY MONITORED FOR PROPER USAGE.

Rohit Bhargav
Practice Head - Could & Security, Cloud Box Technologies

Cyberattacks have evolved dramatically in the past couple of decades regarding their capabilities, scope, fallout, number of targets. CIOs and CISOs are now pressured to prioritize cybersecurity and shift budget to acquiring additional security solutions making sure that they are resilient to cyberattacks.

Testing the cybersecurity posture of organizations is becoming a top priority, it triggered an increased demand for the latest and most comprehensive testing solutions. The three pillars under Gartner Breach and Attack simulations are insider threat, lateral movement and data exfiltration using continuous and consistent testing. There are no siloed environments. We are using SaaS business application in business and it needs a solution that takes 360-degree approach to protect all the 3 verticals keeping data protection at the core.



Security solutions on prem are predictable and have longer procurement and implementation cycle. However, vendors today are bringing CASB (cloud access security broker) SaaS solution approach to supplement their on-prem offering of securing IT infrastructure and data that gets accessed by the application. This approach will add an additional layer of protection to ever evolving security attacks.

Debanjali Ghosh
Technical Evangelist at ManageEngine

As the cybersecurity landscape continues to evolve, it is crucial to develop solutions that help actively combat and mitigate security threats. One such solution is a hybrid approach to cybersecurity, where enterprises integrate their SaaS tools with their existing on-premises solutions to enhance security. For example, hybrid deployments that support single sign-on and access management enable users to securely access all their enterprise applications from a single console. This eliminates the need to log in multiple times to different applications, reducing the attack surface.

To start with, DNS security can be the first line of defense, acting as an early warning system to flag zero-day threats in the network. This ability can be leveraged best when organisations use on-premises DNS servers to block access to domains based on alerts from the threat intel platform and when they further improve the threat assessment model based on the wide range of threat data available in the cloud.

Automation is a natural fit for hybrid deployments. For example, it lets organisations stay ahead of risks rather than just respond to them. With a clear set of rules, policies, and risk scoring in place, IT teams can prevent attacks entirely. A unified hybrid cloud derives valuable context from on-premises infrastructure, which helps with prioritising threats better. Sharing of data with a broader security ecosystem ensures a proactive and optimised incident response.

TESTING THE CYBERSECURITY POSTURE OF ORGANIZATIONS IS BECOMING A TOP PRIORITY, IT TRIGGERED AN INCREASED DEMAND FOR THE LATEST AND MOST COMPREHENSIVE TESTING SOLUTIONS.

Hybrid solutions also offer granularity and visibility over the organisational network. User activities within the on-premises network are continuously shared with the SaaS component of the solution, and indicators of compromise detected by the SaaS tool are immediately forwarded to the on-premises SOC. Based on these inputs, the organisation's security infrastructure (on-premises or in the cloud), including IAM, endpoint security, and SIEM solutions, triggers the automated incident response.

A hybrid cloud strategy also helps address security and data compliance regulations by providing enterprises with the flexibility to decide where to store their data. For instance, an enterprise can store highly sensitive data in a private cloud and relatively less sensitive data in a public cloud. It also allows organisations to host their business-critical data within on-premises data centers, eliminating the risk of external cyberattacks during migration. Since regulations vary with geographic locations, the flexibility provided by a hybrid cloud approach can be leveraged to make the data compliant with specific regional requirements.

Preventing today's sophisticated threats involves strengthening the defenses of three components: users, processes, and technology. The hybrid approach is key to ensure that organisations are "incident-response-ready" for both known and unknown attacks.