Enterprise Strategy Group | **Getting to the bigger truth.™**

White Paper

The Case for Host-based Micro-segmentation

By Jon Oltsik, Senior Principal Analyst

May 2018

This ESG White Paper was commissioned by Illumio
and is distributed under license from ESG.

Contents

Executive Summary

With the proliferation of virtual servers, cloud-based workloads, and containers, enterprise organizations have found themselves in a cybersecurity quandary where they are being asked to safeguard workloads residing on infrastructure they don't own or control. What can CISOs do to provide ample protection for hybrid cloud applications? This white paper concludes:

- **Traditional security controls are a mismatch for hybrid cloud security**. Organizations often try to extend their existing security tools and processes to protect hybrid cloud-based workloads. Unfortunately, these tools introduce chokepoints within dynamic cloud environments, complicating network configurations. Furthermore, traditional controls can't keep up with mobile and temporal workloads often used to build cloud-based applications. ESG research reveals that many of these projects end in failure as organizations abandon traditional tools in pursuit of cloud-based alternatives.

- **Micro-segmentation is on the rise.** Once they move beyond traditional security controls, many organizations turn to micro-segmentation technologies, but decisions on which type of micro-segmentation technology to use can be confusing. Security professionals often weigh the strengths and weaknesses of three choices: infrastructure, hypervisor, and host-based micro-segmentation technologies.

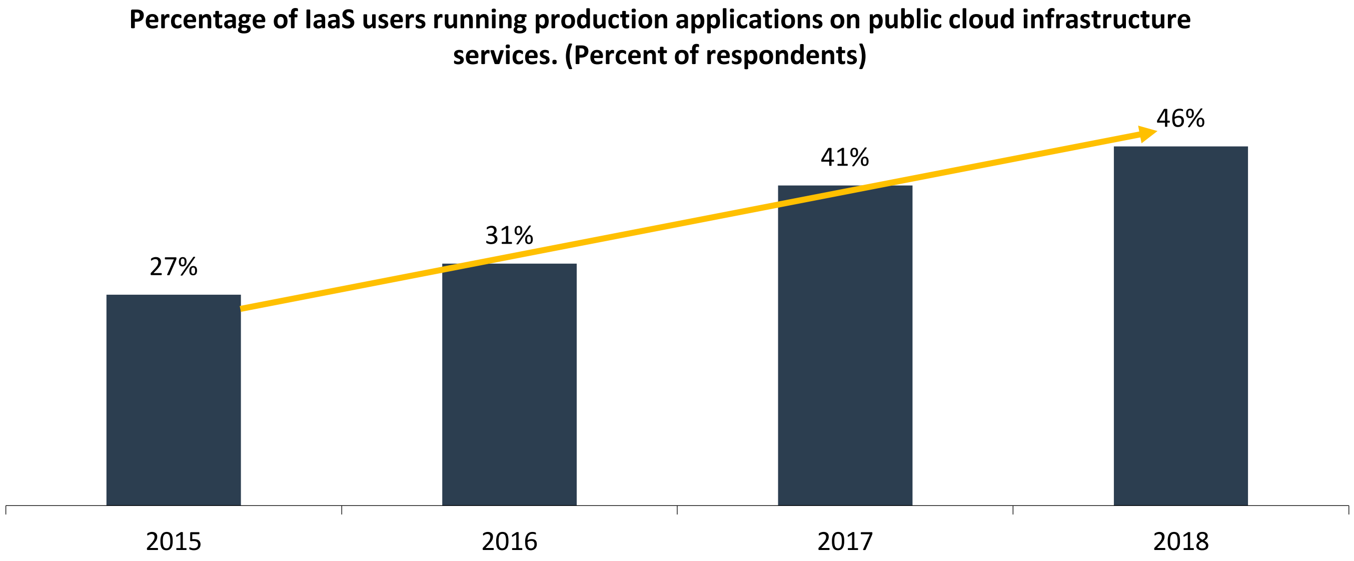
- **Host-based micro-segmentation deserves consideration.** Too often, security professionals dismiss host-based security technologies based upon historical biases. In the past, host-based security tools contained agents that can throttle system performance. Provisioning and managing hundreds or thousands of agents can introduce lots of operations overhead. And host-based technologies are vulnerable to hackers who compromise systems and disable security controls. These were all legitimate objections historically, but modern host-based micro-segmentation tools have addressed these problems to offer central management, distributed enforcement, tamper-proofing, and strong security that aligns well with the requirements for large distributed hybrid cloud environments.

The Changing Security Landscape

Today's data centers are densely packed with workloads of all kinds—bare metal servers, virtual servers, cloud-based workloads, containers, etc.—and this situation has only accelerated due to the growing use of public cloud computing. According to ESG research, 85% of organizations use public clouds for IaaS services in 2018 and continue to move more production applications to public clouds annually (see Figure 1).[1]

[1] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

Figure 1. Increasing Percentage of Product Applications Run on Public Clouds



Source: Enterprise Strategy Group

In the past, data center networks were protected using perimeter firewalls, network packet filtering rules, ACLs, and network segmentation (i.e., VLANs and IP subnets) used to separate networks by zones or functions based upon things like business units, departments, regulated/unregulated workload types, etc.

Unfortunately, many organizations now find themselves at a network security crossroads. With the rise of dynamic, heterogeneous, and distributed data centers, existing network security controls can no longer provide adequate protection because:

- **Cyber-adversaries bypass security controls to compromise systems and steal data.** Hackers are aware of the data they want to steal and have good ideas about the digital doors, fences, and locks used to protect these valuable assets. Armed with this knowledge, cyber-adversaries use tactics, techniques, and procedures (TTPs) designed to circumvent network security controls such as phishing emails, malicious scripts/attachments, supply chain compromises, and social networking attacks. For example, the Anthem and JPMorgan Chase data breaches originated with spear-phishing campaigns, while the Office of Personnel Management (OPM) and Target breaches were the result of supply chain compromises. In these and many other cases, traditional network security controls proved ineffective at blocking attacks or even decreasing the network attack surface.

- **Complex and costly security tools can't keep up with dynamic data center scale.** Traditional network security tools are based upon network hardware and physical devices acting as "bumps on the wire" within corporate networks. These technologies were really designed to secure traffic when network sources and destinations were physical boxes rather than virtual servers, cloud-based workloads, or application containers. Not surprisingly, forcing hybrid cloud traffic through physical devices can be complicated, especially when cloud-based workloads spin up and down or move from one data center to another. Furthermore, network devices are costly to purchase, deploy, and maintain. Finally, there is a fundamental incongruity between rigid physical network security devices and temporal cloud-based workloads designed for flexibility and real-time utilization.

- **Application traffic spans multiple data centers.** In the past, mission-critical applications sat "behind the firewall" but that is no longer the case. Today's applications based upon containers and micro-services are highly transient and often span multiple public and private data centers. Network security appliances can only understand and secure local traffic that can be inspected as they have no context for application traffic flowing amongst data centers. As a result, granular protection is minimized, increasing risk.

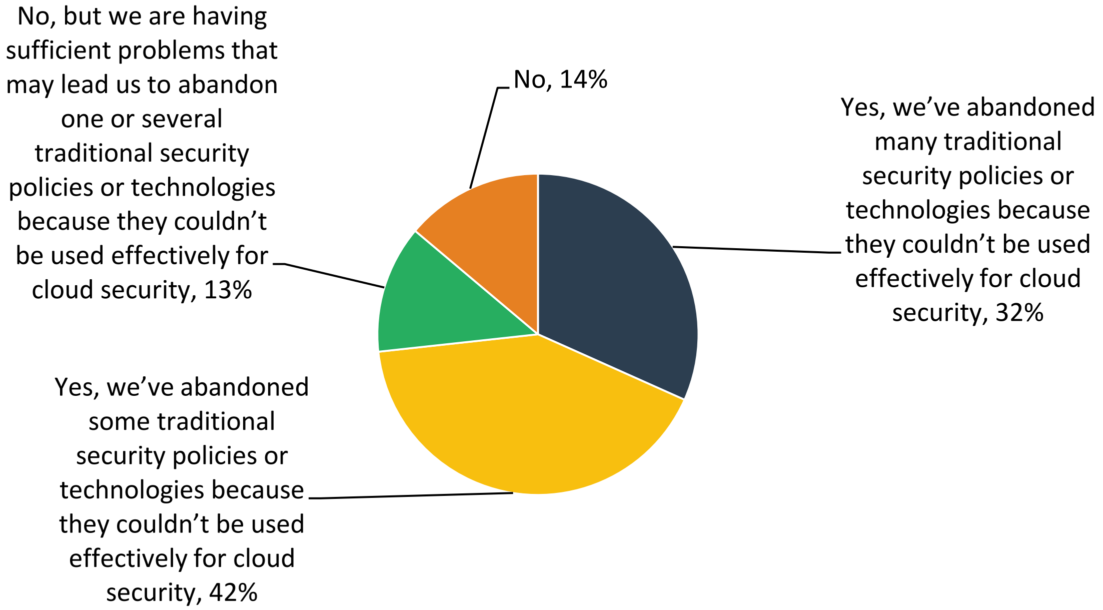
Given today's cyber-risks, CISOs want to bolster network security by safeguarding east/west traffic amongst data center workloads. This increases the scale and complexity of network security as it exacerbates the problems described above.

The Case for Micro-segmentation

Legacy network security tools are a mismatch for today's requirements as they were designed to filter traffic between physical devices in a data center. While some organizations try to force-fit security controls, ESG research indicates that 74% have had to abandon all or some traditional security controls because they couldn't be used effectively for cloud protection, while another 13% are having problems with traditional security controls that may lead to replacement (see Figure 2).[2]

Figure 2. Traditional Security Controls Are a Mismatch for Cloud Computing

Has your organization had to abandon its use of any traditional security policies or technologies because it couldn't be used effectively for cloud security? (Percent of respondents, N=303)



Source: Enterprise Strategy Group

Given the limitations of traditional security controls, CISOs need an alternative technical strategy. Fortunately, the industry has responded with new types of micro-segmentation technologies based upon:

- **Software-defined networking (SDN).** SDN is designed to separate the network control and data planes, providing more network agility and flexibility. With SDN, network flows and rules can be programmed, making it easier to segment the network at a more granular level, decreasing the attack surface.

[2] Source: ESG Research Report, *The State of Cloud Security in the Enterprise*, October 2016.

- **Open standards and APIs.** SDN technology standards like OpenFlow provide access to the data forwarding plane of networks, enabling security tools to program the network to enforce granular micro-segmentation rules. Additionally, public cloud services like AWS, Google Cloud Platform (GCP), and Microsoft Azure provide APIs that allow similar programming for workload-to-workload micro-segmentation.

- **Central command-and-control.** Traditional network segmentation was a cumbersome process that could require advanced networking knowledge and manual implementation on a switch-by-switch basis. This limited the usage of Layer 2 VLANs. These problems are overcome with new micro-segmentation tools that can discover all workloads, map out communications patterns, and provide a centralized platform for micro-segmentation policy management. The marriage of central management and distributed enforcement allows micro-segmentation tools to address dynamic application environments and scale to support hundreds to thousands of hybrid cloud workloads.

Micro-segmentation Methods

As cloud computing expands, organizations are interested in protecting hybrid cloud workloads with micro-segmentation. Nevertheless, many security professionals remain confused by the different types of micro-segmentation technologies available. There are three types of micro-segmentation technologies to choose from—infrastructure technologies, hypervisor technologies, and host-based technologies—each with its own strengths and weaknesses (see Table 1).

- **Infrastructure Technology.** With the advent of software-defined networking, organizations have the option of deploying and using SDN controllers for micro-segmentation. This can be accomplished through third-party security tools that tap into SDN controller APIs or through direct SDN programming. This method is especially attractive to organizations investing in SDN for network engineering and committing to SDN technologies from a single vendor. Infrastructure technology for micro-segmentation is a good fit for relatively static private cloud deployments but can't protect dynamic hybrid cloud deployments with mobile and temporal workloads. This type of micro-segmentation can introduce chokepoints that may impact network performance and complicate network engineering.

- **Hypervisor Technology.** This option is especially appealing to organizations with large VMware installations. Hypervisor technology for micro-segmentation emulates SDN controller functionality within the hypervisor. Within VMware, this function is assigned to NSX. NSX is a good fit for large VMware shops as it is based upon familiar tools and aligns with common operations processes. Alternatively, hypervisor-based micro-segmentation may not be a good match for organizations using heterogeneous cloud and server virtualization technologies as it may not support these other environments or provide protection for mobile workloads that migrate outside of the hypervisor domain.

- **Host-based Technology.** Rather than delegate micro-segmentation to the network, some organizations opt to collocate security controls with the workloads themselves. In this way, policy enforcement rules live beside the assets that need protection, which is a security best practice. Furthermore, host-based technology leverages existing assets like host-based firewalls, leading to strong ROI. Host-based micro-segmentation is especially useful for mobile and temporal workloads because micro-segmentation rules can be programmed into the hosts when provisioned and then remain with the workloads regardless of location or duration. Host-based technologies can be complex as they introduce the need to manage policy and enforcement rules for hundreds or thousands of workloads rather than a few centralized networks or hypervisors. Finally, host-based technology can introduce a security vulnerability as well. If a host is compromised, a hacker can then alter micro-segmentation rules and gain access to the broader network.

Table 1. Strengths and Weaknesses of Micro-segmentation Technologies

Micro-segmentation technology	Strengths	Weaknesses
Infrastructure	• Aligns with SDN deployments for network engineering • Fits well with single network equipment vendor strategy for investment protection and common operations	• Cannot support mobile or temporal workloads • Cannot support heterogeneous hybrid cloud deployments • Introduces a chokepoint on the network that can impact performance and network engineering
Hypervisor	• Aligns with large deployments of server virtualization technology (i.e., VMware) • Fits with common operations tools and processes	• Cannot support mobile or temporal workloads • Cannot support heterogeneous hybrid cloud deployments
Host-based	• Collocates security controls with assets • Acts as an antenna and collects information on workloads that can then be used for micro-segmentation policy and enforcement • Takes advantage of existing host-based security functionality (i.e., host-based firewalls and network filtering) • Good match for mobile and temporal workloads	• Policy management and enforcement for hundreds or thousands of workloads can be complex • Can introduce a security vulnerability if hosts are compromised

Source: Enterprise Strategy Group

Host-based Micro-segmentation: Overcoming Historical Biases

Of the three types of micro-segmentation technologies, host-based solutions are probably the most misunderstood. Security professionals have regularly eschewed host-based security controls in the past due to the scalability and security issues described above. After all, deploying and managing security agents can be a time-consuming slog, while host-based agents have been known to consume resources and impact system performance. Furthermore, host-based security tools were often viewed as vulnerable to attack. These problems were “show-stoppers” for security and IT teams.

Host-based security concerns were certainly valid a few years ago, but ESG believes that cybersecurity professionals should be open-minded about host-based micro-segmentation today for several reasons:

- **Performance issues are obsolete.** Unlike other security products like antivirus software and HIPS, host-based micro-segmentation tools tend to be based on lightweight agents. These agents are not inline, nor do they route traffic from kernel to user space for filtering and inspection. Rather, the agents are used to look at connection tables, collect telemetry, and report on workload behavior to a central management system. Once a policy is established, local agents are used for policy enforcement and monitoring only. Security professionals with remaining performance concerns would be best served by conducting performance testing on host-based micro-segmentation agents so they can assess performance and operations impact for themselves.

- **Security concerns have been noted and addressed.** The security vulnerability theory goes as follows: A hacker that compromises a single workload can manipulate the agent to override security controls, perform network reconnaissance, and gain access to all other workloads across hybrid cloud infrastructure. Modern host-based micro-segmentation tools overcome this vulnerability through distributed firewalling and tamper resistance. Security policies and firewall rules are germane to individual workloads so even if a host is compromised and firewall policies are erased, the workload will only be able to connect with only those workloads it has permission to communicate with. All other workloads still act as a distributed firewall, blocking unauthorized connections based upon policy. Some host-based micro-segmentation tools also have tamper resistance built into their agents. If a hacker tries to delete the agent or change firewall policies, the compromised workload will alert the central policy manager as well as other security operations tools (i.e., SIEM) in the SOC. In this way, host-based micro-segmentation agents also act as a distributed tripwire, alerting operations when they detect suspicious tampering of any node.

- **Central management addresses operational overhead.** Today's host-based micro-segmentation tools are built with a design of central management and distributed enforcement. When agents are installed on workloads, they collect telemetry and then report back to central management about application and network behavior. This information can then be used to recommend or customize granular micro-segmentation policies. In this way, host-based micro-segmentation tools not only centralize management, they also ease configuration and policy creation by applying advanced analytics and automation to ease micro-segmentation operations across hybrid cloud environments.

Aside from overcoming historical problems, host-based micro-segmentation tools can also deliver a cost advantage over infrastructure and hypervisor-based alternatives. By taking advantage of native host capabilities (i.e., host-based firewalls and packet filtering), organizations can avoid deploying costly hardware and software while maintaining security protection for distributed workloads in public clouds that other micro-segmentation technologies can't support.

In summary, modern host-based micro-segmentation tools can take advantage of the benefits of workload collocation while overcoming the historical problems associated with host-based security controls. This scenario is especially true in large hybrid cloud environments and distributed applications based upon mobile and temporal workloads. In these deployments, chokepoints are impractical and ineffective. As such, CISOs should be open-minded about host-based micro-segmentation solutions moving forward.

The Bigger Truth

George Bernard Shaw is often quoted for warning people to "Beware of false knowledge as it is more dangerous than ignorance." The historical biases about host-based security technologies are certainly valid in some applications but can be thought of as "false knowledge" with regards to micro-segmentation. Based upon this mindset, organizations must understand the tradeoffs associated with different micro-segmentation technologies and make their decisions based on technologies available in 2018 rather than 2008.

Highly distributed heterogeneous hybrid clouds represent an evolving compute model. As such, organizations must be open-minded about security, and cast a wide and open-minded net when seeking out the most appropriate and comprehensive security solutions for safeguarding mobile and temporal workloads. CISOs should make their decisions based upon security efficacy, ease of use, scalability, and operational efficiency. Given these criteria, host-based micro-segmentation tools deserve consideration.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.