Rethink Firewalls

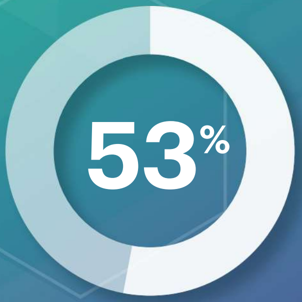
Security and Agility for the Modern Enterprise

Ponemon INSTITUTE | Guardicore

Independently conducted by
Ponemon Institute LLC

Sponsored by Guardicore

Contents



Over half of respondents report their organizations are ready for an alternative or complementary solution to their legacy firewalls.

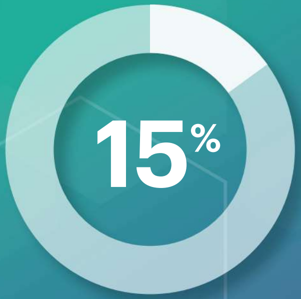
Introduction

Ponemon Institute is pleased to present the findings of the study on the effectiveness of legacy firewalls in an agile and hybrid environment. With sponsorship from Guardicore, Ponemon Institute surveyed 603 security professionals in the United States to gain insight into how legacy firewalls are used in the modern enterprise. Based on the findings, one of the most obvious trends we saw was that legacy firewalls are losing their effectiveness in securing applications and data in the cloud from cyberattacks. It's the primary reason we see the majority of respondents in this study, ready to find alternatives to their firewalls. This is to be expected. If security products do not evolve with the changing technology needs, it becomes that much more difficult to adhere to new security requirements.

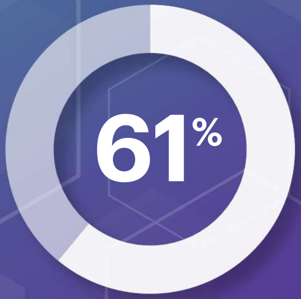
If the cybersecurity industry is to make better progress, all the ways in which we use legacy firewalls must be reconsidered in a new light, with a fresh perspective. This report invites you to rethink the use of legacy firewalls, to reevaluate your security posture, and to consider micro-segmentation as an addition or alternative to legacy firewalls in your organization.

What do we mean by Legacy Firewalls?

For the purposes of this research, we define legacy firewalls as network or NGFW appliances, including virtual firewall appliances. Legacy firewalls encompass both stateful and next-generation firewalls (NGFW). Stateful firewalls provide inspection of incoming and outgoing network traffic, while next-generation firewalls often include additional features such as threat intelligence, intrusion prevention (IPS), as well as application access and control.



Only 15% of respondents feel most prepared to defend against lateral movement with their legacy firewalls.



of respondents don't rely on their legacy firewalls to contain a breach of their organization's data center perimeter.

Research Highlights

Legacy firewalls are ineffective in preventing cyberattacks against applications.

More than 60% of respondents say their legacy firewalls don't prevent cyberattacks against critical business and cloud-based applications.

Legacy firewalls leave data centers vulnerable to a breach.

More than 60% of respondents don't rely on their legacy firewalls to contain a breach of their organization's data center perimeter.

Legacy firewalls do not protect against ransomware attacks.

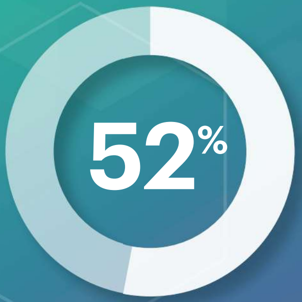
Only 36% of respondents believe that their legacy firewalls are effective against ransomware attacks.

Legacy firewalls are failing to enable Zero Trust.

More than 60% of respondents say their legacy firewalls do not enable Zero Trust across the enterprise.

Legacy firewalls are ineffective in securing applications and data in the cloud.

More than two thirds of respondents consider cloud security essential (34%) or very important (30%). However, only 39% of respondents say their legacy firewalls are very or highly effective in securing applications and data in the cloud.



of respondents say that legacy firewalls do not provide adequate security for internal data center east-west traffic.

Research Highlights (cont.)

Legacy firewalls kill flexibility and speed.

Organizations are at risk due to the lack of flexibility and speed in making changes to legacy firewall rules as reported by 57% of respondents. It takes three weeks to a month (32%) or more than a month (25%) to change firewall rules to accommodate an update or a new application.

Legacy firewalls lack granular access controls and are slow to implement.

Access control polices are not granular enough for 62% of respondents, while 48% respondents state it takes too long to implement segmentation with legacy firewalls.

Most organizations are ready to reduce their legacy firewall footprint.

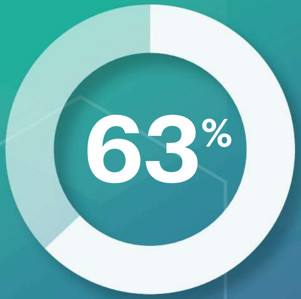
Over half of respondents say their organizations are ready for an alternative or a complementary solution. The two top reasons are: 1) the need to have a single security solution for on-premises and cloud data center security 2) to improve the ability to prevent lateral movement.

Legacy firewall costs are too high.

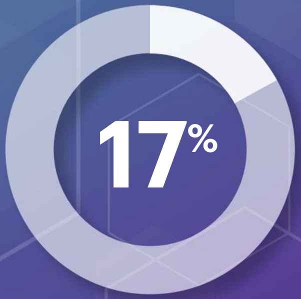
Two thirds of respondents would consider reducing their legacy firewall footprint due to the high labor and other costs.

Legacy firewalls do not protect against lateral movement.

More than half of respondents don’t trust their legacy firewalls to provide adequate security for internal data center east-west traffic.



of respondents say their organizations' legacy firewalls do not enable Zero Trust across the enterprise.



Only 17% of respondents rate their organization's legacy firewalls as very effective in protecting applications and data in the cloud.

Key Findings

In this section, we present a deeper dive into the findings from the research. The complete audited findings are featured in the **Appendix** of this report. We have organized the report according to the following topics:

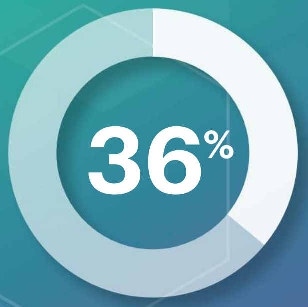
1 | **LEGACY FIREWALLS ARE INEFFECTIVE IN SECURING THE DATA CENTER**

2 | **LEGACY FIREWALLS ARE INSUFFICIENT FOR CLOUD SECURITY**

3 | **LEGACY FIREWALLS ARE NOT IDEAL FOR ZERO TRUST**

4 | **THE SEARCH FOR AN ALTERNATIVE SOLUTION TO THE LEGACY FIREWALL**

5 | **THE USE OF MICRO-SEGMENTATION AND SEGMENTATION IN A CHANGING IT ENVIRONMENT**



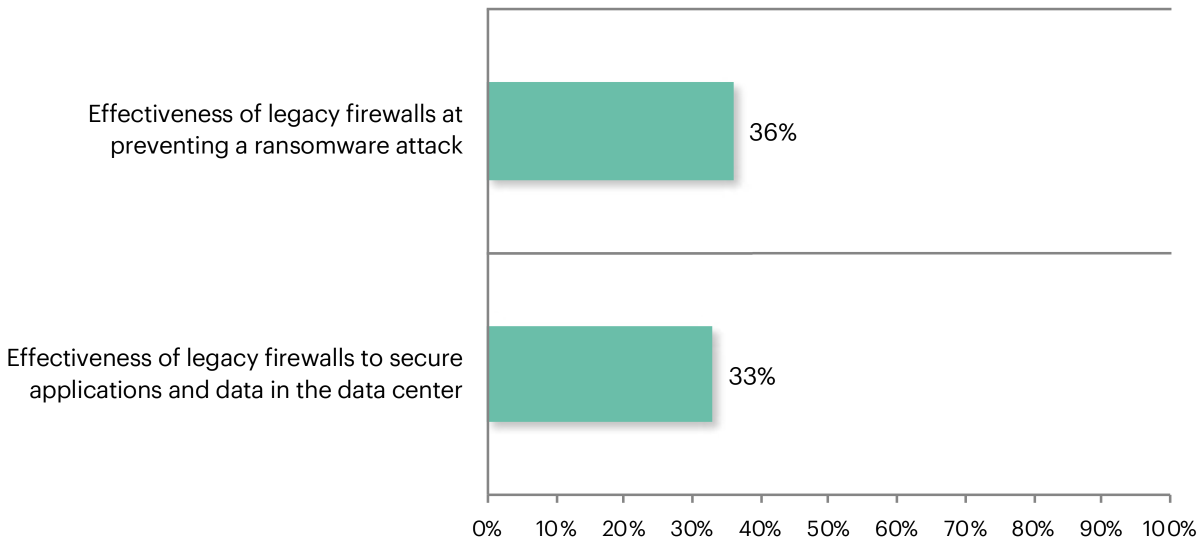
Only 36% of respondents believe that their legacy firewalls are effective in preventing a ransomware attack.

1 LEGACY FIREWALLS ARE INEFFECTIVE IN SECURING THE DATA CENTER

Respondents were asked how effective their legacy firewalls are on a scale from 1 to 10 where 1 indicates "not effective" and 10 indicates "very effective". **Figure 1** shows the responses of those who rated their firewalls effectiveness at 7 or higher. According to the Figure, only 33% of respondents say their organizations' firewalls are very or highly effective in securing applications and data in the data center. Legacy firewalls are also mostly ineffective at preventing a ransomware attack. Only 36% of respondents say their organizations' firewalls are highly effective in preventing such an attack. This means that two-thirds of respondents are not very or highly confident that their firewalls are effective to address these critical security use cases.

Figure 1. Effectiveness of legacy firewalls.

On a scale from 1 = not effective to 10 = very effective, 7+ responses presented



Guardicore

67%

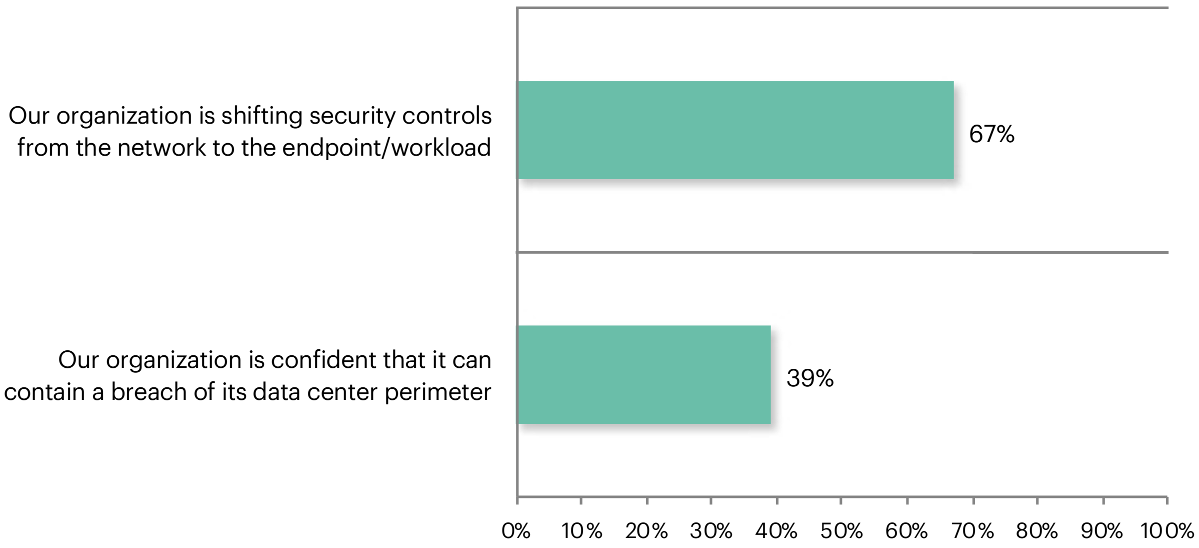
of respondents say their organizations are shifting security controls from the network to the endpoint/workload, indicating a change in strategy.

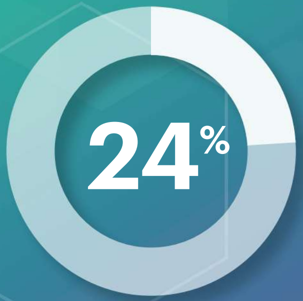
Legacy firewalls leave data centers vulnerable to a breach. As shown in **Figure 2**, only 39% of respondents say their organizations are confident that they can contain a breach of the data center perimeter.

To improve their ability to defend against breaches, 67% of respondents say their organizations are shifting security controls from the network to the endpoint/workload, indicating a change in strategy.

Figure 2. Perceptions about your organization's approach to cybersecurity in the data center, network and cloud.

Strongly agree and Agree responses combined



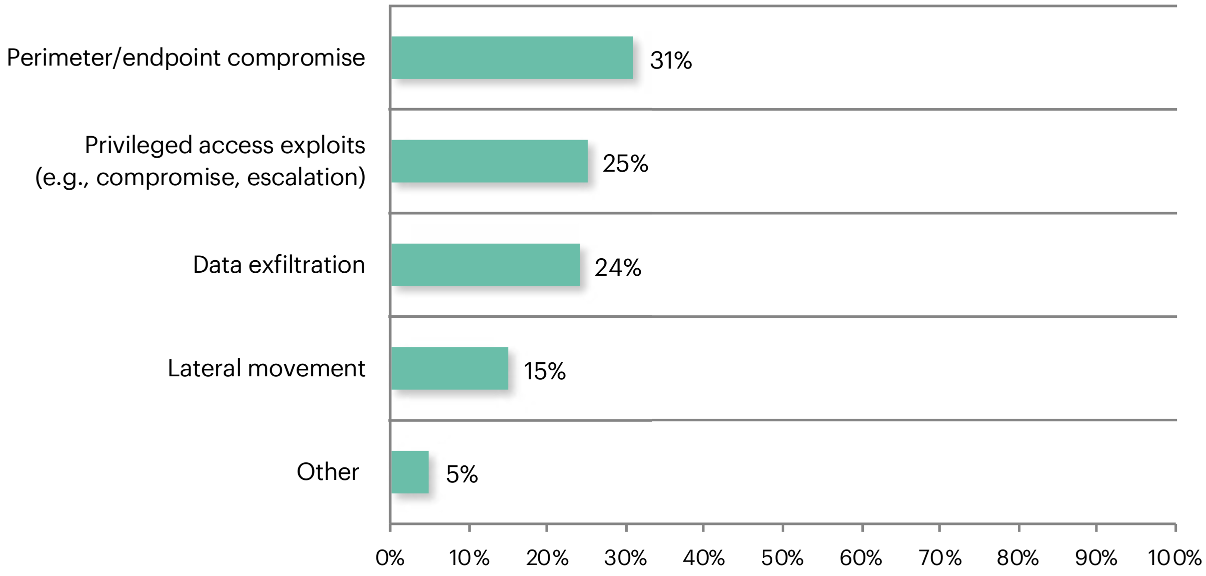


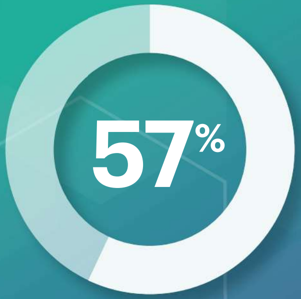
Only 24% of respondents believe that their legacy firewalls could defend against data exfiltration.

However, as shown in **Figure 3**, when asked what part of the attack cycle respondents' organizations are most prepared to defend against, only 31% of respondents say they are prepared to defend against the compromise of the data center perimeter or the endpoint/workload. This finding is followed by the preparedness to defend against the privileged access exploit with only 25% of respondents.

Figure 3. What part of the attack cycle does your organization feel most prepared to defend against?

Only one response permitted





of respondents say that it takes three weeks to one month (32%) or more than one month (25%) to configure legacy firewall rules.

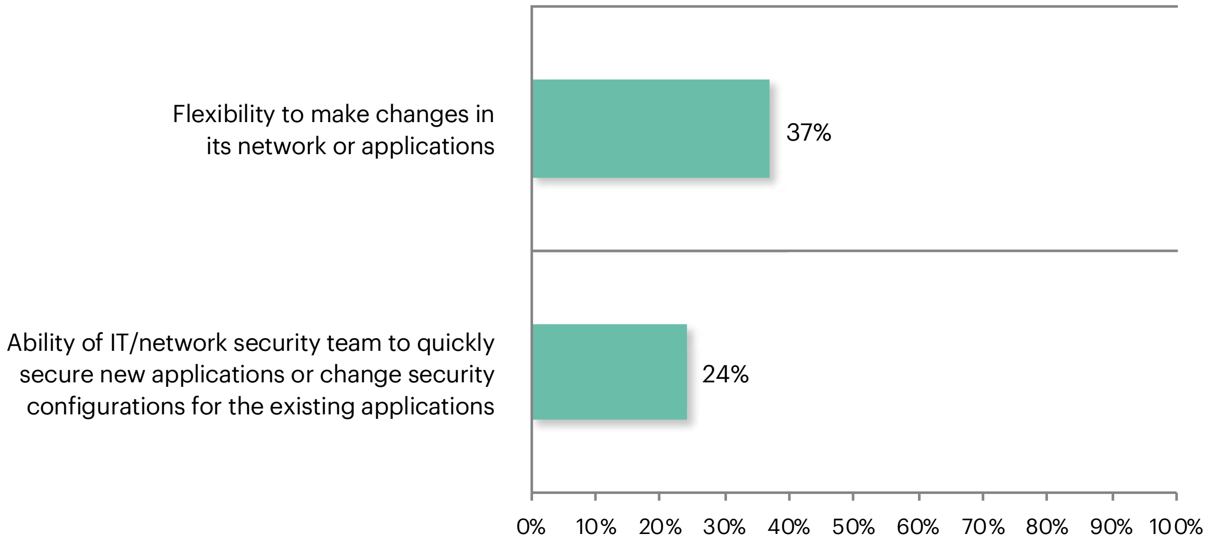
Only 24% of respondents rely on their legacy firewalls to quickly secure new applications or change security rules for the existing ones.

Legacy firewalls kill flexibility and speed. Organizations are at risk due to the lack of flexibility and speed in making changes to legacy firewall rules. Fifty seven percent of respondents say it takes three weeks to a month (32% of responses) or more than a month (25% of responses) to configure legacy firewall rules to accommodate an update or a new application.

As shown in **Figure 4,** only 37% of respondents say their organizations are very flexible in making changes to its network or applications and only 24% of respondents say their organizations have a high ability to quickly secure new applications or change security configurations for existing applications.

Figure 4. Perceptions about agility in the network security.

On a scale from 1 = no flexibility to 10 = high flexibility, 7+ responses presented



Multicloud is the use of two or more cloud environments of the same type (public or private) from different vendors.

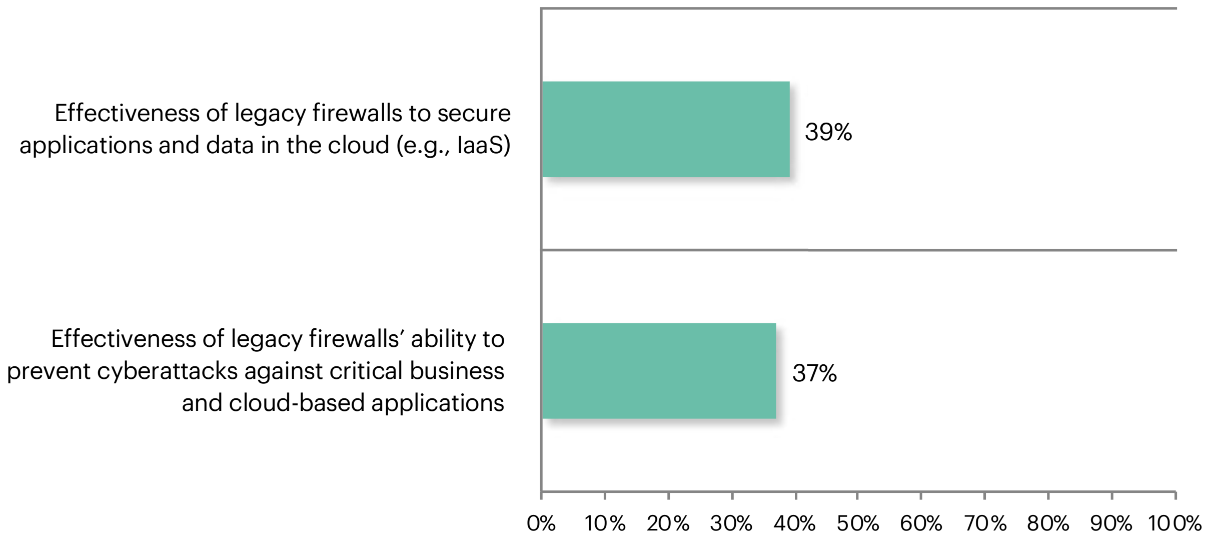
2 LEGACY FIREWALLS ARE INSUFFICIENT FOR CLOUD SECURITY

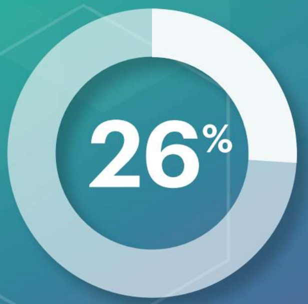
Legacy firewalls are not effective in securing applications and data in the cloud. Seventy-three percent of respondents say their organizations have multiple cloud environments and their use of cloud services averages to 43% of the entire IT environment.

Sixty-four percent of respondents say cloud security is essential (34%) or very important (30%). However, as shown in **Figure 5**, only 39% of respondents say the legacy firewalls are very or highly effective in securing applications and data in the cloud. Further, only 37% of respondents say their legacy firewalls' ability to prevent cyberattacks against critical business and cloud-based applications is high or very high.

Figure 5. Effectiveness of legacy firewalls in securing the cloud.

On a scale from 1 = not effective to 10 = very effective, 7+ responses presented





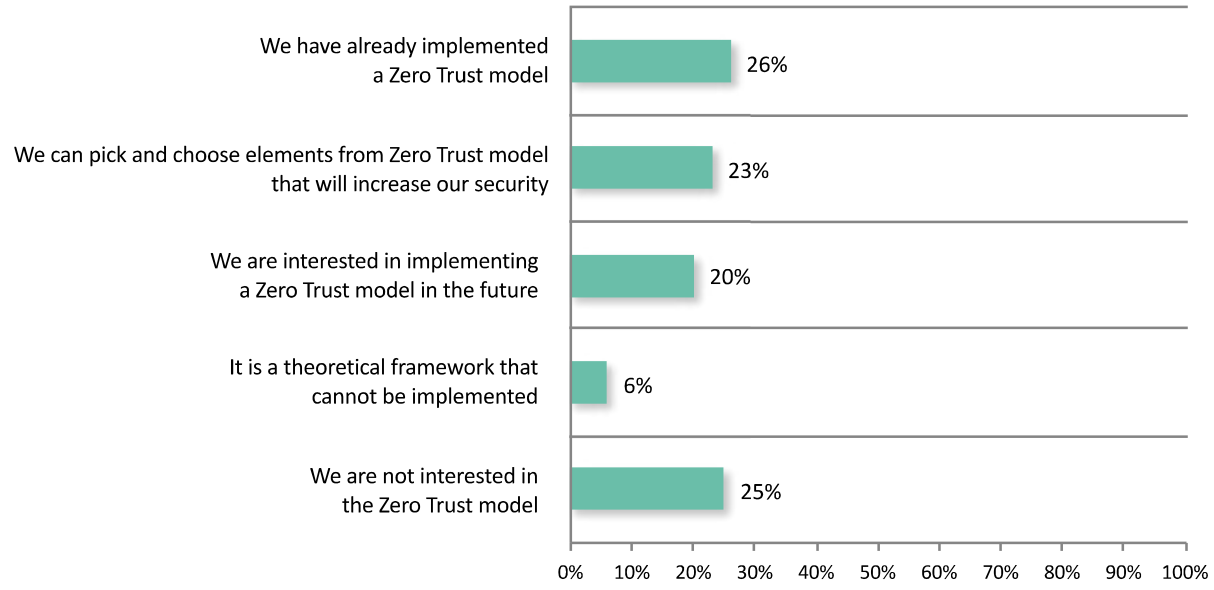
of respondents have already implemented a Zero Trust model.

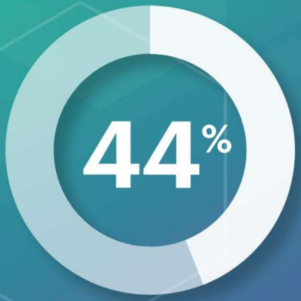
3 LEGACY FIREWALLS ARE NOT IDEAL FOR ZERO TRUST

Initially introduced by Forrester in 2010, Zero Trust assumes that every user, device, system or connection is already compromised (by default) whether they are inside or outside of the network. According to **Figure 6**, 49% of respondents have implemented a Zero Trust model to some extent.

As shown in this study, legacy firewalls are failing to enable Zero Trust across the enterprise. Out of the total respondents who report their organizations have implemented a Zero Trust model, only 37% rate their organizations' legacy firewalls as very or highly effective enabling Zero Trust across the enterprise.

Figure 6. Which one statement best describes your organization's approach to a Zero Trust security model?





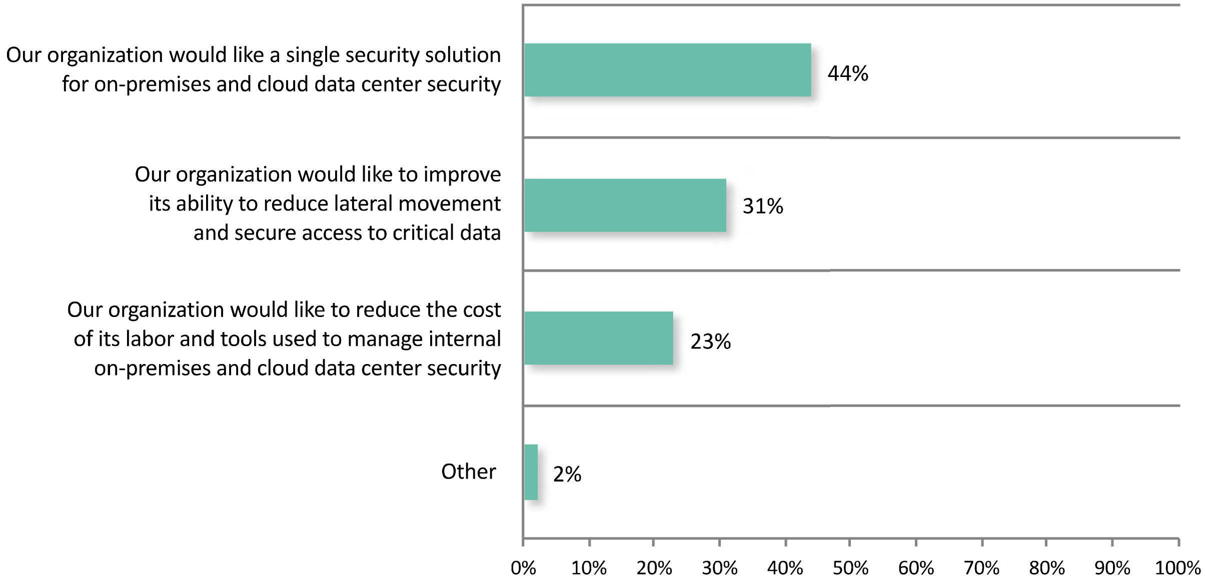
of respondents would like a single security solution for on-premises and cloud data center security.

4 THE SEARCH FOR AN ALTERNATIVE SOLUTION TO THE LEGACY FIREWALL

Most organizations are ready to reduce their legacy firewall footprint. Fifty-three percent of respondents say their organizations are ready for an alternative or a complementary solution.

As shown in **Figure 7**, the two top reasons are: 1) the need to have a single security solution for on-premises and cloud data center security (44% of respondents);
2) to improve the ability to reduce lateral movement and secure access to critical data (31% of respondents).

Figure 7. If your organization is ready to purchase alternative or complementary solutions, what best describes its readiness?

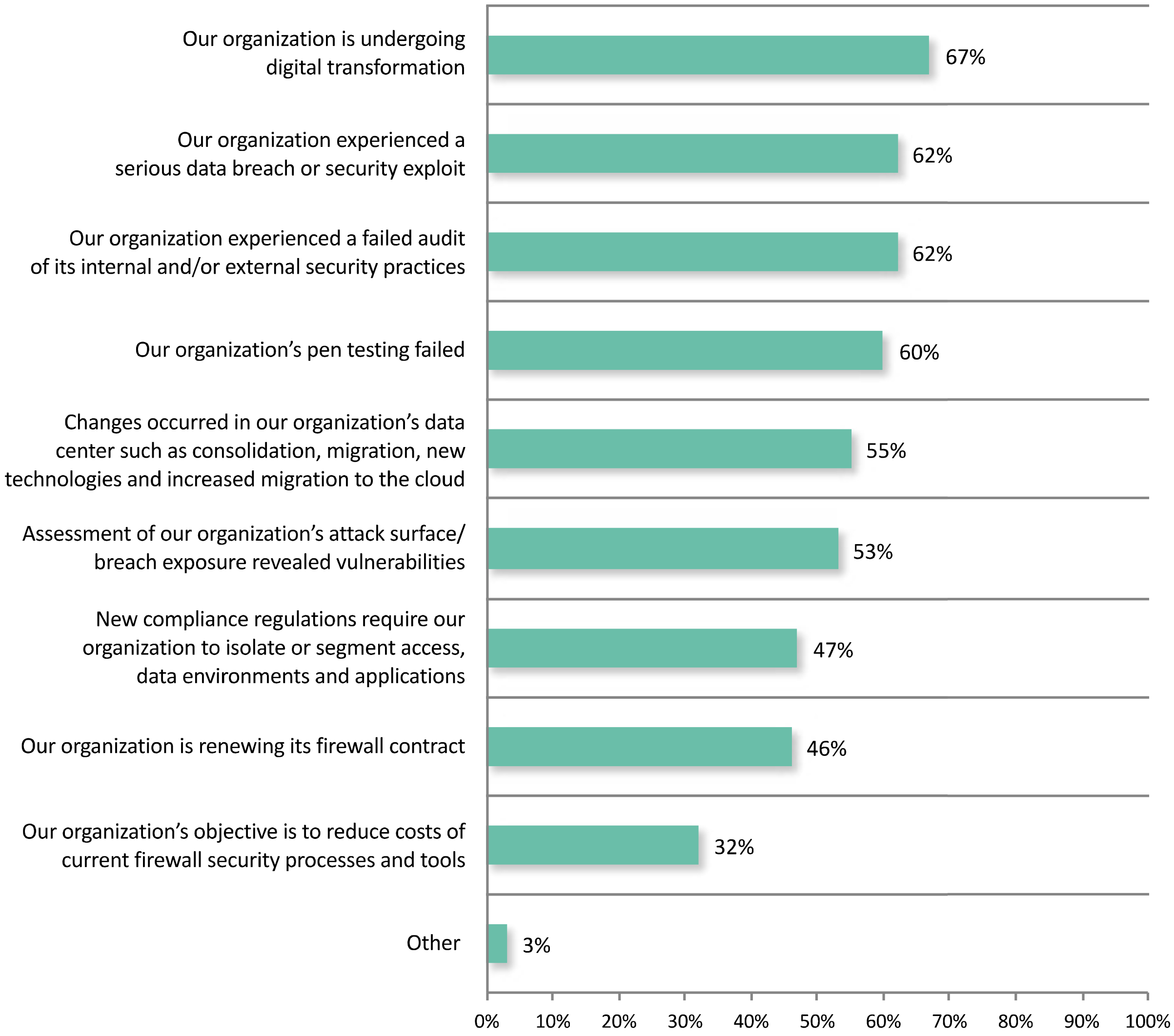


Certain events that could diminish an organization's security posture would encourage organizations to purchase an alternative or complementary solution to its existing firewall. Forty-seven percent of respondents are not considering investing in an alternative or complementary solution to its current firewall. However, certain events would make organizations reconsider their decision.

Figure 8 presents a list of events that could affect the security posture of an organization. The top four events are: going through digital transformation (67% of respondents), experiencing a serious data breach or security exploit (62% of respondents), having a failed audit of its internal and/or external security practices (62% of respondents), and having a failed pen test (60% of respondents).

Figure 8. What events would encourage your organization to invest in an alternative or complementary solution to its current firewall?

More than one response permitted



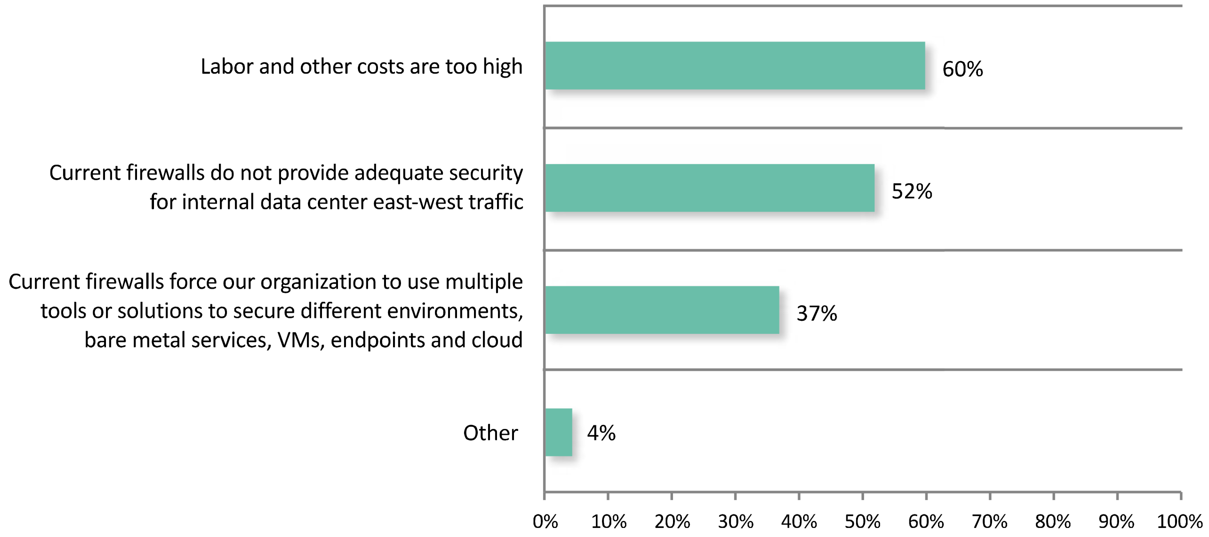
Guardicore

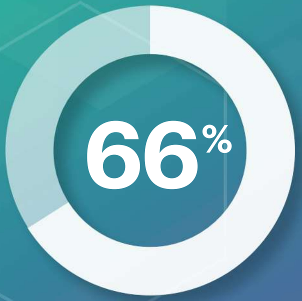
of respondents say their organizations would consider reducing their firewall footprint because of the high costs.

Legacy firewall costs are too high.
Two thirds of respondents would consider reducing their legacy firewall footprint because of the high costs. Organizations are considering a reduction in their firewall footprint because of high labor and other costs (60% of respondents) and current firewalls do not provide adequate security for internal data center east-west traffic (52% of respondents), as shown in **Figure 9**.

Figure 9. Why would your organization consider a reduction in its firewall footprint?

More than one response permitted





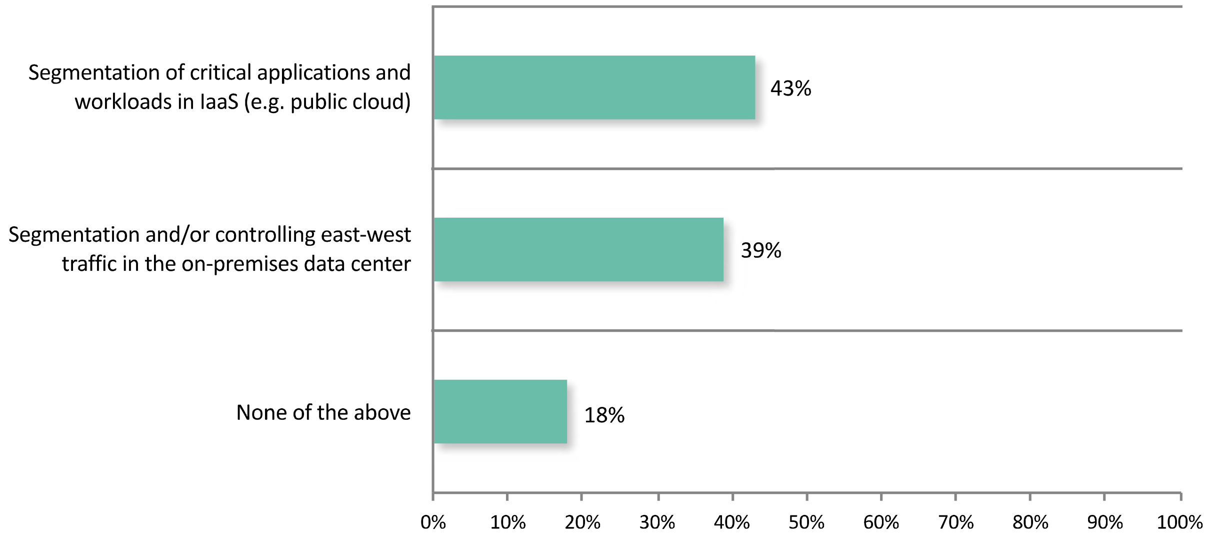
of respondents say that micro-segmentation is important to their organizations' security posture.

5 THE USE OF MICRO-SEGMENTATION AND NETWORK SEGMENTATION IN A CHANGING IT ENVIRONMENT

Micro-segmentation is important to organizations' security posture. Micro-segmentation is a technique of inserting security services between two workloads to isolate them from one another and secure them individually. It allows system administrators to deploy flexible security policies that restrict traffic between workloads based on the principle of least privilege.

Fifty-four percent of respondents say their organizations have adopted micro-segmentation. Out of these respondents, 66% say micro-segmentation is important to their organizations' security posture. As shown in **Figure 10**, 43% of these respondents say their organizations segment critical applications and workloads in IaaS and 39% of respondents say their organizations segment and/or control east-west traffic in the on-premises data center.

Figure 10. How does your organization use micro-segmentation?



Only 40% of respondents currently use legacy firewalls for network segmentation inside the data center.

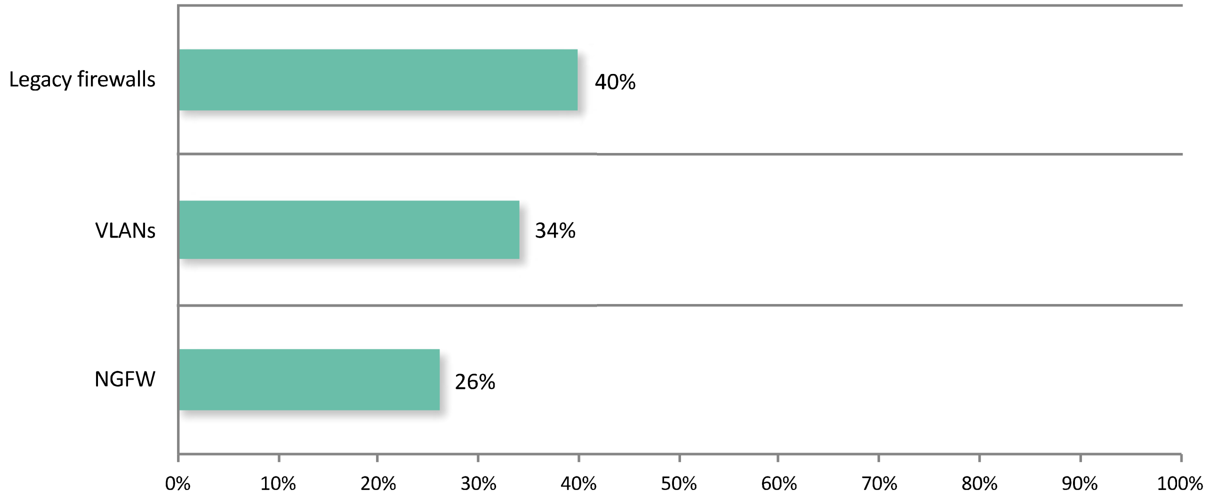
More than half of respondents have adopted network segmentation in their organizations.

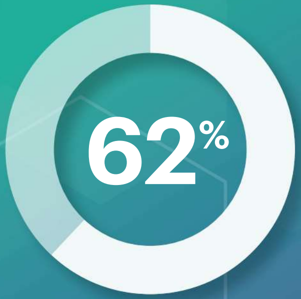
Network segmentation is a pivotal component in an organization's network security posture. Network segmentation is the practice of dividing an enterprise network into smaller sub-networks. Network segmentation is typically achieved by installing internal firewalls to restrict traffic between segments, improving network performance and efficiency, and improving security.

Fifty-four percent of respondents say their organizations have adopted network segmentation and 40% of these respondents say their organization uses legacy firewalls for network segmentation.

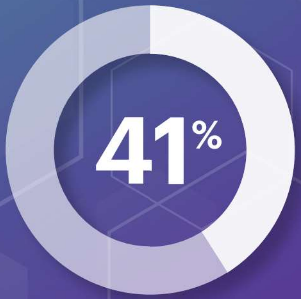
As shown in **Figure 11**, the tools most often used for network segmentation and/or controlling east-west traffic in the on-premises data center are legacy firewalls (40% of respondents) VLANs (34% of respondents) and NGFWs (26% of respondents). Virtual firewalls are most often used to achieve segmentation of critical applications and workloads in IaaS.

Figure 11. What tools does your organization use for network segmentation inside the data center?





of respondents say that the access control policies in their legacy firewalls are not granular enough.

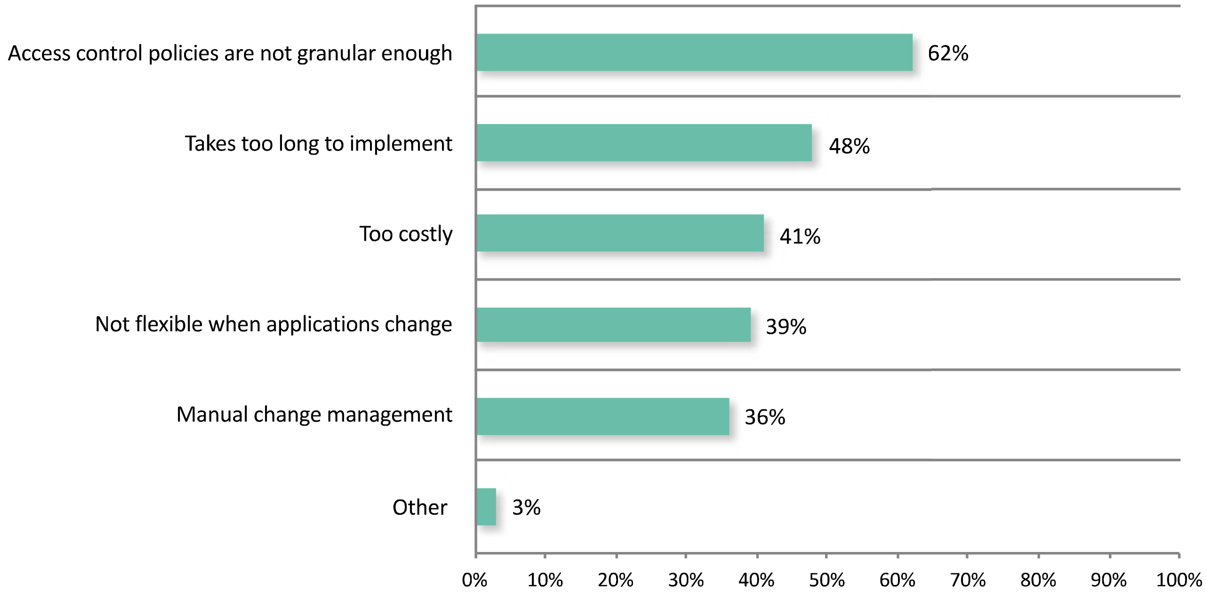


of respondents say that using legacy firewalls for network segmentation in the data center is too costly.

Legacy firewalls lack granular access controls and are slow to implement. According to **Figure 12**, the primary shortcomings when using legacy firewalls for network segmentation in the data center are: 1) access control policies are not granular enough (62% of respondents), 2) it takes too long to implement (48% of respondents) and 3) it is too costly (41% of respondents). It also takes more than a week to create a new VLAN for the purposes of network segmentation in the respondents' data center.

Figure 12. What are the shortcomings when using legacy firewalls for network segmentation in the data center?

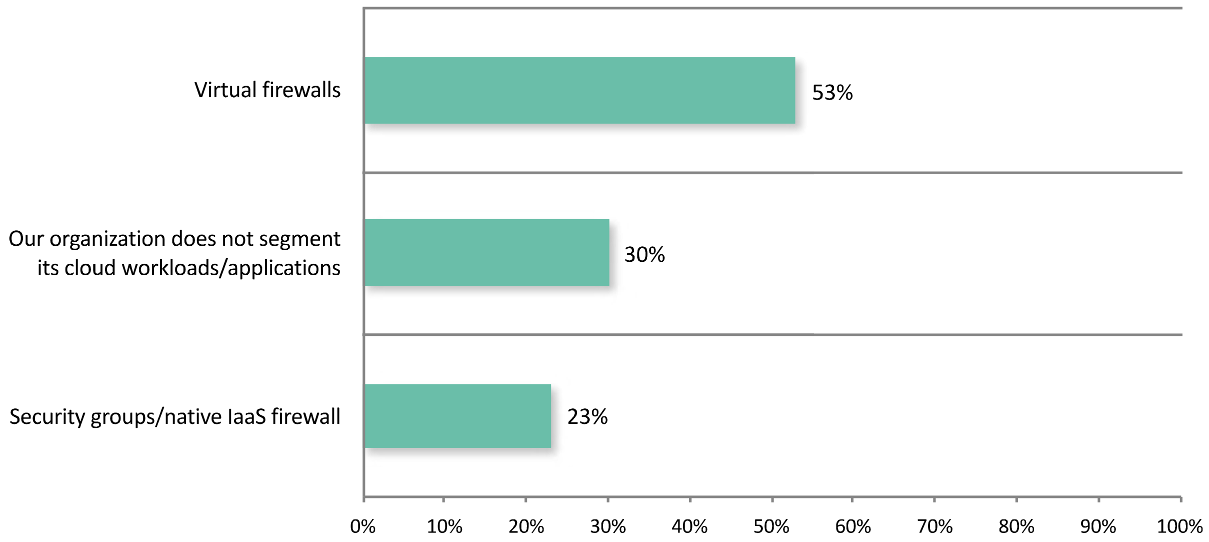
More than one response permitted



of respondents say their organization does not segment its cloud workloads or applications.

One-third of respondents say their organization does not segment its cloud workloads or applications. According to **Figure 13**, more than 50% of respondents' organizations use virtual firewalls to segment critical applications and workloads in IaaS.

Figure 13. What tools does your organization use to achieve segmentation of critical applications and workloads in IaaS?



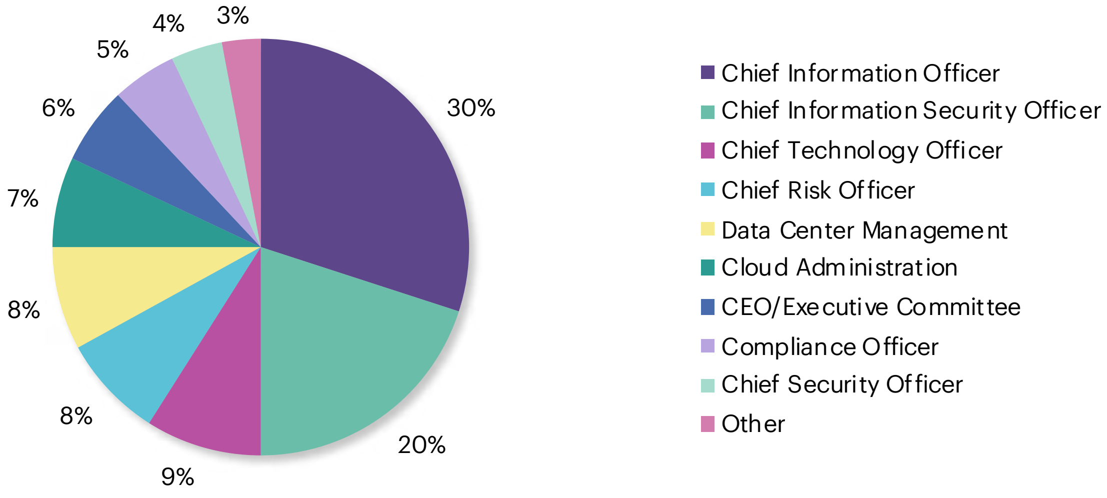
Methods

The sampling frame is composed of 16,240 IT and IT security practitioners who are familiar with the technologies used by their organization to protect the network and the data center. As shown in **Table 1,** 650 respondents completed the survey. Screening removed 47 surveys. The final sample was 603 surveys resulting in a 3.7% response rate.

Table 1. Sample response	**Freq**	**Pct%**
Total sampling frame	16,240	100.0%
Total returns	650	4.0%
Rejected or screened surveys	47	0.3%
Final sample	603	3.7%

As shown in **Pie Chart 1**, 30% of respondents report to the chief information officer, 20% of respondents report to the chief information security officer, 9% of respondents report to the chief technology officer, 8% of respondents indicated they report to the chief risk officer and 8% of respondents report to data center management.

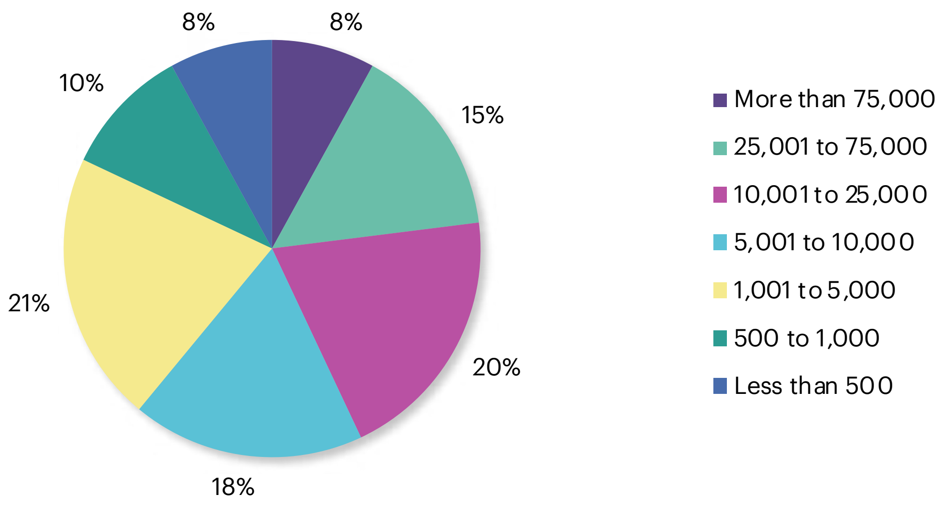
Pie Chart 1. Direct reporting channel.



Guardicore

Pie Chart 2 summarizes the total worldwide headcount of respondents' organizations. More than half (61%) of respondents are from organizations with a worldwide headcount greater than 5,000 employees.

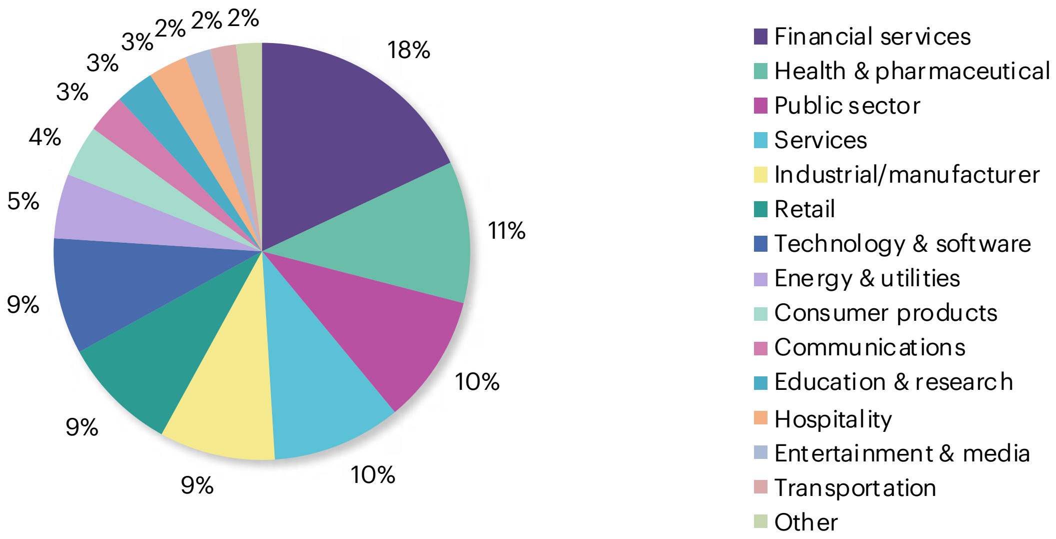
Pie Chart 2. Global headcount of respondents' organizations.



Pie Chart 3 shows the distribution of respondents' companies across 15 industries. Financial services represent the largest industry sector (18% of respondents), which includes banking, insurance, brokerage, investment management and payment processing.

This is followed by health and pharmaceutical (11% of respondents), public sector (10% of respondents), services (10% of respondents), industrial/manufacturer sector (9% of respondents), retail (9% of respondents) and technology and software (9% of respondents).

Pie Chart 3. Primary industry focus of respondents' companies.



Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias

The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling-frame bias

The accuracy is based on contact information and the degree to which the list is representative of individuals who are knowledgeable about the technologies used by their organization to protect the network and data center. Because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

Self-reported results

The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, the possibility remains that a subject did not provide accurate responses.

Appendix

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in September 2020.

Survey response	Freq	Pct%
Sampling frame	6,240	100.0%
Total returns	650	4.0%
Rejected surveys	47	0.3%
Final sample	603	3.7%

Part 1. Screening

S1. How familiar are you with the technologies used by your organization to protect the network and data center?	Pct%
Very familiar	45%
Familiar	37%
Somewhat familiar	18%
No knowledge (stop)	0%
Total	100%

S2. Has your organization deployed a legacy firewall as part of its network security protocol?	Pct%
Yes	100%
No (stop)	0%
Total	100%

Appendix (cont.)

S3. Do you have responsibility in managing cybersecurity activities within your organization?	Pct%
Yes, full responsibility	49%
Yes, some responsibility	51%
Minimum or no responsibility (stop)	0%
Total	100%

S4. What is your role in the purchase or use of firewall technology?	Pct%
Final decision maker	16%
I make recommendations	36%
I am a user/operator of firewalls	24%
All of the above	24%
None of the above (stop)	0%
Total	100%

S5. Do you and your team manage any of the following?	Pct%
On-premises data security only	33%
Cloud security only	29%
Both on-premises data security and cloud security	38%
Neither on-premises data security or cloud security(stop)	0%
Total	100%

Appendix (cont.)

Part 2.
Background on the IT infrastructure and security posture of organizations

Q1. How large is your organization’s IT infrastructure?	Pct%
Less than 500 servers/VMs	19%
500 to 1,000 servers/VMs	26%
1,001 to 5,000 servers/VMs	30%
More than 5,000 servers/VMS	25%
Total	100%
Extrapolated value	2,681

Q2. What part of the attack cycle does your organization feel most prepared to defend against? Please select only one choice.	Pct%
Perimeter/endpoint compromise	31%
Privileged access exploits (e.g. compromise, escalation)	25%
Lateral movement	15%
Data exfiltration	24%
Other (please specify)	5%
Total	100%

Appendix (cont.)

Please use the scale below each statement to express your opinions about your organization's approach to cybersecurity in the data center, network and cloud. Strongly Agree and Agree response combined.	Pct%
Q3a. Our organization is confident that it can contain a breach of its data center perimeter.	39%
Q3b. Our organization is shifting security controls from the network to the endpoint/workload.	67%

Q4. Which one statement best describes your organization's approach to a Zero Trust security model?	Pct%
We have already implemented a Zero Trust model	26%
We can pick and choose elements from Zero Trust model that will increase our security	23%
We are interested in implementing a Zero Trust model in the future (please skip to Q6)	20%
It is a theoretical framework that cannot be implemented (please skip to Q6)	6%
We are not interested in the Zero Trust model (please skip to Q6)	25%
Total	100%

Appendix (cont.)

Part 3.
Application workload security

Q5. Using the following 10-point scale, how would you rate the effectiveness of your organization’s legacy firewalls at enabling zero trust across the enterprise on a scale from 1 = not effective to 10 = highly effective.	Pct%
1 or 2	15%
3 or 4	22%
5 or 6	26%
7 or 8	18%
9 or 10	19%
Total	100%
Extrapolated value	5.58

Q6. Using the following 10-point scale, please rate the effectiveness of your organization’s use of legacy firewalls to secure applications and data in the cloud (e.g. IaaS) from 1 = not effective to 10 = very effective.	Pct%
1 or 2	20%
3 or 4	18%
5 or 6	23%
7 or 8	22%
9 or 10	17%
Total	100%
Extrapolated value	5.46

Appendix (cont.)

Q7. Using the following 10-point scale, please rate the effectiveness of your organization’s use of legacy firewalls to secure applications and data in the data center from 1 = not effective to 10 = very effective.	Pct%
1 or 2	17%
3 or 4	16%
5 or 6	34%
7 or 8	18%
9 or 10	15%
Total	100%
Extrapolated value	5.46

Q8. Using the following 10-point scale, please rate your organization’s flexibility to make changes in its network or applications from 1 = no flexibility to 10 = high flexibility.	Pct%
1 or 2	15%
3 or 4	25%
5 or 6	23%
7 or 8	22%
9 or 10	15%
Total	100%
Extrapolated value	5.44

Appendix (cont.)

Q9. Using the following 10-point scale, what is the ability of your organization's IT/network security team to quickly secure new applications or change security configurations for the existing applications on a scale from 1 = no ability to 10 = high ability.	Pct%
1 or 2	13%
3 or 4	27%
5 or 6	36%
7 or 8	14%
9 or 10	10%
Total	100%
Extrapolated value	5.12

Q10. Typically, how long does it take to update your legacy firewall rules to accommodate an update or a new application?	Pct%
Less than one week	12%
One to two weeks	31%
Three weeks to a month	32%
More than a month	25%
Total	100%

Appendix (cont.)

Part 4. Effectiveness of legacy firewalls

Please use the scale provided below each statement to express your opinions about your organization's legacy firewalls. Strongly Agree and Agree response combined.	**Pct%**
Q11a. Legacy firewalls and NGFW appliances are effective in restricting lateral movement in today's modern data centers.	34%
Q11b. Legacy firewalls are very flexible when it comes to segmentation of east-west traffic inside the data center.	38%

Q12. Using the following 10-point scale, please rate your organization's legacy firewalls' ability to prevent cyberattacks against critical business and cloud-based applications from 1 = no ability to 10 = high ability.	**Pct%**
1 or 2	11%
3 or 4	18%
5 or 6	34%
7 or 8	22%
9 or 10	15%
Total	100%
Extrapolated value	5.74

Appendix (cont.)

Q13. Using the following 10-point scale, please rate the effectiveness of your organization's legacy firewalls at preventing a ransomware attack on a scale from 1 = not effective to 10 = highly effective.	Pct%
1 or 2	9%
3 or 4	12%
5 or 6	43%
7 or 8	21%
9 or 10	15%
Total	100%
Extrapolated value	5.92

Q14a. What is your organization's perceptions about keeping its current firewall?	Pct%
Our organization would like to reduce the cost of its labor and tools used to manage internal on-premises and cloud data center security	23%
Our organization would like to improve its ability to reduce lateral movement and secure access to critical data	31%
Our organization would like a single security solution for on-premises and cloud data center security	44%
Other (please specify)	2%
Total	100%

Appendix (cont.)

Q14b. If ready to purchase alternative or complementary solutions, which one statement best describes your organization's readiness? Please select only one choice.	Pct%
Our organization would like to reduce the cost of its labor and tools used to manage internal on-premises and cloud data center security	23%
Our organization would like to improve its ability to reduce lateral movement and secure access to critical data	31%
Our organization would like a single security solution for on-premises and cloud data center security	44%
Other (please specify)	2%
Total	100%

Appendix (cont.)

Q14c. If your organization is not currently considering alternatives or complementary solutions to its current firewalls, would any of the following events change its decision? Please select all that apply.	Pct%
Our organization's objective is to reduce costs of current firewall security processes and tools	32%
Our organization is renewing its firewall contract	46%
Changes occurred in our organization's data center such as consolidation, migration, new technologies and increased migration to the cloud	55%
New compliance regulations require our organization to isolate or segment access, data environments and applications	47%
Our organization experienced a failed audit of its internal and/or external security practices	62%
Our organization's pen testing failed	60%
Assessment of our organization's attack surface/breach exposure revealed vulnerabilities	53%
Our organization experienced a serious data breach or security exploit	62%
Our organization is undergoing digital transformation	67%
Other (please specify)	3%
Total	487%

Appendix (cont.)

Q15a. Is your organization considering a reduction in its firewall footprint?	Pct%
Yes	51%
No (please skip to Q16)	44%
Unsure	5%
Total	100%

Q15b. If yes, why?	Pct%
Labor and other costs are too high	60%
Current firewalls do not provide adequate security for internal data center east-west traffic	52%
Current firewalls force our organization to use multiple tools or solutions to secure different environments, bare metal services, VMs, endpoints and cloud	37%
Other (please specify)	4%
Total	153%

Appendix (cont.)

Part 5. The use of micro-segmentation and segmentation

Q16. Has your organization adopted micro-segmentation?	Pct%
Yes	54%
No (please skip to Q21)	46%
Total	100%

Q17. Which team is most responsible for micro-segmentation in your organization? Please select only one choice.	Pct%
IT security/security operations	35%
Network operations	30%
No team is most responsible	32%
Other (please specify)	3%
Total	100%

Q18. How extensively has micro-segmentation been deployed in your organization?	Pct%
Fully deployed	29%
Partially deployed	46%
Deployed on a limited basis	25%
Total	100%

Appendix (cont.)

Q19. How important is micro-segmentation to your organization's overall security posture?	Pct%
Essential	10%
Very important	35%
Important	21%
Somewhat important	11%
Not important	23%
Total	100%

Q20. How does your organization use micro-segmentation? Please select all that apply.	Pct%
Segmentation and/or controlling east-west traffic in the on-premises data center	39%
Segmentation of critical applications and workloads in IaaS (e.g. public cloud)	43%
None of the above	18%
Total	100%

Q21. Has your organization adopted network segmentation?	Pct%
Yes	54%
No (please skip to Q26)	46%
Total	100%

Appendix (cont.)

Q22. Does your organization use legacy firewalls for network segmentation inside the data center?	Pct%
Yes	40%
No	60%
Total	100%

Q23. What tools does your organization use for network segmentation and/or controlling east-west traffic in the on-premises data center? Please select all that apply.	Pct%
Legacy firewalls	40%
VLANs	34%
NGFW	26%
Other (please specify)	0%
Total	100%

Q24. What are the shortcomings when using legacy firewalls for network segmentation in the data center? Please select all that apply.	Pct%
Takes too long to implement	48%
Not flexible when applications change	39%
Access control policies are not granular enough	62%
Manual change management	36%
Too costly	41%
Other (please specify)	3%
Total	229%

Appendix (cont.)

Q25. On average, how long does it take to create a new VLAN for the purposes of network segmentation in your data center?	Pct%
1 day	10%
2 to 7 days	21%
More than 1 week	33%
More than 2 weeks	36%
Total	100%

Q26. What tools does your organization use to achieve segmentation of critical applications and workloads in IaaS (e.g. public cloud)?	Pct%
Virtual firewalls	53%
Security groups/native IaaS firewall	23%
Our organization does not segment its cloud workloads/applications	30%
Total	106%

Appendix (cont.)

Part 6.
Security in the cloud

Q27. What best describes your organization's use of cloud resources?	Pct%
Less than 15% of the entire IT environment	11%
15% to 25% of the entire IT environment	19%
26% to 50% of the entire IT environment	36%
51% to 75% of the entire IT environment	21%
76% to 100% of the entire IT environment	13%
Total	100%
Extrapolated value	43%

Q28. How important is cloud security to your organization's security posture?	Pct%
Essential	34%
Very important	30%
Important	15%
Somewhat important	11%
Not important	10%
Total	100%

Appendix (cont.)

Q29. How many cloud environments does your organization currently have?	Pct%
One	27%
Two to three	40%
More than three	33%
Total	100%
Extrapolated value	2.92

Part 7. Your role and organization

D1. Check the primary person you or your IT security leader reports to within the organization.	Pct%
CEO/Executive Committee	6%
Chief Information Officer	30%
Chief Information Security Officer	20%
Chief Risk Officer	8%
Chief Security Officer	4%
Chief Technology Officer	9%
Compliance Officer	5%
Data Center Management	8%
Cloud Administration	7%
Other (please specify)	3%
Total	100%

Appendix (cont.)

D2. What is the worldwide headcount of your organization?	Pct%
Less than 500	8%
500 to 1,000	10%
1,001 to 5,000	21%
5,001 to 10,000	18%
10,001 to 25,000	20%
25,001 to 75,000	15%
More than 75,000	8%
Total	100%

D3. What best describes your organization's primary industry classification?	Pct%
Agriculture & food services	1%
Communications	3%
Consumer products	4%
Defense & aerospace	1%
Education & research	3%
Energy & utilities	5%
Entertainment & media	2%
Financial services	18%
Health & pharmaceutical	11%

Appendix (cont.)

D3. What best describes your organization’s primary industry classification?	Pct%
Hospitality	3%
Industrial/manufacturer	9%
Public sector	10%
Retail	9%
Services	10%
Technology & software	9%
Transportation	2%
Other (please specify)	0%
Total	100%