illumio

The State of Security Segmentation

How organizations protect against lateral movement

Contents

illumio

The reality of today's cyber risks

Security incidents are inevitable. Motivated attackers will find their way in. They might rely on clever pieces of never-before-seen malware, effective phishing campaigns that yield employee credentials, containers left exposed to the internet or invariably, vulnerable software.

What else have we come to accept? That attackers, once inside, seek to move laterally, looking to steal important intellectual property or sensitive customer information. Perhaps they merely want to lock up data with ransomware that moves laterally on its own or worse, destroy sensitive information. At this stage, when attackers begin to move laterally, a small security incident can transform into a full-blown breach.

The good news?

Savvy organizations have further invested in modern defense-in-depth, including segmentation to stop attackers from moving laterally (or "east-west" as the kids call it), so they are left with no place to go.

Given its importance, we wanted to get a sense of the state of segmentation as part of defense-in-depth, by conducting a survey with Virtual Intelligence Briefing (ViB) to understand how companies segment today, and what difficulties they face. This survey was independently conducted by ViB—an interactive online community focused on emerging through rapid growth stage technologies. ViB's community is comprised of more than 1.2M IT practitioners and decision makers who share their opinions by engaging in sophisticated surveys across IT domains including Information Security.

What did we learn, in a nutshell?

- Today's IT norm is hybrid: on-prem data centers and mulitple clouds.
- We still too often hope for the best when trying to stop big data breaches. More than half of respondents do not have and are not planning segmentation in the next six months.
- Two-thirds of respondents think the firewall is an over-the-hill gold digger when it comes to segmentation. It's a 90s technology that can be frightfully expensive.
- Surprise! Firewall technology is not DevOps friendly or business-ready for 2020.

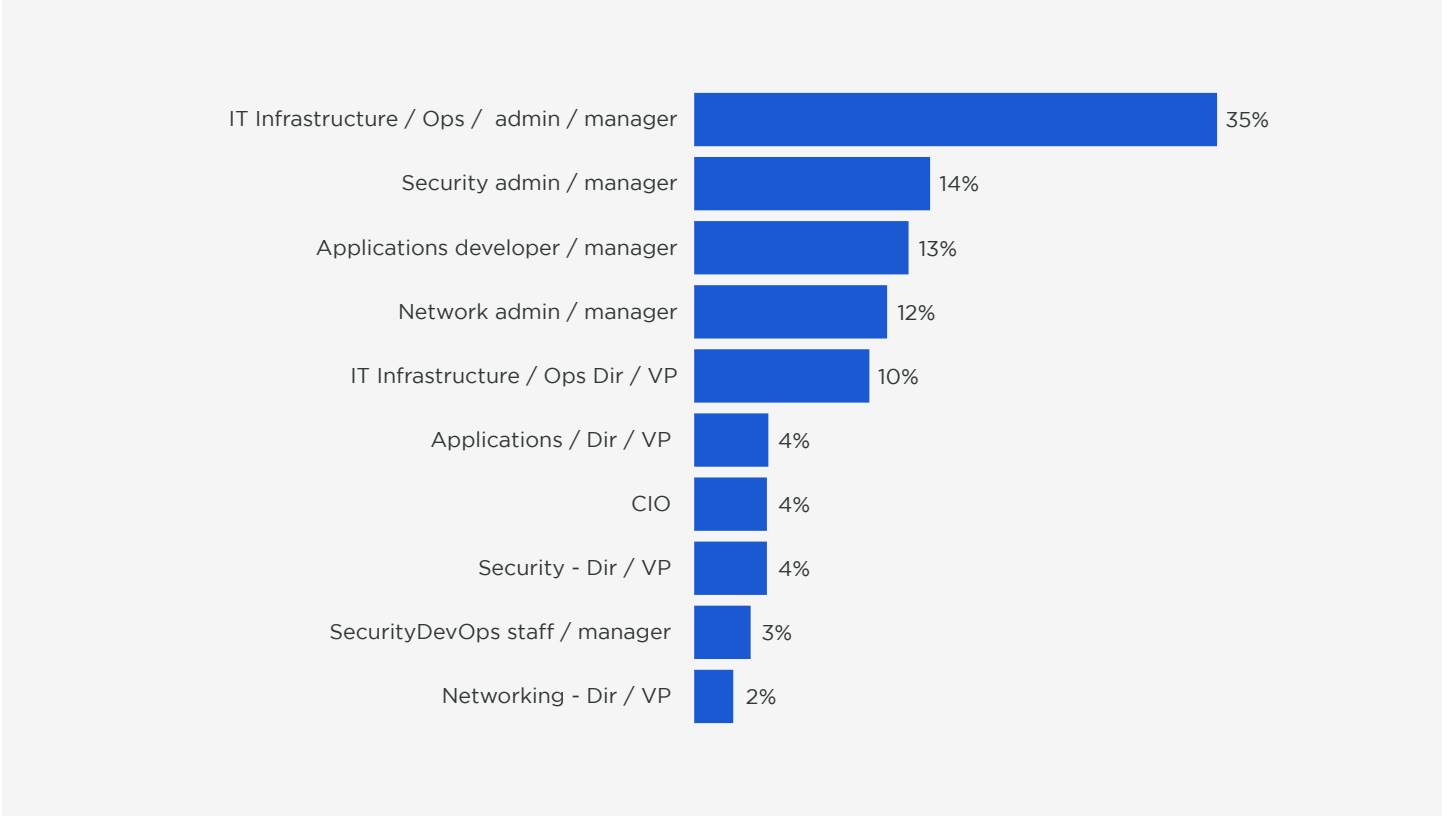
What is segmentation?

It's the act of separating a network into smaller zones—turning each one into a segment; thereby, enhancing overall security and preventing attackers from moving laterally inside networks, data centers and clouds.

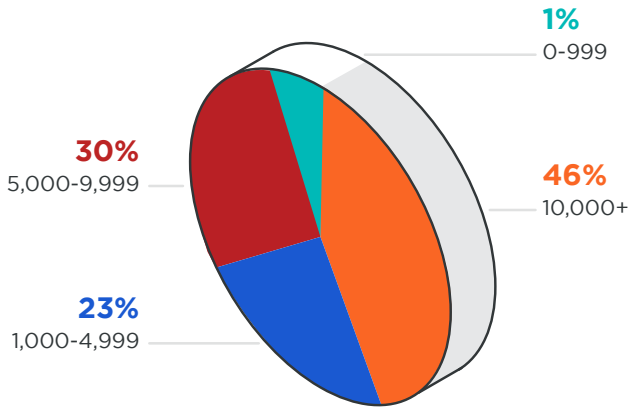
Who did we talk to?

We spoke to over 300 IT professionals from a cross-section of mid- to large-sized companies, most from companies with over 1,000 employees.

JOB ROLE



COMPANY SIZE



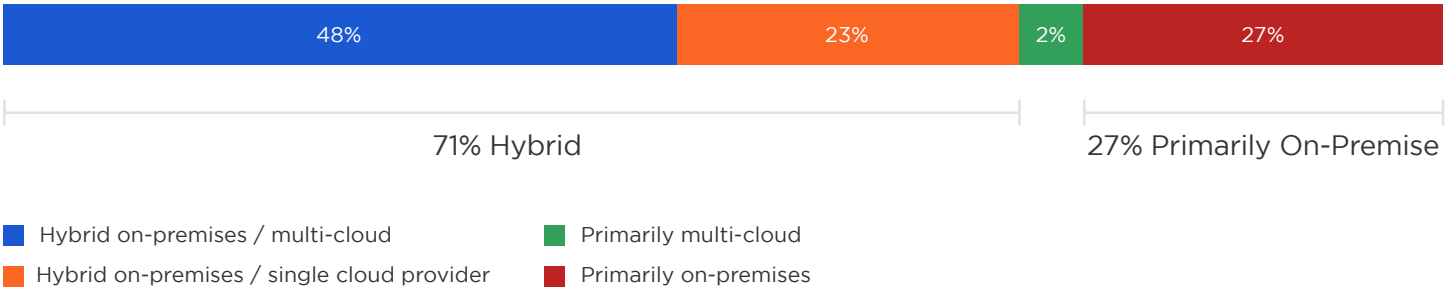
illumio

Protecting a hybrid world

We wanted to know what environments organizations need to protect, so we asked. 71% of respondents are "hybrid on-premises", meaning they rely on both data centers and clouds working together. 48% told us they have multiple cloud providers.

An application-centric world

It is a microservices world and the rest of us are just living in it. We inquired about apps distributed across infrastructure boundaries. Guess what? Only 3% say they do not distribute apps across boundaries; however, 30% say more than half of their applications are distributed and 37% have between 21-50% distributed.



Massive data breach, no big deal?

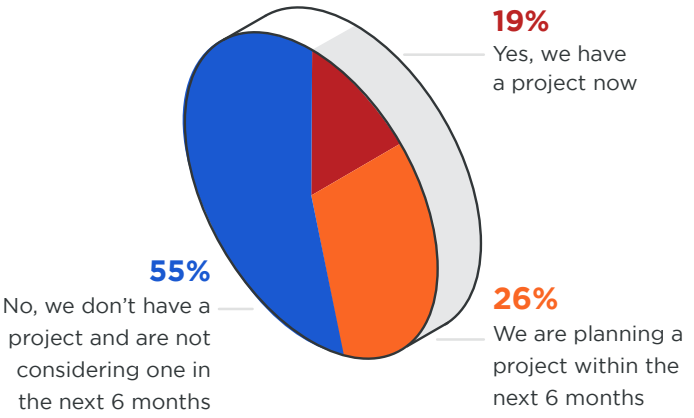
Who's segmenting today to reduce the risk of a data breach? Alarmingly few organizations, is who. 19% of companies we spoke to protect against breaches with segmentation. About a quarter are actively planning a project. Yet, more than half are not protecting with segmentation or planning on it in the next six months.

The firewall still hasn't been fired

How do we actually do segmentation today? Most often it's with firewalls.

A whopping 86% of respondents still use firewalls to segment their applications.

Some 46% have tried to coax segmentation out of software-defined networking (SDN) and 44% look to host-based segmentation, either segmentation via individual host IP addresses or using segmentation that harnesses firewalling in the host operating systems.



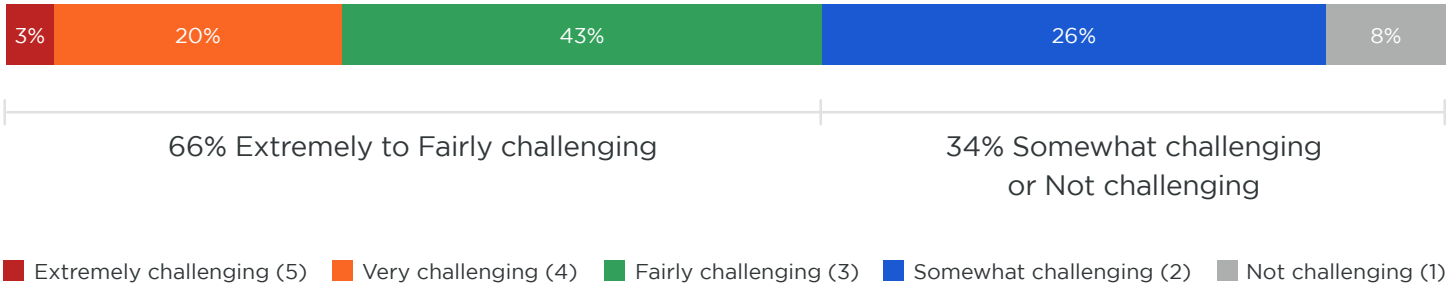
45% Have a project or are planning on one

illumio

How challenging is it to manage firewalls?

In a word: hard. Two thirds of respondents found their firewalls fairly to extremely challenging to maintain. Among their most pressing concerns were cost, troubleshooting, deployment and making changes.

OVERALL CHALLENGE OF MANAGING FIREWALLS

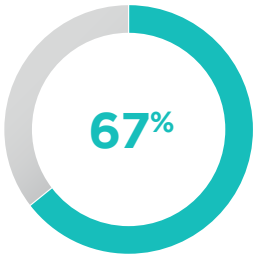


Did you know?

Security segmentation deploys 4-6 times faster than firewalls, and application updates can be taken care of in hours.

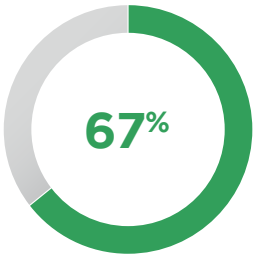
What's really wrong with firewalls?

The difficulties respondents had with their firewalls ranged from deployment to obtaining budgets, implementing changes and verifying them. Here's a look at how they described these challenges.



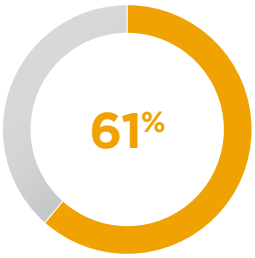
Initial deployment and tuning

67% say initial deployment and tuning of firewalls is extremely to somewhat challenging



Implementing changes

67% say implementing changes in firewalls is extremely to somewhat challenging



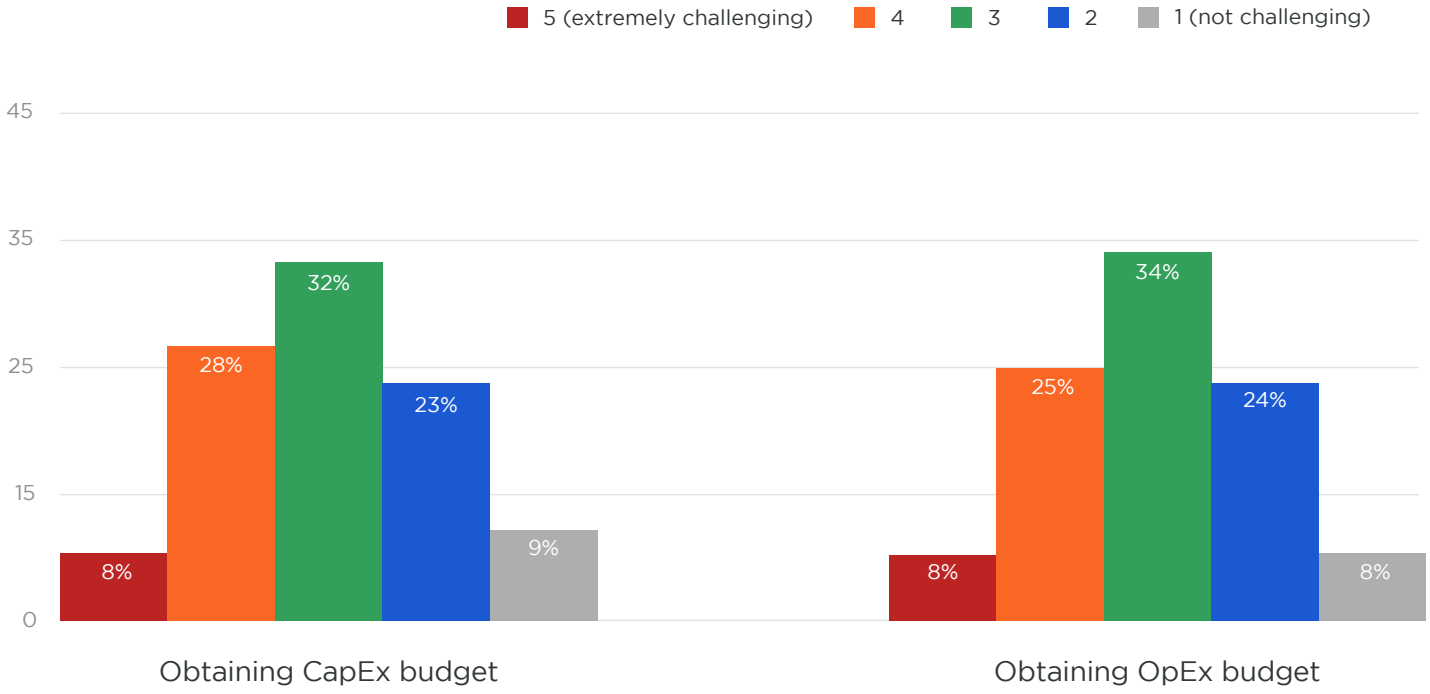
Verifying changes

61% say verifying changes within firewalls is extremely to somewhat challenging

illumio

Gold digging firewalls

One of the biggest obstacles was related to how hard firewalls hit your pocketbook. They are expensive, with 68% of respondents having a hard time securing initial capital budgets. And they are costly to maintain, with 66% having been challenged to some degree in finding operating expenditure budgets. Maybe this isn't surprising since firewalls are six-figure purchases and cost millions to implement and manage.



Did you know?

Security segmentation is a more cost effective and reliable option which uses firewalling built into the operating system. This can be at least 200% more cost effective.

illumio

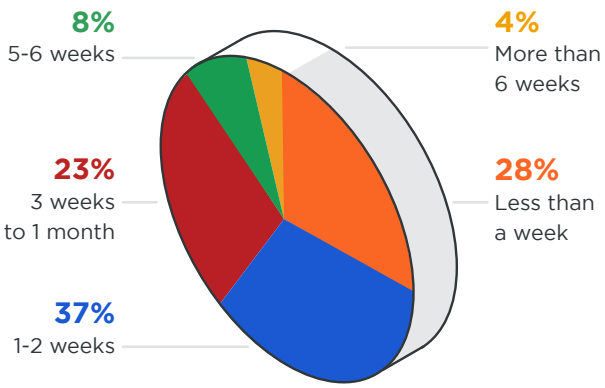
Broken app, broken career?

Like it or not, we often use 90s firewall technology to keep pace with today's DevOps. More than 2/3 of respondents acknowledge firewalls make it hard to test rules prior to deploying, making it easier to accidently misconfigure rules and break applications.

We don't need to remind you that code changes happen fast, requiring lots of timely firewall rule updates as part of the change control process. However, making a single firewall update to accommodate a new application or application behavior takes, on average, 1 to 2 weeks.

Accommodating new applications

The firewalls make it dead simple... to slow business, break apps and land people in the doghouse, career-wise.



1-2 weeks on average 37%

Only 28% of respondents confidently state that they can update segmentation firewalls to accommodate a new application or application update in less than a week.

What's the big deal?

Security segmentation is software-based and isn't tied to the network. What's the big deal? Well, here are a few of the benefits:

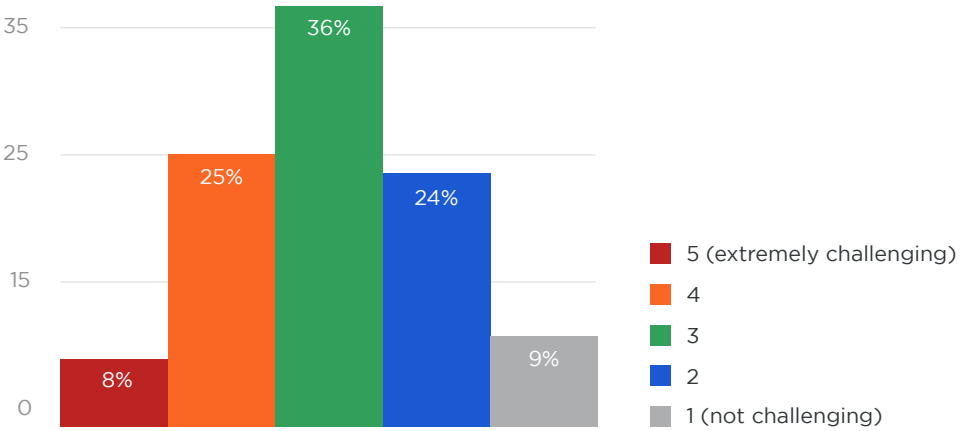
- Easy to test before deployment, never breaking apps;
- 90% fewer rules;
- And they can be updated in hours.

illumio

How long is too long?

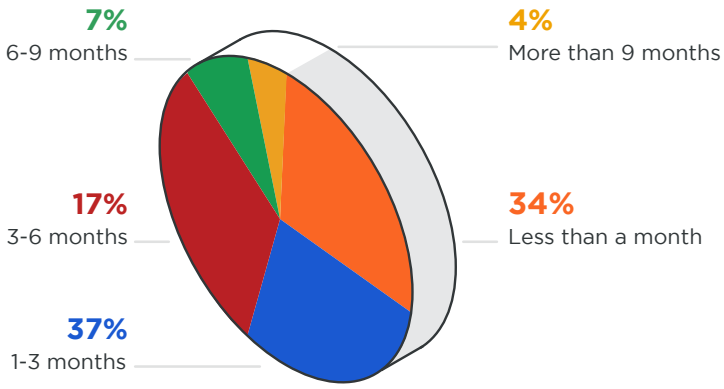
The average time for respondents to deploy and tune firewalls for segmentation was 1-3 months. Why do firewalls take so long? Well, let's begin with their size and complexity. Data center firewalls are huge, get dropped off on the loading dock, then require racking and stacking. They have thousands of complicated policy rules that need to be set-up, along with planning network segments, and then there's the change control process. It all adds up to months of deployment time.

LEVEL OF DIFFICULTY TO DEPLOY AND TUNE



Initial deployment and tuning

TIME TO DEPLOY AND TUNE FIREWALLS



1-3 months on average 37%

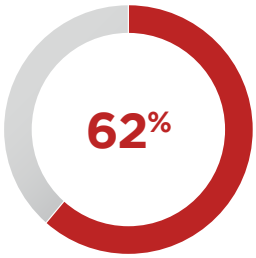
illumio

How many is too many?

The more the merrier when it comes to firewall rules... said nobody, ever.

62% of organizations have more than one thousand rules on each firewall used for segmentation. Given organizations have multiple sites and many firewalls, you won't be shocked to hear that some large organizations have hundreds of thousands of firewall rules.

Staying on top of massive rule sets for segmentation has become nearly impossible. Many rules have been in place for years that no one wants to touch for fear of screwing something up.



62% of organizations have more than one thousand rules on each firewall used for segmentation.

illumio

Why stay in a relationship with firewalls?

Because change, even for the positive, is uncomfortable. 57% cite potential risks induced by change as the leading reason why they won't stop using firewalls. Many also worry about organizational resistance to change, the problems that would arise and the troubleshooting headaches it would cause.

The undelivered promise of SDN

Despite concerns over migrating away from firewalls, most companies are evaluating software-defined networking. Some are considering trying to use it for rudimentary segmentation also. Almost 30% of companies are already in the process of deploying it or have already done so.

CURRENT STATUS OF SOFTWARE-DEFINED NETWORKS (SDN)

29% Deployed or deploying

56% Estimation about or Have a plan

15 % No need

This vendor neutral research was independently conducted by Virtual Intelligence Briefing (ViB). ViB is an interactive on-line community focused on emerging through rapid growth stage technologies. ViB's community is comprised of more than 1.2M IT practitioners and decision makers who share their opinions by engaging in sophisticated surveys across IT domains including Information Security. The survey methodology incorporated extensive quality control mechanisms at 3 levels: Targeting, in-survey behavior, and post-survey analysis. The Calculated Margin of error is +/-3.4%. The Effective Margin of Error as a result of extensive quality controls to assure high data quality is estimated to be +/1 2.7%. Learn more about ViB's research capabilities at https://vibriefing.news/research-services/.

illumio

The final frontier... for segmentation

Despite their shortcomings, firewalls for segmentation are still the devil we know—if companies are ever bothering with segmentation to ensure headline-driving breaches never take hold.

We do see alternative approaches being considered, like host-based, security segmentation that leverages firewalling on workload operating systems to better protect data centers and clouds.

That's because it offers:

- Superior lateral data breach protection in data centers and cloud;
- The freedom of not being tied to the network;
- Ease and quickness of deployment;
- Being able to test rules prior to deployment;
- No risk of breaking applications;
- Cost effectiveness;
- And its sheer simplicity.

Illumio enables organizations to realize a future without high-profile breaches by providing visibility, segmentation, and control of all network communications across any data center or cloud. Founded in 2013, Illumio's Adaptive Security Platform® uniquely stops the lateral movement of attackers with real-time application dependency mapping coupled with security segmentation across container, virtual machine, and bare-metal environments. The world's largest enterprises, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite, trust Illumio to reduce cyber risk. For more information, visit www.illumio.com/what-we-do.