IDG CONNECT

10-MINUTE READ

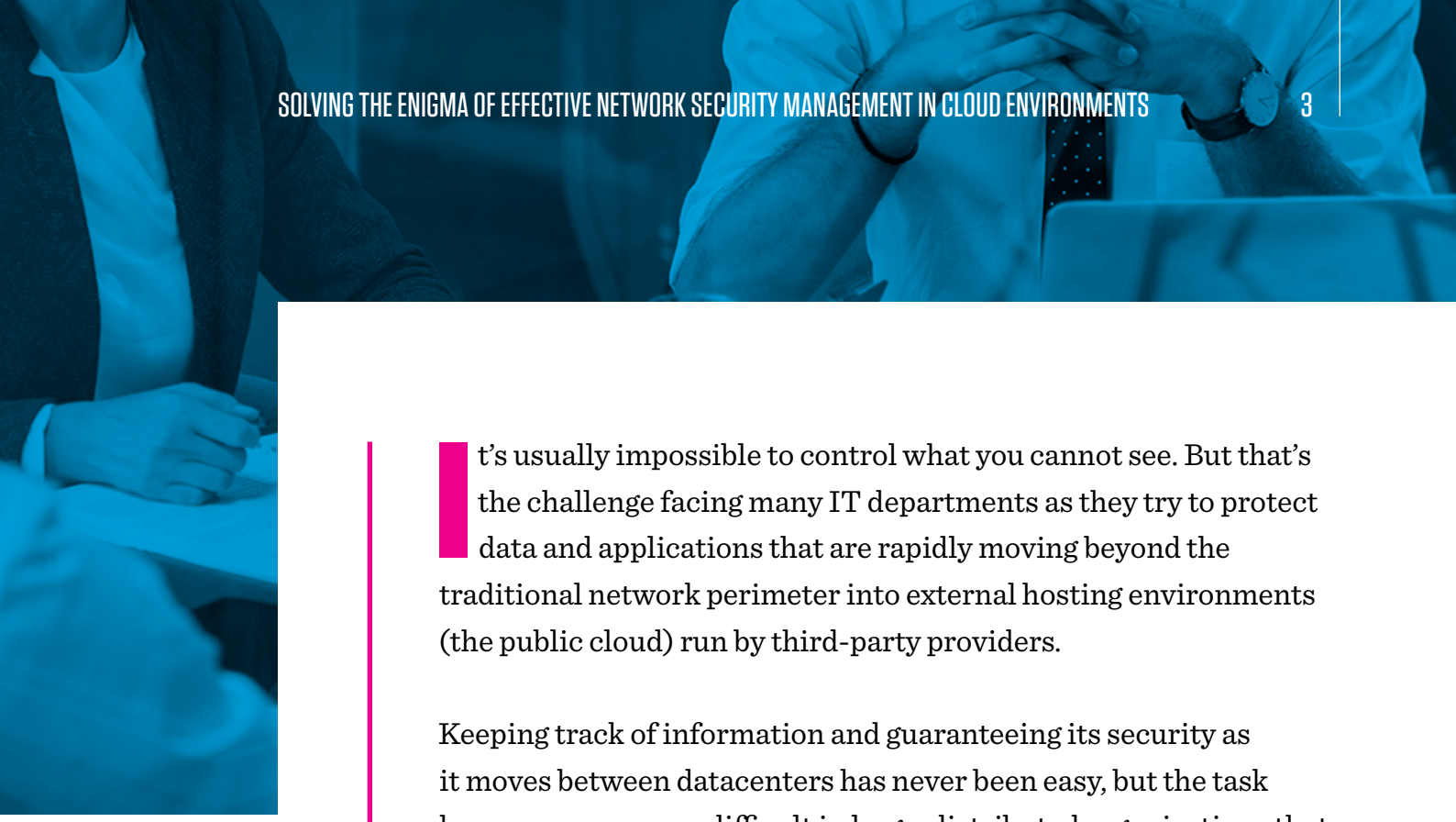
Solving the enigma of effective network security management in cloud environments

Cloud migration brings a wealth of benefits to the distributed enterprise, but organizations must be careful to reduce security risks through efficient application-connectivity and firewall-policy management.

A Management Briefing by IDG Connect in association with Algosec

algosec

Contents



It's usually impossible to control what you cannot see. But that's the challenge facing many IT departments as they try to protect data and applications that are rapidly moving beyond the traditional network perimeter into external hosting environments (the public cloud) run by third-party providers.

Keeping track of information and guaranteeing its security as it moves between datacenters has never been easy, but the task becomes even more difficult in large, distributed organizations that rely on a complex mesh of applications and management platforms spread over multiple sites and systems—physical and virtual—to manage their IT service delivery.

All the while, a growing flock of national and industry regulators are circling, ready to slap heavy fines on any organization found to be in breach of stringent data-protection rules, increasing pressure on IT departments to audit their network security policies on demand to demonstrate compliance.

Cloud: New opportunities bring new risks

"Research firm IDC predicts that global spending on public cloud services and infrastructure will reach $160bn in 2018."

The cloud is a major contributor to the complexity. Organizations everywhere are steadily moving more workloads into various forms of hosted services, driven by the unrelenting need to optimize application and service delivery, reduce costs and introduce more flexibility into the way they procure, provision and manage their IT capacity. Analyst predictions point firmly to an acceleration in cloud-migration projects over the next five years. Research firm IDC predicts that global spending on public cloud services and infrastructure will reach $160bn in 2018, an increase of 23% over 2017.

If keeping up with the pace of all that change is not daunting enough, the ongoing, large-scale migration of applications and services into the public cloud is merely part of the equation. There is much more. Many organizations are also building private clouds that sit squarely on their own internal datacenter infrastructure to meet specific security, performance and availability requirements.

In many cases, resident IT departments are also integrating those private clouds with their public counterparts to form hybrid environments that span on-and-off premise infrastructure and cut across cloud vendors. In these heterogeneous and cross-cloud deployments, IT departments use a mixture of different virtualization platforms, including VMware NSX, Cisco Application Centric Infrastructure (ACI), HPE GreenLake and Rackspace OpenStack Private Cloud, to mix and match the data and applications they host and process to optimize cost, availability and performance.

Lack of visibility amplifies cloud security gaps

"IT managers are justifiably nervous that 'out of sight' could mean 'out of mind.'"

But that wholesale migration also presents significant challenges, especially when it comes to maintaining the security of data and applications migrating away from datacenters while keeping the extended network security management overhead to a minimum and preserving compliance posture.

IT managers are justifiably nervous that "out of sight" could mean "out of mind"—that the data and applications moving beyond the shelter of their network perimeter become difficult to monitor due to a lack of visibility into the network traffic security policies that control flows between virtual machines and across hybrid cloud platforms linked by a mixture of physical and software-defined networks.

Network managers worry that what they cannot see, they cannot control—that once security change management disappears out of their control and beyond the purview of their on-premise

firewalls, they are left blind to the risks generated by automated policy reconfiguration. This is especially true in complex hybrid network environments that can require hundreds of policy changes per month. As security-configuration change requests pile up, that same lack of visibility into the underlying application connectivity increases the risk of outages and disruption.

Cloud security speaks its own language

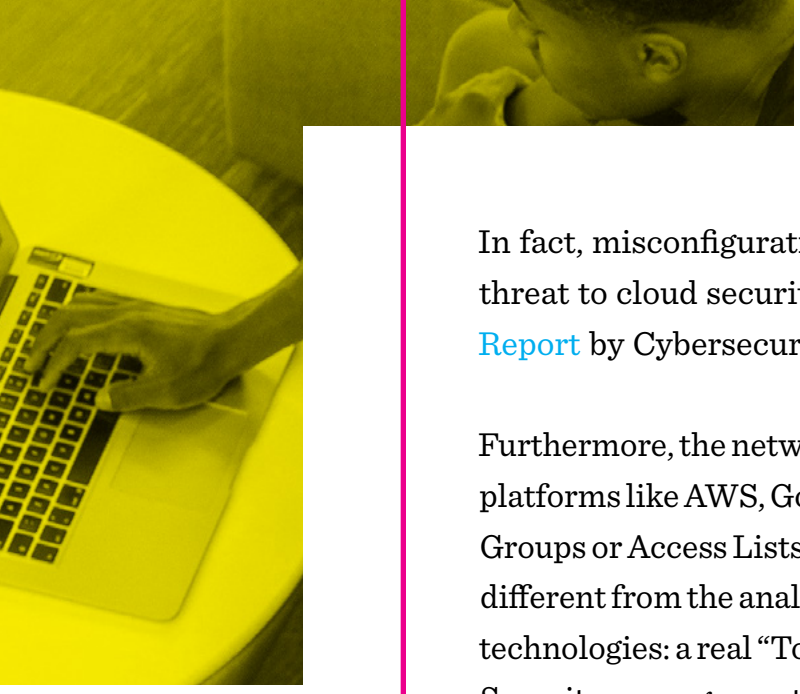
"Misconfiguration of cloud platforms is the single biggest threat to cloud security, according to the 2018 Cloud Security Report by Cybersecurity Insiders."

The complexity of hybrid cloud exacerbates the problem of 'common language'. Different types of clouds employ different tools and processes to monitor and manage security policy compared with the firewalls and routers that IT departments already work with, making it doubly hard to maintain effective control.

Moreover, many organizations find themselves running applications and spreading data across multiple clouds. In some cases, this is the result of a conscious decision, to limit single-vendor lock-in or to reduce costs. In other cases, a multi-cloud environment is the outcome of separate, un-correlated IT projects. Research company, Forrester, estimates that 86% of enterprises have already adopted multi-cloud deployments as they try to keep the cost of service delivery down and find the best match between individual provider capabilities and specific application performance requirements.

Trying to monitor and control security policy changes across multiple clouds, in conjunction with on-premise environments, complicates life for IT staff who are forced to access different management consoles and portals to get a consistent view of security across the entire estate.

The absence of a unified view of the data, applications and networks that require a coherent security policy, exacerbated by complex control and management processes, increases the risk of misconfiguration due to human error.



In fact, misconfiguration of cloud platforms is the single biggest threat to cloud security, according to the 2018 Cloud Security Report by Cybersecurity Insiders.

Furthermore, the network filtering controls provided by cloud platforms like AWS, Google and Microsoft (usually called Security Groups or Access Lists) are different from each other as they are different from the analogous controls available in on-premise technologies: a real "Tower of Babel" of incompatible languages. Security-management staff often find it difficult and time-consuming to ensure that all the necessary controls are consistently configured to provide exactly the required network access and no more. Even gaining a full understanding of what the current security posture is, across a hybrid estate, is a major challenge.

Growing regulatory compliance overhead

That lack of visibility and control over cloud security can also hinder IT managers, chief information officers (CIOs), chief information security officers (CISOs) and their teams who need to understand and audit the risks associated with networks, firewall policies and application vulnerabilities. They must demonstrate ongoing compliance with industry governance rules and national data protection regulations.

"GDPR violators may face severe penalties. A severe breach can result in a fine that is more than enough to cripple them or even put them out of business."

The European Union's General Data Protection Regulation (GDPR) is the latest and most far-reaching in a long and growing list of data protection laws. GDPR, which came into force in May 2018, ensures that any organization collecting or processing the personal data of EU citizens (US companies included) comply with its stipulations. Violators may face severe penalties—a serious breach can result in a fine as high as €20m ($24m) or up to 4% of annual turnover, more than enough to cripple them or even put them out of business. On top of that, reputational damage and restricted access to EU markets is likely to ensue.

Similar national data-protection laws are growing in numbers and scope in other parts of the world as well. On top of that, organizations in certain industries must comply with other regulations that govern the way they handle customer data, such as the Payment Card Industry Data Security Standard (PCI-DSS) in the financial services industry and the Health Insurance Portability and Accountability Act (HIPPA) for US healthcare organizations. IDC has noted that even heavily regulated industries like finance and banking now rely on the cloud for IT service delivery—including SaaS as an alternative to on-premise licensed software for non-mission-critical applications, PaaS for application development and testing, and IaaS as an infrastructure testbed for new, customer-facing services.

"IDC has noted that even heavily regulated industries like finance and banking now rely on the cloud for IT service delivery."

In most cases, it is not enough for IT and legal departments to make certain that their data security systems and processes meet the requirements of these regulations as a one-off exercise. They must continue to demonstrate ongoing compliance through regular audits and be ready to meet the demands of ad hoc e-discovery requests at any point during the year. Making sure they are prepared to conduct regular and unplanned audits puts a considerable burden on IT departments, costing them considerable time, effort and expense.

Migrating applications and data to the cloud does not diminish these regulatory compliance requirements. Quite the contrary! Regulators typically adopt a "shared responsibility" attitude toward cloud-based applications: the cloud provider needs to ensure the security of the infrastructure and the enterprise needs to ensure the security of its own applications and data within the cloud. This means, from the enterprise's point of view, that the scope of an audit for a cloud-based application is the same as for its on-premise sibling—with the added burden that all the cloud-native controls are properly configured. Gaining full visibility of the security policies and controls of a hybrid estate, including the cloud-native ones, is essential for maintaining compliance with any regulation.

Where network security management tools and solutions can help

When it comes to cyber security, there is rarely any simple answer to any single problem, even for those organizations lucky (or deluded) enough to believe that they are facing a one-dimensional threat. But it is equally true that many of the challenges outlined earlier can be mitigated through the deployment of specialized network security management tools and solutions from suppliers such as AlgoSec. These solutions are purposely designed to help large organizations administer numerous firewalls and security controls with tens of thousands of rules to protect data and applications hosted in public and private cloud estates as well as in on-premise datacenters.

"When it comes to cyber security, there is rarely any simple answer to any single problem."

By providing better visibility into network and application traffic flows, these solutions bestow an application-centric view of the connectivity map which can help align security management and control with the actual needs of the business.

Security managers use a single-pane-of-glass console to view and manage security policy across the entire network estate. That includes virtual and software-defined as well as physical infrastructure spread across multiple on-and off-premise public, private and hybrid clouds, operated by different providers using hardware and software platforms from multiple vendors.

The cross-platform, vendor-agnostic console helps to identify weak spots wherever they reside and gives staff more control over network security management. They can prioritize which vulnerabilities to address according to the severity of the risk, particularly at the application level. This eases the cloud migration process and has the knock-on effects of minimizing disruption to daily business operations and circumventing gaps in application availability caused by network misconfiguration.

Automatic aids to auditing and compliance

"More efficient network security policy management helps to strengthen enterprise security defenses."

Powerful network security management tools also take some of the strain off busy network security teams by replacing manual processes with automation tools that do much of the work for them. Automatically translating application-connectivity requirements into firewall rules and processing network security policy changes on a large scale in minutes rather than the days/weeks required with manual configuration, these tools can free staff time up for other tasks. Significant cost savings become possible by extending the useful life of legacy firewall devices which may otherwise have reached the end of their lifecycle with limited potential for upgrade.

More efficient network security policy management helps to strengthen enterprise security defenses by making better use of network segmentation to limit the lateral movement of malware from one side of the network to another. Tightly managed firewall policies inevitably help to reduce the attack surface by eliminating low-level vulnerabilities caused by human error and misconfiguration.

Enhanced network visibility and security management has additional advantages for business managers, CIOs, CISOs and compliance officers. Armed with a better view of the risks and vulnerabilities in front of them, they can compile more relevant and practical reports on demand, presented in formats which are easy to understand and which pinpoint where existing security frameworks may fall short of regulatory requirements.

Using automated network security solutions can slash significant time from the auditing process, helping the organization document and maintain compliance with best practices and regulatory and corporate governance initiatives with minimal resource expenditure. That's a big deal for companies who find themselves struggling to push digital transformation agendas around cloud migration while meeting cost-optimization goals and proper implementation of network security policies.

Customer successes prove AlgoSec's value

Large-scale network service providers deal with enormous network security-management requirements that can be aided by network security policy management solutions. One giant telco used AlgoSec to prove that the firewall policies configured on its off-the-shelf, automated network-security solutions were implemented in the approved manner. AlgoSec could instantly identify rogue connections. The telco was able to automate its enterprise customers' change-management workflows using AlgoSec's Security Management Solution to deliver far more robust business continuity.

"When digital assets are migrated to the cloud, IT staff have little or no indication of how their digital assets are being protected."

Other large enterprises that manage security across multiple sites also reap significant benefits. A European multi-national pharmaceutical company was able to reduce the time its IT team spent on datacenter migration projects by no less than 80% by using AlgoSec to determine how its hundreds of firewall devices spread across 100+ industrial sites would be affected by its cloud migration program.

Elsewhere, a global managed services provider that delivers security services to hundreds of its own customers, including major banks and retailers, used AlgoSec to rapidly identify compliance issues and assess risks associated with current and proposed network configurations.

Strong network security needs intelligent control

The cloud continues to alter the network-security landscape by extending the digital borders of the enterprise into third-party hosting facilities. However, when digital assets are migrated to the cloud, IT staff have little or no indication of how their digital assets are being protected.

The lack of visibility and control of mission-critical data and applications is exacerbated for organizations managing network security policies in large-scale, distributed hybrid IT environments, and especially those in heavily regulated industries.

The communication gap between technology-focused IT staff and business-oriented managers and boardroom executives often makes it difficult for all sides of the organization to understand and digest the scale and nature of the risks facing them and to prioritize when and how to deal with them. The organization as a whole requires a strong, automated network-security management solution that provides a clear view and control of the entire IT estate: everything from on-and-off premise firewalls, physical and virtual security appliances, and the network connections that underpin application security and performance.

"The organization as a whole requires a strong, automated network-security management solution."

That enhanced visibility and control will go a long way to helping them conduct regular audits and demonstrate compliance while reducing unscheduled downtime by automatically applying uniform security policies across cloud and on-premise systems. But perhaps most importantly, a solution like AlgoSec can provide a common platform that brings business and technical teams closer together as they collaborate on how best to effectively tackle the risks and vulnerabilities confronting them. ■

Learn how to effectively manage your network security in cloud environments with AlgoSec here.

The leading provider of business-driven security management solutions, AlgoSec helps the world's largest organizations align security with their business processes. With AlgoSec users can discover, map and migrate business application connectivity, proactively analyze risk from the business perspective, tie cyber-attacks to business processes and intelligently automate network security changes with zero touch across their cloud, SDN and on-premise networks. Over 1,500 enterprises, including 20 of the Fortune 50, utilize AlgoSec's solutions to make their organizations more agile, more secure and more compliant – all the time. Since its inception, AlgoSec has provided the industry's only money-back guarantee.

IDG Connect is the demand generation division of International Data Group (IDG), the world's largest technology media company. Established in 2006, it utilizes access to 44 million business decision makers' details to unite technology marketers with relevant targets from any country in the world. Committed to engaging a disparate global IT audience with truly localized messaging, IDG Connect also publishes market specific thought leadership papers on behalf of its clients, and produces research for B2B marketers worldwide. For more information visit: www.idgconnect.com

IDG CONNECT