FIREMON PULSE

The Future of Network Security

Through the Turbulence of IT Transformation, Clear Priorities Emerge for Network Security

1 Introduction

We won't bore you with details about why network security is getting more challenging. You already have a front row seat. But here's the short version:

- Always-on always-multiplying threats
- Skyrocketing complexity caused by accelerated adoption of cloud/hybrid networks
- A pandemic-fueled explosion in the permanently distributed and remote workforce
- Business demands for an ever-increasing drive for agility, speed of innovation, and impeccable user experiences

To complicate matters, the journey to the cloud is a long one. Most organizations will live in a hybrid world for many years to come - creating new challenges in managing access to resources distributed across disparate systems.

So, the question is, where should your organization place its chips to ensure a secure, compliant, and agile future?

This report is designed to help you understand: (a) **How your peers are prioritizing their investments to prepare for the future**; and (b) **the drivers behind those priorities**.

We welcome your feedback and comments.

Satin H. Mirchandani
President & CEO
FireMon

2 Survey Methodology

Pulse Media, a 27,000+ member knowledge community for verified technology leaders, and **FireMon**, the leading network security policy management company for enterprise cloud and hybrid network infrastructure, surveyed 500 directors, vice presidents and C-Suite involved in IT security for organizations of between 1,001 to 10,000+ employees.

This study, completed in January 2021, was conducted to learn how respondents' network security operations have changed as a result of major trends, the solutions they're planning to implement in the next 12 months, and the most critical initiatives they're launching to optimize their network security posture.

500 IT Security Leaders from North America and EMEA*

Company size

10,000+ employees	24%
5,001 - 10,000 employees	21%
1,001 - 5,000 employees	55%

Title

C-Suite	23%
VP	27%
Director	49%
Manager	1%

Industry

Finance, Banking & Insurance	32%
Retail	28%
Health Care & Social Assistance	25%
Utilities	9%
Government	6%

* Europe, Middle East and Africa.

3 Executive Summary

Given the magnitude of the network security challenges and the speed with which they are shifting, according to Forrester, 62%* of security decision-makers expect to increase spending on network security in 2021 in areas including:

- Growing security threats
- Acceleration of cloud adoption
- Proliferation of complex distributed infrastructure/hybrid architectures
- Rise of DevOps and demand for agility and rapid innovation
- Difficulty of system and software integration and interoperability
- Increasingly remote, and distributed, and mobile workforce

Given those challenges, the question is:

Where are your peers investing?

Our survey revealed that, even in the face of unprecedented enterprise demands, complexity and uncertainty, clear priorities are emerging in several key areas to achieve “secure agility” in a heterogeneous hybrid or cloud-based future. These investments include **security automation**; **Zero Trust Architecture**; and best of breed security technology with **flexible APIs** for integration. These and other primary themes will be examined further in this report.

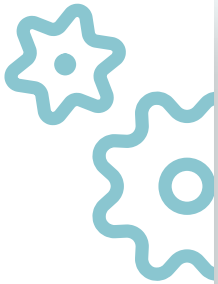
* SOURCE: Forrester, The State of Network Security, 2020 to 2021

4

Key Findings

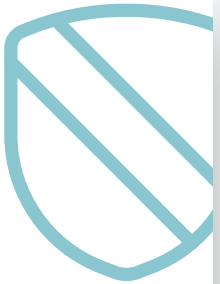
A

Amping Up Automation



B

Embracing Zero Trust



C

Implementing SASE

D

Addressing Security-Dev Misalignment

E

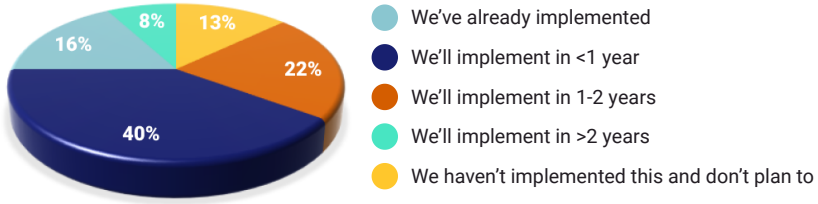
Managing Accelerating Heterogeneity

Amping Up Automation

The need for speed is driving widespread investments in security automation

with nearly 8 in 10 respondents saying they'll implement security orchestration and automation within 2 years and 98% of organizations having already automated security policies to some degree.

Most organizations have already implemented security orchestration and automation or plan to in the next 2 years.



The top drivers behind an organization's decision to implement security orchestration and automation are:

1. Improving agility and responsiveness
2. Reducing time to discovery and resolution
3. Improving compliance
4. Improving security efficiency through automation

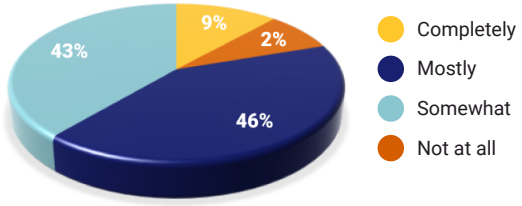
Amping Up Automation

What is typically an inefficient, manual and therefore risky function,

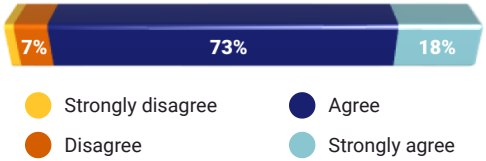
management of network security policies, is a key area where automation is being adopted.

In fact, more than 9 in 10 organizations agree that network security policy management (NSPM) is a strategic investment to help them improve speed and responsiveness.

Only 9% of organizations have completely automated their network security policies.



To combat rising complexity, network security policies automation will spike in the next 2 years.



53%
plan to invest in NSPM within 12 months

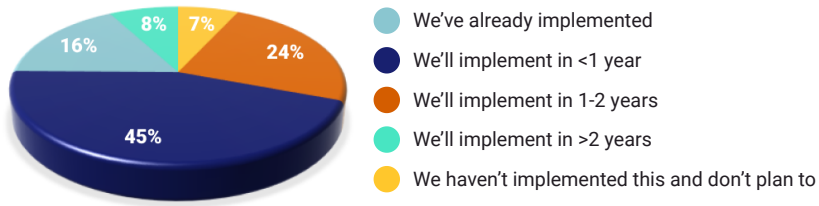
Embracing Zero Trust

Fueled by a more distributed and mobile workforce and increasing reliance on cloud-based applications,

86% organizations have either implemented a Zero Trust Architecture (ZTA)

or plan to do so within 2 years.

Zero Trust will achieve broad adoption, with 69% of organizations planning to implement within 2 years. This is in addition to the 16% that have already implemented.



The decision to adopt Zero Trust is driven in large part by:

1. Greater need for secure remote access due to COVID-19
2. Reducing cybersecurity risk
3. Supporting the transition to cloud architectures
4. Streamline trusted user access to corporate applications
5. Managing risk from third-party software, BYOD, and shadow IT

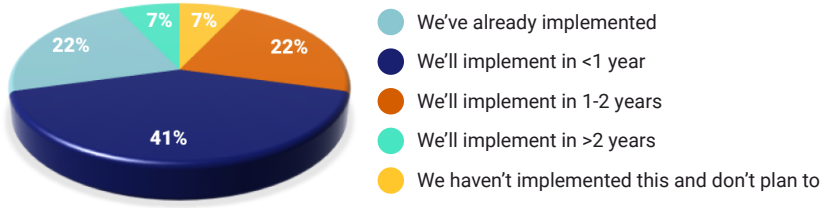
Implementing SASE

To many experts, the recent massive attack on Solarwinds that spread to its customers and partners, reinforces the need for

new trust models such as Zero Trust and SASE

(Secure Access Service Edge) to mitigate malware's ability to spread across the network.

Nearly 2/3 of respondents plan to implement a SASE (ex. Zscaler, CATO Networks, Palo Alto Prisma, etc.) **platform within 2 years. Notably, another 1/4 of respondents have already implemented SASE.**



The top 3 factors fueling the need to adopt SASE are:

1. The replacement of legacy VPNs with Zero Trust Network Access
2. Reducing cost and complexity
3. Enabling an increasingly mobile and distributed workforce

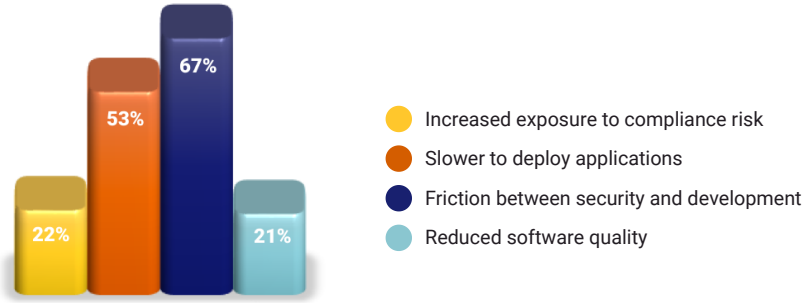
Addressing Security-Development Misalignment

Widespread lack of alignment

between network security operations and application development and delivery processes slows deployment of applications and leads to unplanned downtime.

Only 18% of organizations said their application development and delivery processes are completely aligned with network security operations.

The primary risks and dangers of this misalignment are costly delays in application deployment and friction between security and development.



Managing Accelerating Heterogeneity

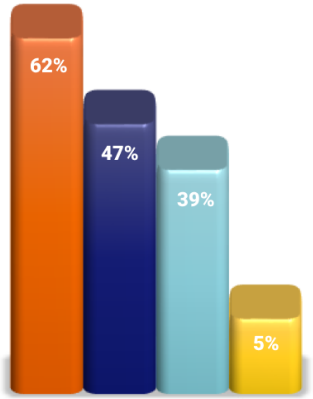
More than half of organizations place the highest of importance on

having the best technology, even if it that requires using multiple vendors

while more than 8 in 10 will use network security tools with an open API to integrate security with development, deployment and IT, and tools and processes.

Despite preferring specific types of integrations and prioritizing a lack of diversity, most organizations prefer to have the best technology available, even if that means using multiple vendors.

- Having the best technology, even if it means using multiple vendors
- Having unified technology from a single vendor
- Not sure



Only 5% of IT leaders are not concerned about network security integration with their current IT environment.

- Prefer tightly-bound, predefined integrations between vendors
- Prefer some predefined integrations with an open API to integrate security capabilities into our workflows as desired
- Prefer an API-first approach to integrate security capabilities into our workflows

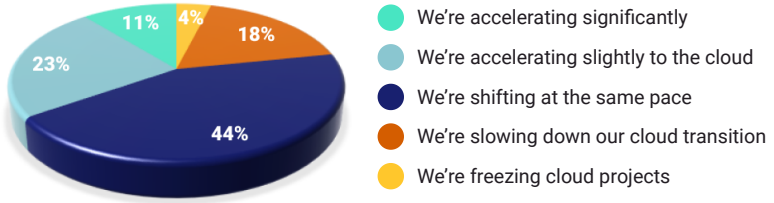
Managing Accelerating Heterogeneity

The challenges magnified by

heterogeneous environments are increasing rapidly

with the advent of COVID-19, with more than one-third of respondents saying the pandemic has accelerated their IT infrastructure transition to the cloud.

As distributed work continues, so does the cloud transition - as well as rising network security challenges.



5 Conclusion

While no one questions the challenges caused by the compounding enterprise demands for agility and speed, accelerating complexity and increasing hybrid architectures, the fact is there are a number of important areas where IT security leaders' priorities and investments are converging.

As this study shows, there is more than a little clarity for those seeking it. Zero Trust Architecture, edge-based protection, security automation, particularly for more efficient management of network security policies, plus a preference for best of breed security technology with API-based capabilities are the primary areas where network security leaders' priorities are converging.

These priorities point to the importance of managing the accelerating heterogeneity of network security environments. COVID-19 has been a catalyst, however, the change we see in network security has been long in the making. This study illustrates the importance each of these components plays while integrating them into a cohesive security strategy for today and well into the future.

91%

agree that NSPM is a strategic investment.

Tweet it

About Pulse Media

Pulse is a social research platform trusted by 27K+ verified CxOs and global IT leaders. These executives rely on the community to make connections, share knowledge, get advice, and stay on top of current trends in the technology space.

The questions, polls, and surveys posted in the platform are curated in Pulse's One-Minute White Paper reports, which reflect what IT leaders care about right now—and in the rapidly evolving world of software, real-time data and insights is what matters most.

For more information, visit pulse.qa

7 About FireMon

FireMon is the only agile network security policy platform for firewalls and cloud security groups providing the fastest way to streamline network security policy management, which is one of the biggest impediments to IT and enterprise agility.

Since creating the first-ever network security policy management solution, FireMon has delivered command and control over complex network security infrastructures for more than 1,700 customers located in nearly 70 countries around the world.

For more information, visit www.firemon.com

LEARN MORE