# Network Security Forecast for 2019

An AlgoSec Whitepaper

## Introduction

“It’s difficult to make forecasts, especially about the future,” mused movie mogul, Samuel Goldwyn. With the rapid changes in digital transformation, 2019 is likely to surprise us in significant ways. But one thing is certain: IT predictions for 2019 will include swift expansion into the cloud and solutions for the myriad challenges of providing security, compliance and business continuance across the growing on-premise and cloud estates.

Enterprises have jumped with both feet into a hybrid world where best practices and tools are still in formation. According to RightScale’s 2018 State of the Cloud Survey, 96% of enterprises already have applications deployed in the cloud. Just about everybody. The survey also reveals that over 80% of enterprises are going beyond mere deployment and are already embarking on a multi-cloud strategy, exploiting the advantages of each public cloud for compute, storage and networking, and, of course, cost.

Cloud adoption brings with it a whole new set of challenges. Traditional perimeter and host-based security, maintained by firewalls and other physical security devices, can’t easily be replicated in off-premise cloud environments that are not under the control of the enterprise. Lateral east-west traffic that traverses hypervisors, containers and multiple clouds necessitates new approaches to visualization, segmentation, management and protection in these brave new environments.

Given the rapidly changing landscape of enterprise networks, what security issues and trends will we be dealing with over the coming 12 months? Here are AlgoSec’s predictions.

## We’re All Hybrid Now

The overwhelming majority of enterprises plan to use multiple cloud platforms and this trend will only increase in the coming year. Not only are enterprises turning to multiple public clouds to host applications, they will continue to expand their private cloud estates as well. There is clear evidence of private-cloud growth in numbers, physical plant and processing power.

Despite the acceleration of adoption of public and private clouds, the traditional data center will not be disappearing any time soon. In fact, the physical data center will continue to grow in tandem with the private- and public-cloud environments. All these environments will be utilized simultaneously and will constitute the *hybrid cloud* or *hybrid estate*.

## Network Security across the Hybrid Estate: Complexity and Speed

Enterprises will need to employ multiple controls to extend their security across the different environments constituting their *hybrid estate*. Securing data, applications and even parts of applications, regardless of hosting environment, will further complicate already time- and effort-consuming security-management processes.

Even after enterprises carefully plan and lay out their hybrid estates, deploying and configuring controls for each type of environment must be carefully orchestrated so as to create an iron-clad yet flexible security posture. Each public cloud, physical firewall and virtual environment has its own security language and methodology along with a management console to make sense of it all. With so many environments in simultaneous use, the art of security-posture creation, management and enforcement will become increasingly complex.

In addition, the dynamic nature of digital transformation means that today's secure and stable estate is tomorrow's porous, application connectivity-challenged invitation to hackers and outages. In 2019, the speed of change requests and coordination between environments will increase substantially, placing new pressures on over-worked security staffs.

## Clear Visibility

You can't protect what you can't see. Enterprises must acquire holistic visibility of the enterprise-wide security policy that is enforced across their hybrid estate. The requirement for such visibility will grow substantially in 2019. Enterprises will long for a single-pane-of-glass view that delivers security-posture visibility across the entire estate along with constantly updated and on-demand maps of connectivity requirements within and between each environment.

## The Crucial Role of Intelligent, Intent-Based Policy Automation

As applications migrate from one environment to another, their connectivity requirements change significantly. The scale and frequency of change management, and the scope of security and compliance auditing will escalate drastically in 2019. But the enterprise cannot allow the pace of compliance and security audits to slow down their business. Therefore, security staff will need to speed up their security-policy-management processes and improve the accuracy of their policy changes across their on-premise, private and public cloud environments via cross-environment automation of:

Application discovery

Change management

Application decommissioning

Yesterday’s automation capabilities helped, but, fueled by the growing complexity of securing a complex hybrid estate, the need for *intelligent, intent-based policy automation* capabilities that take on a larger security role will spike upward in the coming year.

Intent-based policy automation must address the entire network-security policy-change lifecycle, from submission through audit, by continuously tracking the application responsible for observed traffic or for a requested policy change. Intent-based automation enables security staff to make security-related changes and assess potential risks quickly to maximize the agility and safety of the business. Always-active intelligence delivers auto-discovery of application-connectivity requirements, proactive risk analysis from the business perspective and automation of time-consuming security changes enhanced with business context, all seamlessly orchestrated across the hybrid estate. Intelligence takes on much of the load from security staff by pro-actively alerting on conditions that depress security posture below a threshold while guiding security personnel toward proper remedy.

## Micro-Segmentation for Security and Efficiency

A key and growing strategy for reducing the attack surface of networks, micro-segmentation is a method of creating secure zones that isolate workloads from one another while securing them individually.  Just as a system of watertight compartments in an ocean-going vessel contain flooding in case of hull breach, micro-segmentation isolates servers and systems into separate zones, preventing intruders or malware from moving from one zone to another, thus limiting the potential damage from a security breach or incident.

In their traditional use, firewalls inspect and secure traffic coming into the data center in a north-south direction. Micro-segmentation provides greater control over the growing amount of east-west or lateral communication that occurs between servers, bypassing perimeter-focused security tools. If breaches occur, micro-segmentation limits potential lateral exploration of networks by hackers.

So, it’s no surprise that the use of micro-segmentation, as a defense-in-depth strategy for data center networks, is becoming popular.  However, deciding exactly where to place the boundaries that will separate network segments isn’t easy, especially in complex, multi-network, multi-vendor environments.

Designing an efficient micro-segmentation scheme that limits data exposure and prevents attackers from moving laterally is challenging for on-premise networks that rely on physical separation.  The cloud’s huge advantage lies in the fact that all this segmentation design and deployment is software-defined.

But the hybrid estate multiplies the difficulty by combining physical and software-defined segmentation. How many zones are needed? What is the ‘flavor’ of each zone? Which patterns of communication should be allowed between them?

Environment-specific tools can help with this process by accurately discovering and mapping application-connectivity flows across hybrid environments, thereby aiding in the determination of where segment borders should be placed. In 2019, we will see the

## Containment with Containers

Enabling a low-overhead, easy-to-deploy method of application development and delivery along with a small-footprint alternative to virtual machines, container technology is enjoying increased use in on-prem and cloud-based production environments. Containers virtualize a single application (or microservice that is part of an application) and create a lightweight isolation boundary at the microservice level rather than at the virtual machine level. Containers are easy to replicate and are well suited to DevOps-based elastic environments with rapid scale-out requirements.

Enforcing a security policy within a container-based environment entails both technological and policy-management challenges. On the technology side, the container platform necessitates exposure of the controls that allow enforcement of security policy decisions. Inherently, such controls are at a highly granular level—and it's this granularity that produces the policy-management challenge: how to secure the entire container-based environment. Each segmented network zone can have multiple containers within it, effectively creating zones within zones, and forcing security teams to make many more complex security-policy decisions.

The jury is still out on how organizations will elect to address containers. We predict that, in 2019, enterprises will focus on securing and segmenting their wider cloud environments and will defer deploying granular security controls offered by containers to a later phase.

## Maintaining the Balance of Power

Beyond the technology aspects of the hybrid estate, it's vital to consider the stakeholders who are involved in enterprise cloud deployments. Often, a certain level of tension exists between DevOps, cloud operations and security teams. Each team rightly stresses its own priorities:

01 DevOps
requires agility and automation in order to roll out new applications quickly

02 The cloud team
is charged with controlling the cost while maximizing the advantages of cloud-platform capabilities

03 The security team
requires acute visibility to maintain governance across the entire hybrid estate

These priorities often clash. The challenge over the coming year will be to provide capabilities that bridge those priorities, enabling the disparate teams to work in harmony toward a common, business-driven objective that supports agility, maximizes use of cloud and virtual resources and maintains tight security and compliance.

With a comprehensive security policy management (SPM) solution, security teams can be automatically notified when security policies have been changed. They can obtain an automatic impact assessment of these changes on the rest of the enterprise estate.

In 2019, large and medium-size enterprises will adopt an SPM solution that will enable DevOps teams to embed the solution into a continuous integration (CI) tool chain that will verify that changes to applications remain aligned with security-policy requirements. The solution will quickly address mismatches early, before they impact the business.

## New Responsibilities for Network Security in the Cloud

Deploying production-grade applications in the public cloud exposes new security challenges that used to be “someone else’s problem”. For instance, in an on-premise environment, local workloads alone have access to local file systems and databases. Securing access to storage is typically not considered part of network security but is the responsibility of the server or platform team.

This long-standing division of responsibility breaks down in cloud environments. Unlike in the data center, storage in the cloud is fundamentally network-accessible. To make matters worse, network security controls (firewalls, security groups, access lists, etc.), whether offered by the cloud platform (e.g., AWS, Azure) or 3rd-party cybersecurity provider (e.g., Palo Alto Networks, Check Point), offer no direct protection for cloud storage.

In 2018, we saw that this gap in responsibility brought many enterprises to the media’s front pages (Another Misconfigured Amazon S3 Bucket Exposes 48M Records).

In 2019, enterprises will take far-reaching steps—both organizational and technological—to mitigate this challenge. They will come to understand that securing cloud storage should be the responsibility of a new *cloud network security team* who will be tasked with visibility into and managing the dedicated security controls protecting cloud storage.

## 2019 is Upon Us

The coming year will indeed be one of major technological shifts including more private- and public-cloud adoption along with data-center expansion. The hybrid estate will grow greatly. Considerable attention will be focused on cross-environment security that is agile, intelligently automated, and comprehensive.

Let's hope for a productive and secure year ahead.