Firewalls and the Cloud
A Survey of IT Security Professionals Responsible for Cloud Environments

March 2018
Introduction

Next Generation Firewalls (NGF) are a mainstay of IT security organizations, maintaining a perimeter to protect vital systems and data. But as cloud deployments have completely changed network and system topologies, the perimeter is an increasingly complicated concept. It’s no longer easy to define, let alone defend. So what is the role of the firewall in a cloud and hybrid world? Do existing NGF approaches continue to deliver needed protection or are new capabilities needed?

This research investigates the hands-on reality of security in cloud environments, with a specific focus on the role of firewalls. It considers general attitudes towards cloud security, then takes a deep dive into experiences with existing NGFs in cloud environments and the demand for additional cloud-specific firewall capabilities. It also explores potential security challenges associated with the adoption of modern development and deployment methodologies.

This report is based on an online survey of 608 IT decision makers from around the globe. All participants had responsibility for security in an environment with significant cloud investments.
Key Findings

The cloud is redefining the role of the firewall
- More than half (56%) report that their on-premises security is superior to cloud
- At large companies, almost two-thirds (62%) say their on-premises security is better than cloud
- 76% expect cloud security to be a shared responsibility

Value found in cloud-specific security capabilities
- 83% have concerns about NGFs in the cloud
- Top concerns include pricing and licensing, lack of integration, and increased overhead due to a lack of centralized management
- 99% would see value in cloud-specific firewall capabilities including:
  - 74% want integration with cloud-native capabilities
  - 59% value ease of deployment and configuration by cloud developers
  - 56% would benefit from regulating traffic flows between on-premises and cloud
  - 53% see a benefit in distributed policy enforcement

DevOps teams benefit from security automation
- 93% of those who have adopted DevOps, DevSecOps, or CI/CD report that they have faced challenges when integrating security needs into their processes
- Top challenge reported was “limitations with existing security solutions”
The cloud is redefining the role of the firewall

In this first group of questions, respondents were asked to provide their thoughts about the effectiveness of traditional on-premises security tools compared to the effectiveness of security tools available for public cloud environments. The data collected provides insight about current security preferences and feelings about who owns the responsibility — here’s what was discovered:
In your opinion, how does the overall security posture for your company’s cloud services compare to your on-premises security?

- 56% believe on-prem security is superior
- 23% believe there is no difference
- 21% believe cloud security is superior
In your opinion, how does the overall security posture for your company’s cloud services compare to your on-premises security? (By company size)

- **More than 5,000 employees**: 62% On-prem superior, 22% No different, 16% Cloud superior
- **1,000 - 5,000 employees**: 54% On-prem superior, 24% No different, 22% Cloud superior
- **500 - 1,000 employees**: 53% On-prem superior, 25% No different, 22% Cloud superior
- **10 - 500 employees**: 47% On-prem superior, 21% No different, 31% Cloud superior
Cloud security is typically expected to be a shared responsibility

In your opinion, who is responsible for the security of cloud environments?

- The cloud vendor is solely responsible: 12%
- We are solely responsible: 12%
- We share responsibility with our cloud vendors: 76%
In your opinion, who is responsible for the security of cloud environments?

(By job level)
Value found in cloud-specific security capabilities

In this next section, the findings reveal respondents’ feelings about current firewall offerings, and whether they think these tools would work to secure their cloud assets. Additionally, the data collected in this section reveals respondents’ attitudes about cloud-specific features, and which of those features would be beneficial for deployments within their organizations.
Have you currently deployed NGF (Next Generation Firewall) solutions in your on-premises environment?

Have you deployed NGF (Next General Firewall) solutions in your cloud environment?

Security teams are twice as likely to install an NGF on-premises vs. in the cloud.
Half of those who haven’t deployed NGF for cloud usage, plan to do so in the future.

Why haven’t you deployed NGF in your cloud environment?

- We plan to, but haven’t done it yet: 50%
- Too expensive: 24%
- Our cloud environment does not require that level of security: 22%
- Isn’t a fit for our cloud architecture: 21%
- Too cumbersome to deploy: 10%
- Doesn’t scale: 6%
- Other: 3%

Most frequent “Other.” Expect their cloud vendors to do this for them.
83% have concerns about NGFs in the cloud

What concerns do you have about deploying a NGFs (Next Generation Firewall) in a cloud environment?

- Pricing and licensing not appropriate for the cloud (39%)
- Lack of integration prevents cloud automation including deployment, auto-scaling, monitoring, etc. (34%)
- No centralized management across distributed firewalls creates significant overhead (34%)
- Don't integrate with native security tools from cloud vendors (30%)
- Don't properly regulate traffic between on-prem and cloud (20%)
- Too time-consuming to deploy (20%)
- NGF not practical for the cloud (13%)
- I do not have any concerns (17%)
Below is a list of possible new capabilities of a firewall built specifically for the needs of cloud and hybrid environments.

Which of these would your organization find beneficial?

- Integration with cloud management, monitoring, and automation capabilities (i.e. AWS Cloudwatch, Azure Security Center, Azure OMS, etc.): 74%
- Easy to deploy and configure by cloud developers so application security can be integrated during development as opposed to waiting to be deployed in production: 59%
- Regulate traffic flows between on-prem and cloud data centers: 56%
- Distributed policy enforcement that adapts to individual workloads rather than securing multiple services behind a single hardware solution: 53%
- None of these would be beneficial: 1%
96% would find a cloud-specific firewall valuable

How valuable would a firewall built specifically for the needs of cloud and hybrid environments be for your organization?

- Very valuable: 96%
- Somewhat valuable: 42%
- Not valuable: 4%
- Other: 0%

![Bar chart showing the distribution of responses.](chart)
Large companies see the most value in a cloud-specific firewall

How valuable would a firewall built specifically for the needs of cloud and hybrid environments be for your organization?

(By company size)
What type of pricing model would you prefer for a firewall solution built specifically for the needs of cloud environments?

- **Strong preference for usage-based cloud pricing for cloud-specific firewalls**
  - New, flexible pricing options that match cloud deployment (pay-as-you-go, metered,...)
  - Traditional pricing options that mirror the way we have always bought firewalls
  - I don't have an opinion

30% of respondents prefer new, flexible pricing options, while 7% opt for traditional pricing. 30% of respondents are undecided.
DevOps teams benefit from security automation

In this last set of questions, respondents offer a bit of insight into their experiences with some of the common security challenges faced by DevOps, DevSecOps, and CICD (continuous integration and continuous deployment) teams.
Has your company adopted DevOps, DevSecOps, or CI/CD development methodologies?

- Yes: 56%
- No: 44%
Large companies and companies in APAC are more likely to adopt

Has your company adopted DevOps, DevSecOps, or CI/CD development methodologies?

By region:
- AMER: Yes 53%, No 47%
- EMEA: Yes 58%, No 42%
- APAC: Yes 63%, No 37%

By company size:
- 10 - 500 employees: Yes 29%, No 71%
- 500 - 1,000 employees: Yes 40%, No 60%
- 1,000 - 5,000 employees: Yes 59%, No 41%
- More than 5,000 employees: Yes 71%, No 29%

dimensional research
What challenges have you faced integrating security into DevOps, DevSecOps, or CI/CD adoption?

- Existing security solutions don't offer integration into development environments (i.e. REST API) so are not part of code building processes (63%)
- Application developers not comfortable with security (48%)
- Security processes haven't changed so remain a bottleneck (48%)
- We have not had challenges (7%)

$n = \text{Have adopted CI/CD, DevOps, DevSecOps}$
Methodology and Participant Profile
Goals and Methodology

Research Goal
The primary research goal was to capture hard data about security experiences and attitudes in cloud environments, particularly about Next Generation Firewalls (NGF).

Methodology
An online survey was sent to independent sources of IT security stakeholders. A wide range of questions were asked on the current state of security in the cloud, use of NGF, and needs for cloud-specific capabilities.

Participants
A total of 608 participants from around the globe completed the survey. All had responsibility for security in an environment that included a significant cloud investment.
Demographics

Company Size
- More than 5,000 employees: 35%
- 500 - 1,000 employees: 15%
- 1,000 - 5,000 employees: 15%
- 10 - 500 employees: 15%

Region
- AMER: 61%
- EMEA: 27%
- APAC: 12%

Industry
- Technology: 17%
- Financial services: 15%
- Manufacturing: 12%
- Healthcare: 10%
- Education: 9%
- Services: 8%
- Government: 7%
- Retail: 6%
- Telecommunications: 5%
- Transportation or logistics: 2%
- Food and beverage: 2%
- Non-profit: 2%
- Other: 5%
For more information…

About Dimensional Research

Dimensional Research provides practical marketing research to help technology companies make smarter business decisions. Our researchers are experts in technology and understand how corporate IT organizations operate. Our qualitative and quantitative research services deliver a clear understanding of customer and market dynamics.

For more information, visit www dimensionalresearch com.

A Quirk Magazine Top 10 Research Blog:
www dimensionalresearch com/blog