Our sixth annual survey finds network security risk at an all-time high. Automation is not yet an essential part of the security operations toolkit. Hybrid environments add to the complexity and there is no true visibility into where exposures may lie.
The age of digital transformation is well under way. Organizations globally are adopting internet-of-things (IoT) and moving more of their data into cloud environments in an effort to refresh IT infrastructure, enhance productivity, improve customer experience and innovate in ways that were unimaginable a decade ago.

But digital transformation (DX) and interconnectedness have also brought with them a host of new challenges for enterprises — and one of the most pressing is their impact on security. Business leaders want faster performance from networks. Increased traffic must now pass through network firewalls quickly and securely. This means firewalls must be configured correctly — but all too often they are not as IT security teams still rely heavily on manual processes.

FireMon’s sixth annual State of the Firewall report examines how these challenges and stressors are changing the needs of security and risk mitigation teams. In our largest survey pool to date of 573 IT and security professionals, we probed how organizations are managing security amid this sea change of business technology. In addition to security challenges, survey respondents also highlighted the continued dependency on legacy technologies that is getting in the way of DX.

Throughout our research, we note three distinct themes that have emerged in connection with security and digital transformation, which will be examined in depth in this report:

1. **Lack of Automation**
   Manual processes still rule the day when it comes to configuring firewalls and managing change processes, and this is leading to costly misconfiguration errors.

2. **Network Complexity and Visibility**
   There is low confidence in the visibility into networks as an increasingly complex, hybrid environment makes it more difficult to have a full view of threats and vulnerabilities.

3. **Importance of Firewalls**
   Our research finds firewalls are very much a part of enterprise security strategies today — and survey respondents show no sign of slowdown in their firewall investments.

While firewalls continue to be a critical part of their holistic security approach, enterprises remain challenged by the lack of automation, network security complexity, and lack of overall network visibility.
CISOs and other security hiring managers are feeling the impact of lack of skilled talent to fill roles in information security. According to the InfoSec Institute, the shortage of cybersecurity professionals has grown to nearly three million globally, with approximately 498,000 job openings in North America alone. Research from ESG found 51% of organizations currently believe they have a “problematic shortage” of cybersecurity skills. And according to our own 2019 State of Hybrid Cloud Security report, 52% of respondents have a security team of 10 people or less.

The skills gap is a serious problem, and the rising number of breaches worldwide is testament to this. According to Statista, the United States alone saw 1,244 data breaches in 2018, which exposed 446.5 million records. Also, the cost of data breaches continues to rise. Ponemon Institute reports a typical data breach cost $3.86 million in 2019, up 6.4% from $3.62 million in 2018.

The growing number of breaches and their associated costs underscore the importance of having proper configuration of security devices, especially firewalls. Fine-tuning and optimizing firewall rules ensure the ideal balance between speed and security. But all too often, firewalls are misconfigured as a result of human error.

Through 2023, 99% of firewall breaches will be caused by firewall misconfigurations, not firewall flaws, according to Gartner research.¹

CHAPTER 1

Lack of Automation is a Prescription for Human Error

The change agent needed to address this problem is automation, which eliminates guesswork and errors stemming from manual tasks. Yet our report finds that 65% of respondents are not using automation to manage their environment (fig. 1) and 36% of respondents say that inaccuracies, misconfigurations or issues on the network account for 10%-24% of the changes that require rework. Of the 36% reporting inaccuracies and misconfigurations (fig. 2), 32% process between 10-24 change requests per week and 27% process between 25-99 change requests per week.

Fig. 1
How do you currently utilize automation to manage the firewall change process?

- Our change management process is ad hoc/manual (email requests to firewall admins, spreadsheets, etc.) 30.9%
- Our firewall change process is part of the IT change process, but rule engineering and pre-change assessments are done outside the IT change management system (tracked in word documents, spreadsheets, etc.) 33.9%
- Our change management process, including rule engineering, pre-change assessments and approvals, is automated, but not the technical firewall change 26.5%
- Our change management process is fully automated, including automated firewall policy changes (policy push) 8.7%

Fig. 2
What percentage of changes require rework do to inaccuracies, misconfigurations or issues on the network?

- 0% to 9% 2%
- 10% to 24% 2%
- 25% to 50% 10%
- 51% to 75% 36%
- >75% 50%
A lack of automation is also hindering innovation by tying up many teams who could be working on other crucial projects instead of routine requests. 72% of respondents have two or more teams involved in processing and/or approving a typical change request. And of the 72% with two or more teams involved, almost 30% of them have three teams involved in processing and/or approving a typical change request. This points to a clear case for replacing manual tasks with automation to eliminate process bottlenecks (fig. 3).
Cybercriminals can and will take advantage of human errors and mistakes in infrastructure configurations to launch attacks. One perfect example of the vulnerabilities posed by misconfiguration occurred earlier this year when 540 million data records from Facebook were discovered in misconfigured public cloud storage. This is one of many times when data in an Amazon S3 storage bucket was found in a misconfigured state.

The urgent calls that IT security teams receive to alert them to misconfigurations may be alarming, but this is not unusual. Our report reveals that 38% of respondents find out about a misconfigured firewall through urgent communications or phone, text, and email. These panic-inducing situations could be greatly reduced with automation, which can take firewall and network management from being reactive to proactive (fig. 4).

![Fig. 4](image.png)

How do you know when a misconfigured firewall causes issues in your network?

- Urgent communications reporting the issue via phone/text/email: 12%
- We have other methods in place that alert us when there is an issue: 24%
- Our security solution alerts my team about the issue: 26%
- I don’t know when a misconfigured firewall causes an issue in my network: 38%
Complexity + Lack of Visibility = A Black Eye on Your Hybrid Network

IT security teams are simply overwhelmed. Nearly one-third of the 2019 respondents have more than 100 firewalls on their network, up from 26% reported in 2018. And 33% have between 10 and 99 firewalls (fig. 5).

But more firewalls means more complexity. In fact, among the top five firewall challenges listed by respondents, all pointed to some level of frustration with complexity.

The top five challenges include:

1. Complexity of firewall rules/policies
2. Optimizing firewall rules
3. Managing multiple vendors/types of firewalls
4. Gaps in firewall enforcement
5. Lack of automation

Simply overwhelmed: Nearly 1/3 of respondents have more than 100 or more firewalls on their network.
CHAPTER 2

Complexity + Lack of Visibility
= A Black Eye on Your Hybrid Network

This state of complexity is exacerbated by a mix of different types of vendors now needed in a hybrid environment. 78% of respondents use two or more vendors for enforcement points on their network (fig. 6). Almost 60% of respondents have firewalls deployed in the cloud (fig. 7). Managing multiple vendors and types of firewalls is the third-most cited challenge when it comes to firewall management, calling out the dire need for consolidation, integration, and automation in the space.
A lack of overall network visibility is also stressing IT security teams, with 34% of respondents noting they have less than 50% percent of real-time visibility into network security risks and compliance. 28% of respondents said they have at least 80% of real-time visibility into network security risks and compliance (fig. 8); interestingly, only 23% of C-level respondents have at least 80% real-time visibility into network security risks and compliance.

Complexity + Lack of Visibility = A Black Eye on Your Hybrid Network

Fig. 8
On a scale from 1-10, what level of real-time visibility do you have into your network security risks and compliance across your entire environment?

Only 23% of C-level respondents have at least 80% real-time visibility into network security risks and compliance.
CHAPTER 2

Complexity + Lack of Visibility = A Black Eye on Your Hybrid Network

This leads to low confidence levels when it comes to internal or regulatory compliance. Almost one-fourth (24%) of respondents aren’t sure or wouldn’t admit if they failed a compliance audit in the last 12 months, (fig. 9) and only 51.3% of respondents are 60%-80% percent prepared for a compliance audit tomorrow (fig. 10). Among the executive suite, only 45.3% of C-level respondents felt ready for an audit.

The challenge of complexity and visibility is obvious – and managing information centrally is a big ask for IT security teams. A solution that normalizes data from disparate sources and gives a clear view into the hybrid network is critical to truly maximizing the power of your firewalls, and your overall security strategy.
Compliance pressures have never been higher for IT security managers. As the effects of the General Data Protection Regulation (GDPR) continue to be felt, reports of related fines are on the rise. Earlier this year, tech giant Google was fined $57 million by CNIL, a French data protection watchdog group. The regulatory body claimed that Google failed to comply with the law as part of a process for new Android users setting up a new phone.

Most enterprises simply can’t afford these extraordinary fines. And in ever-expanding cloud and hybrid environments, with the introduction of mobile and IoT devices, and with a non-stop, on-the-go workforce, many argue whether or not granular security technologies should replace the firewall for risk mitigation. But the results of our research clearly show that the firewall is still an integral part of a holistic security strategy for enterprises.
CHAPTER 3

Don’t Pull the Plug: The Firewall is Definitely Not Dead

Firewalls are still a pervasive technology, with 95% of respondents noting that firewalls are as critical as always, or more critical than ever, in their security architecture (fig. 11). C-Level respondents rated firewalls more critical than ever at 48%, 7% higher than non-C-Level respondents. An overwhelming 95% of the respondents said that the firewall will be as critical, or more critical than ever, in the next five years (fig. 12).

95% of respondents say that firewalls are as critical as always, or more critical than ever.

**Fig. 11**
How critical is the firewall as part of your overall security architecture today?

- As critical as always: 53.8%
- More critical than ever: 41.2%
- Less critical than in years past: 4.7%
- Not critical at all: 0.3%

**Fig. 12**
In the next five years, how critical will the firewall be to your overall security architecture?

- As critical as always: 55.2%
- More critical than ever: 39.4%
- Less critical than in years past: 4.5%
- Not critical at all: 0.9%
CHAPTER 3

Don’t Pull the Plug: The Firewall is Definitely Not Dead

Spending on firewalls is on the rise as well. A majority, 65% of respondents, spend between 10% and 49% of their security budget on firewall technology (fig. 13). This is an increase from our 2018 State of the Firewall report where 56% of respondents said they spent between 10% and 49% of their security budget on firewalls. Conversely, only 11% of respondents have already deployed Firewall as a Service (FWaaS) or other alternative infrastructure-as-code solutions.

The firewall is still very much a part of the overall security architecture, and it does not appear that IT security managers are pulling the plug on their firewalls now or anytime in the near future.

Fig. 13
What percentage of your total network security budget do you currently spend on all firewall technology (software, hardware, maintenance)?

- < 10%: 16%
- 10%-24%: 30%
- 25%-49%: 49%
- ≥ 50%: 5%

72% of respondents don’t think firewalls will become obsolete with next-gen architectures like Software-Defined Networks (SDN), Zero Trust, etc.
Conclusion

As organizations grapple with the changing state of growing and complex network environments, they must have solutions that address the entire enterprise. The firewall will continue to be part of their security strategy moving forward, but it is critical for enterprises to look at automation to further shore up defenses and ensure misconfiguration mistakes do not make them the next big headline on data breaches.

Implementing automation will help enterprises:

- Reduce human error by eliminating misconfigurations that can increase their attack surface
- Eliminate the friction between DevOps and SecOps so they can deliver security at the speed of the business
- Increase security agility while shortening SLA timeframe
- Maximize efficiency while reducing operational and security costs
- Prevent compliance violations through continuous monitoring of global security policies across their hybrid environment

However, automation isn’t something that is just “turned on.” Enterprises need flexible levels of security automation tailored to their pace and confidence level. It must be done mindfully, with individual needs considered, in order to be done right. When implemented correctly, it can deliver consistency, cost savings, ongoing visibility and assessment, and effective risk management.

As firewalls continue to play a critical role in security and risk mitigation, FireMon’s approach to security policy automation offers enterprises flexibility, intelligence, and control in the automation process. We give IT security teams the context they need to determine and implement change without introducing new risk – and that gives you the confidence and visibility you need to ensure complete security in the midst of rapid change.

Learn more about FireMon Automation.
APPENDIX

The 2019 State of the Firewall survey was designed with a total of 30 questions covering demographics, firewall operations, and the cloud and next-gen architectures.

A total of 573 complete survey responses were collected from July 26, 2019 through September 6, 2019.

Which geographic region is your organization located in?

- Asia Pacific (APAC): 9%
- Australia: 7%
- Europe, Middle East & Africa (EMEA): 1%
- Latin America (LATAM): 1%
- North America: 2%
- Other: 80%

What best describes your position within your organization?

- Auditor: 3.1%
- Cloud Security Architect: 2.0%
- Compliance Manager: 2.8%
- DevOps: 4.0%
- Firewall Administrator: 4.5%
- IT Ops Manager: 20.1%
- Network/Security Engineer: 20.9%
- Security Operations/Architect: 13.8%
- Other: 10.3%
## APPENDIX

### What is your company size by number of employees?

<table>
<thead>
<tr>
<th>Employee Size</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 1,000 employees</td>
<td>47.8%</td>
</tr>
<tr>
<td>1,000-4,999 employees</td>
<td>18.2%</td>
</tr>
<tr>
<td>5,000-14,999 employees</td>
<td>15.2%</td>
</tr>
<tr>
<td>&gt; 15,000 employees</td>
<td>18.8%</td>
</tr>
</tbody>
</table>

### Which industry best describes your organization?

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Services</td>
<td>4.2%</td>
</tr>
<tr>
<td>Education</td>
<td>8.9%</td>
</tr>
<tr>
<td>Energy</td>
<td>3.1%</td>
</tr>
<tr>
<td>Finance</td>
<td>11.7%</td>
</tr>
<tr>
<td>Government</td>
<td>8.9%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>6.6%</td>
</tr>
<tr>
<td>Insurance</td>
<td>2.4%</td>
</tr>
<tr>
<td>IT Services</td>
<td>32.0%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>7.9%</td>
</tr>
<tr>
<td>Retail</td>
<td>3.5%</td>
</tr>
<tr>
<td>Other</td>
<td>10.8%</td>
</tr>
</tbody>
</table>