PULSE FIREMON

The Future of Network Security EXECUTIVE INSIGHTS

IT and security leaders face a transforming digital world. In order to meet the needs of an evolving landscape—an increasing number of security threats, increasingly hybrid architectures, the growing reliance and complexity of the cloud, and the rise of the distributed workforce—these executives must consider the best path forward to maintain security and enable agility.

Pulse and FireMon surveyed IT security executives in North America and EMEA to learn how their network security operations have changed as a result of these 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.

Data collected Nov. 25, 2021 - Jan. 21, 2021

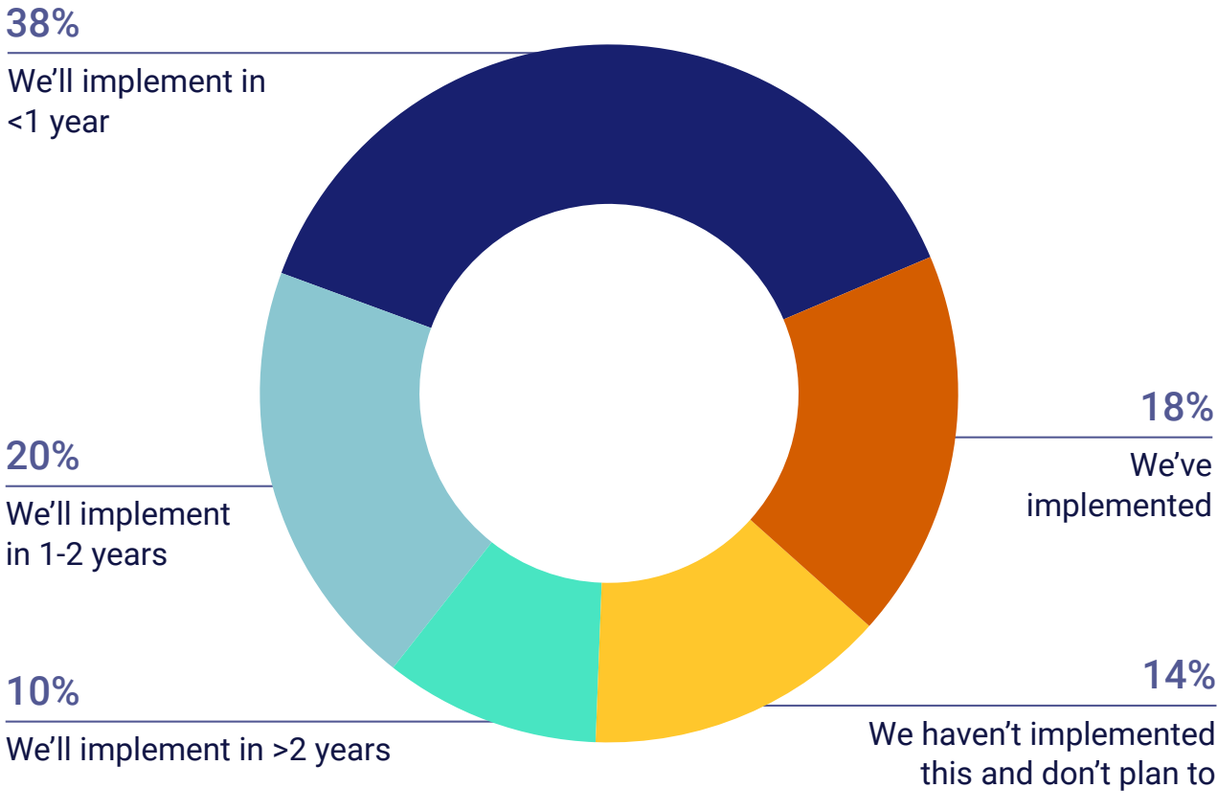
Respondents: 251 IT Security Executives, consisting of 117 C-Suite and 134 VPs in North America and EMEA

A.

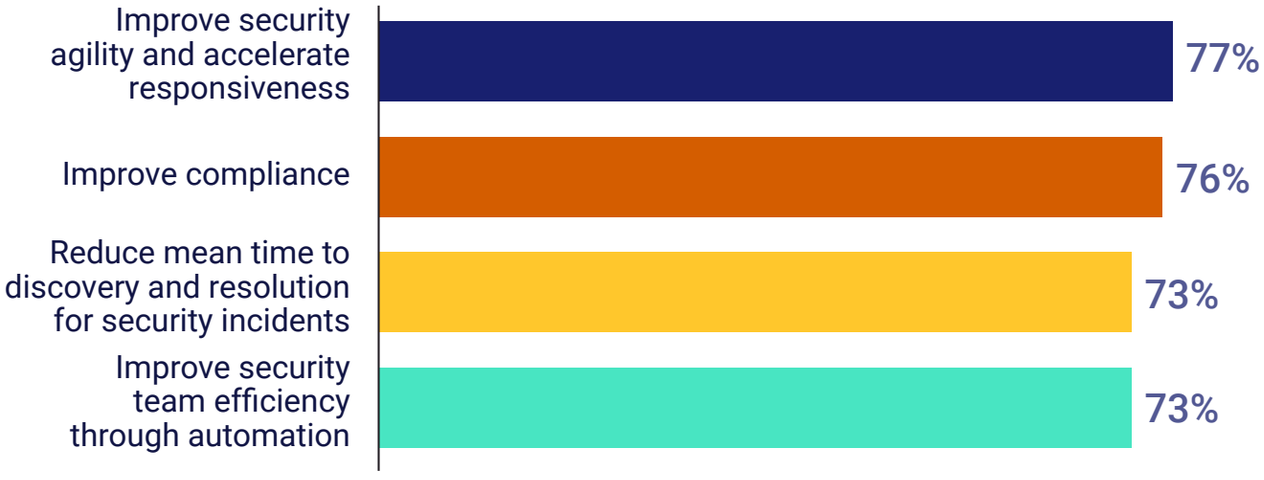
Amping Up Automation

The need for speed is driving widespread investments in security automation, with more than 6 in 10 respondents saying they'll implement security orchestration and automation within 2 years and 97% of organizations having already automated security policies to some degree.

HAS YOUR ORGANIZATION IMPLEMENTED SECURITY ORCHESTRATION AND AUTOMATION?

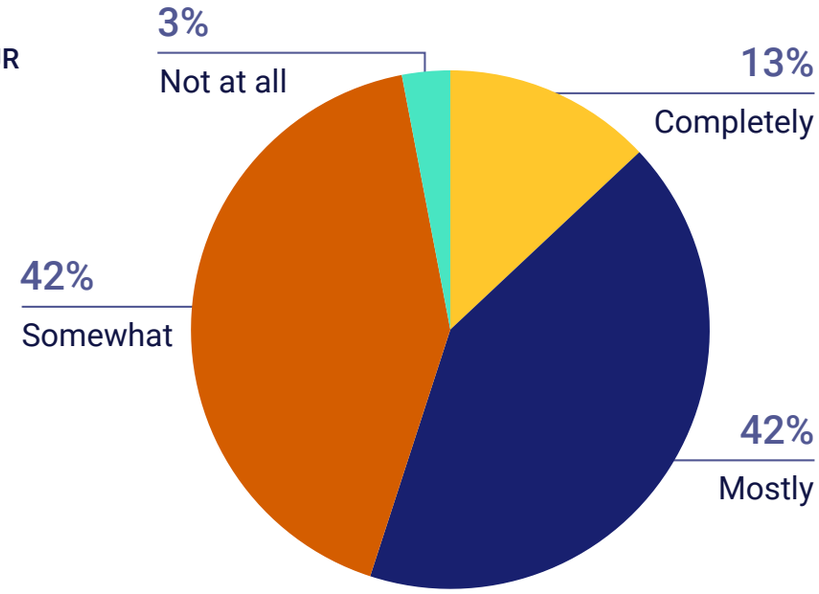


WHAT ARE THE TOP DRIVERS BEHIND YOUR ORGANIZATION'S DECISION TO IMPLEMENT SECURITY ORCHESTRATION AND AUTOMATION?

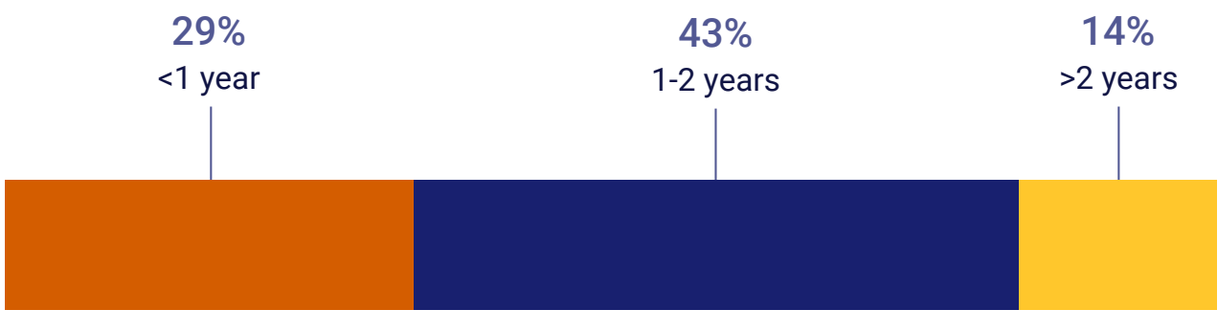


To combat rising complexity, network security policies will see an automation spike in the next 2 years.

TO WHAT EXTENT HAS YOUR ORGANIZATION AUTOMATED YOUR NETWORK SECURITY POLICIES?



IF YOUR ORGANIZATION IS PLANNING TO AUTOMATE NETWORK SECURITY POLICIES, WHAT IS THE TIMELINE TO DO SO?

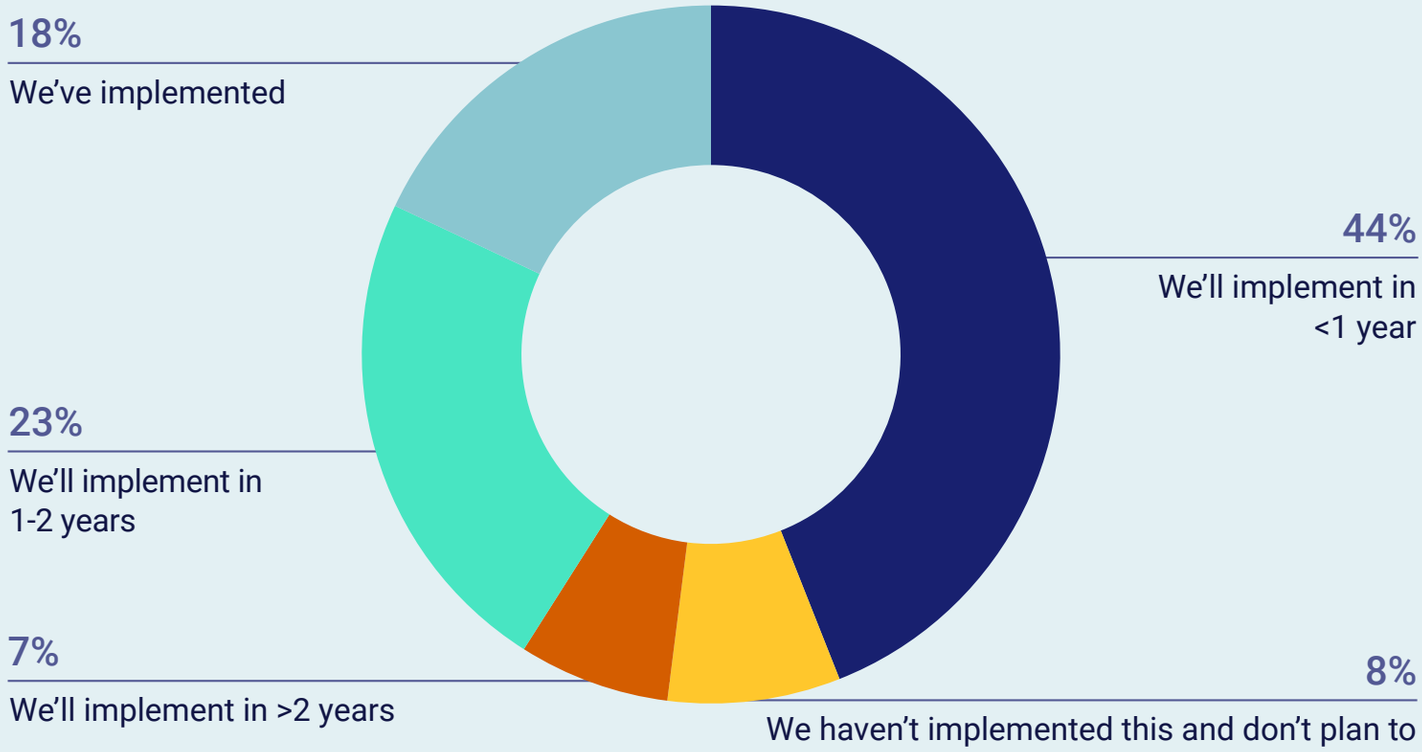


B.

Embracing Zero Trust

Fueled by a more distributed and mobile workforce and increasing reliance on cloud-based applications, 92% of respondents say their organizations have either implemented a Zero Trust architecture or plan to do so within 2 years.

HAS YOUR ORGANIZATION IMPLEMENTED A ZERO TRUST ARCHITECTURE?



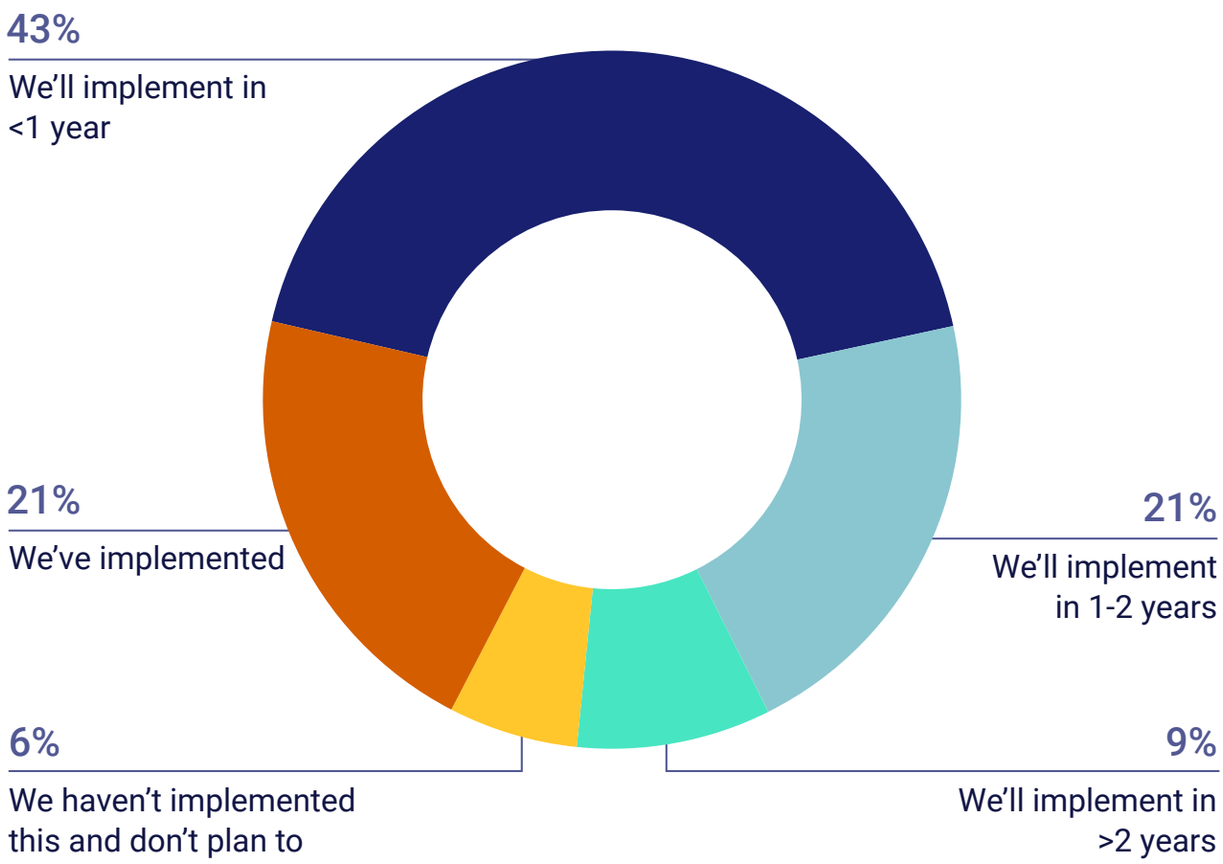
WHAT ARE THE TOP 3 DRIVERS BEHIND YOUR ORGANIZATION'S DECISION TO IMPLEMENT A ZERO TRUST ARCHITECTURE?

C.

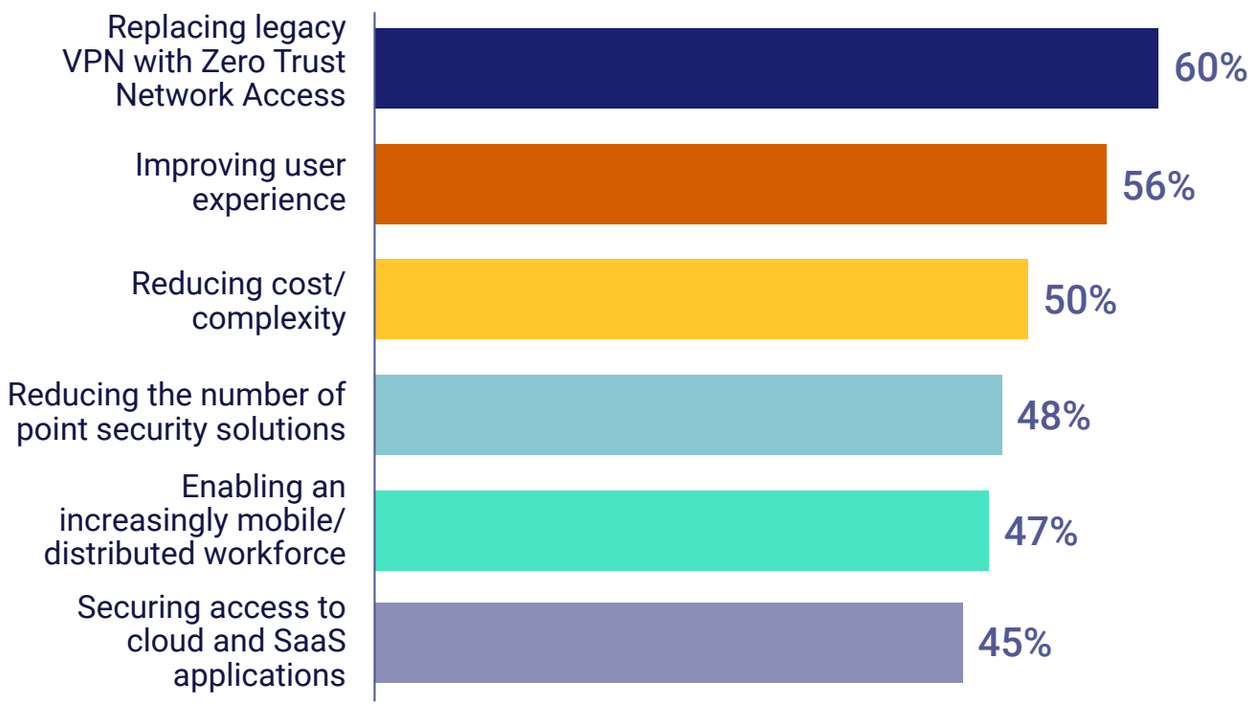
Implementing SASE

The majority of organizations have either already implemented a secure access service edge (SASE) platform or plan to do so within 2 years, driven by the need to adopt Zero Trust architecture, reduce cost and complexity and enable increasingly distributed workforces.

HAS YOUR ORGANIZATION IMPLEMENTED A SASE PLATFORM (EX. ZSCALER, CATO NETWORKS, PALO ALTO PRISMA, ETC.)?



WHAT ARE THE TOP DRIVERS BEHIND YOUR ORGANIZATION'S DECISION TO IMPLEMENT A SASE PLATFORM?

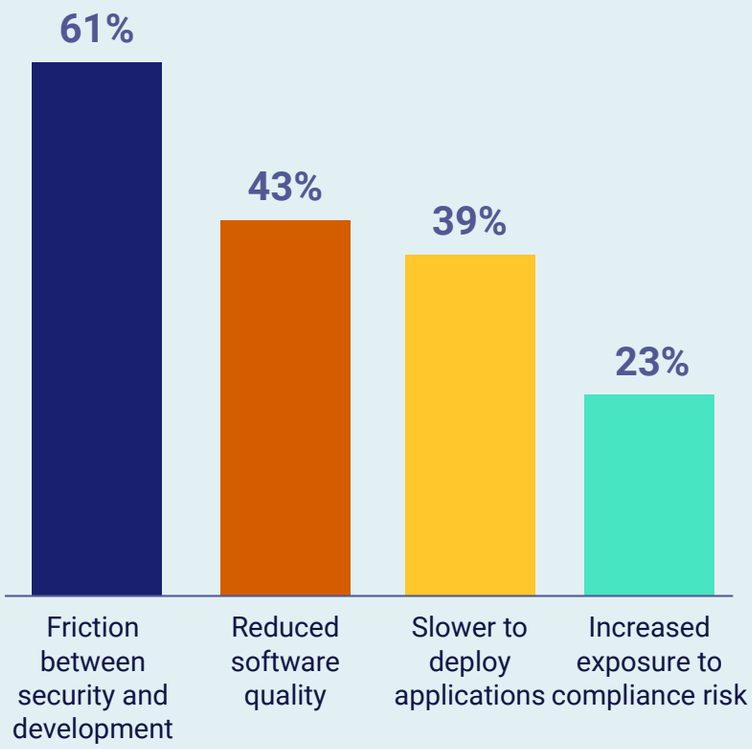


D.

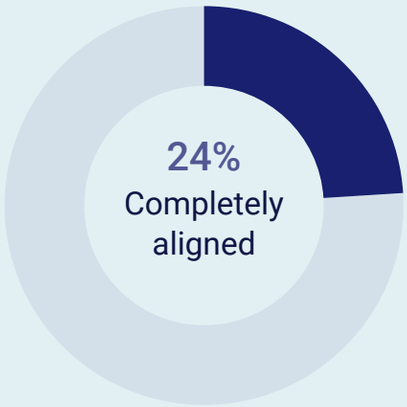
Addressing Security-Development Misalignment

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

TO THE BEST OF YOUR KNOWLEDGE, HOW DOES MISALIGNMENT BETWEEN YOUR APPLICATION DEVELOPMENT AND DELIVERY PROCESSES AND NETWORK SECURITY OPERATIONS IMPACT YOUR ORGANIZATION?

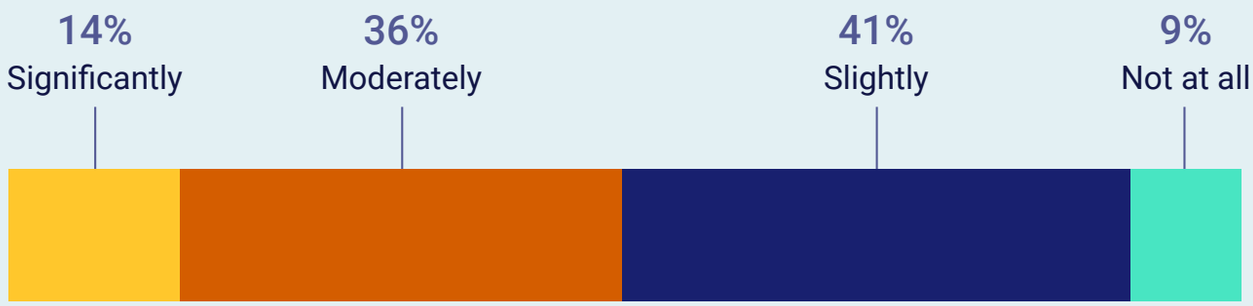


TO WHAT EXTENT ARE YOUR APPLICATION DEVELOPMENT AND DELIVERY PROCESSES ALIGNED WITH YOUR NETWORK SECURITY OPERATIONS?



OVER THE LAST NINE MONTHS, TO WHAT EXTENT HAS UNPLANNED DOWNTIME DISRUPTED ACCESS TO BUSINESS-CRITICAL OR

CUSTOMER-FACING APPLICATIONS?



E.

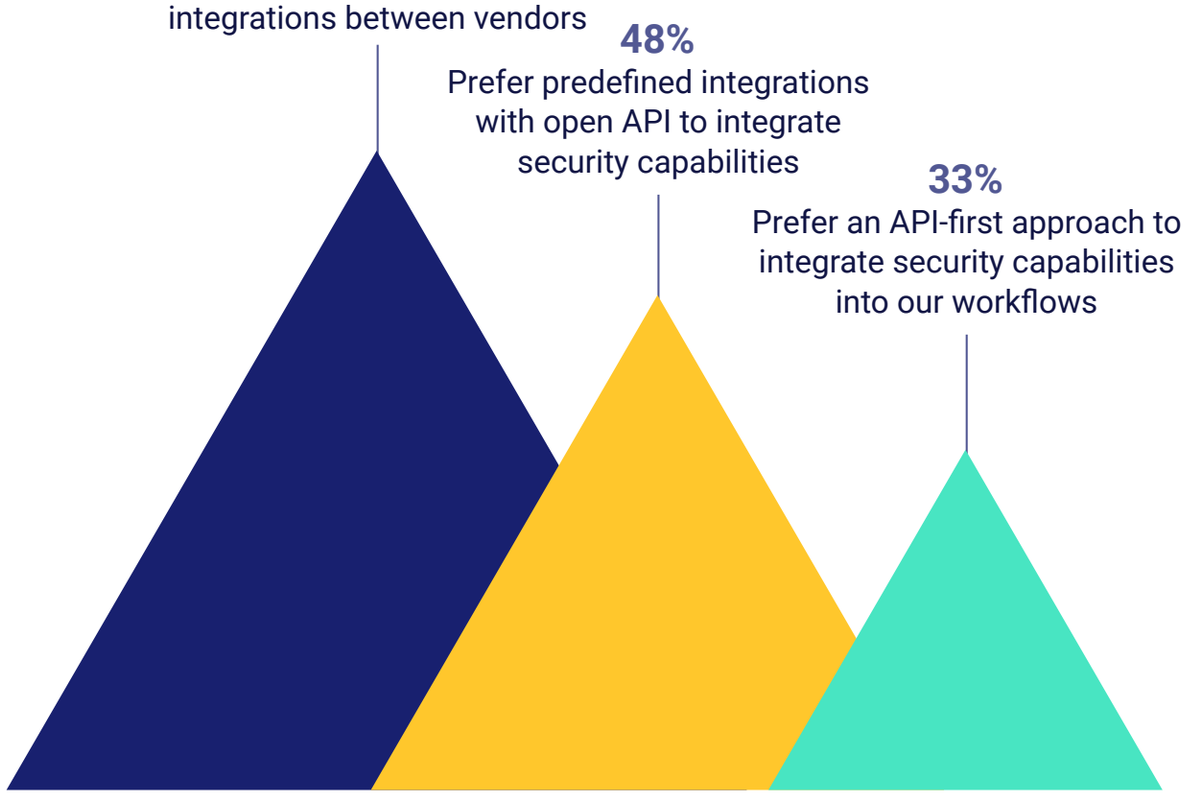
Managing Accelerating Heterogeneity

More than half of organizations place the highest importance on having the best technology, even if 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.

WHEN SELECTING A SECURITY PRODUCT, WHAT IS MOST IMPORTANT TO YOUR ORGANIZATION?

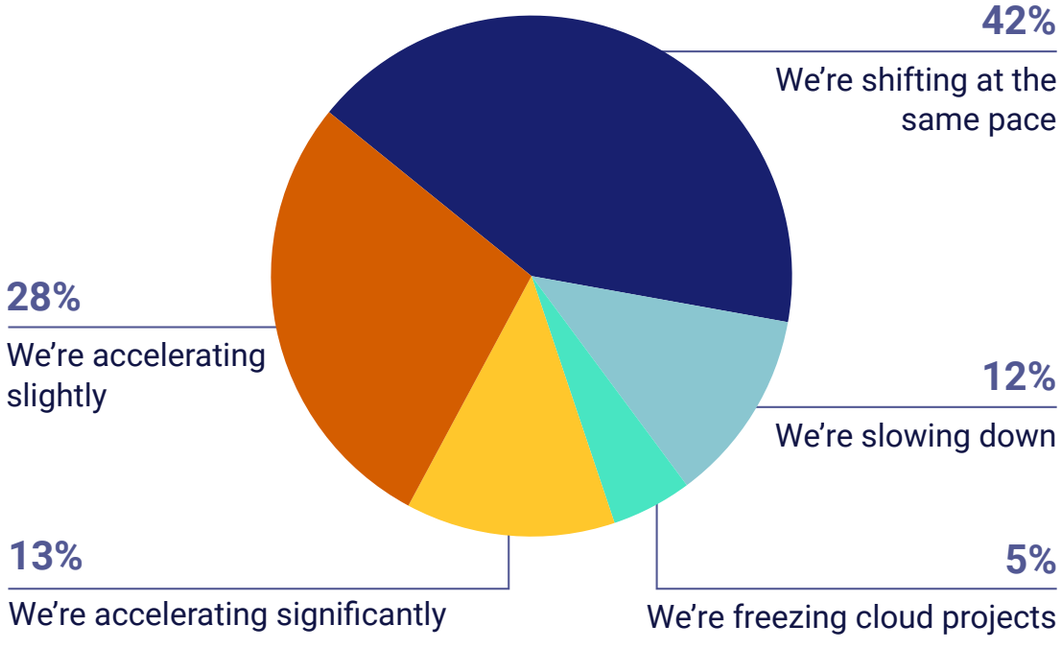
HOW WOULD YOU BEST DESCRIBE YOUR ORGANIZATION'S APPROACH TO INTEGRATING NETWORK SECURITY TOOLS IN YOUR IT ENVIRONMENT?

62%
Prefer tightly-bound, predefined



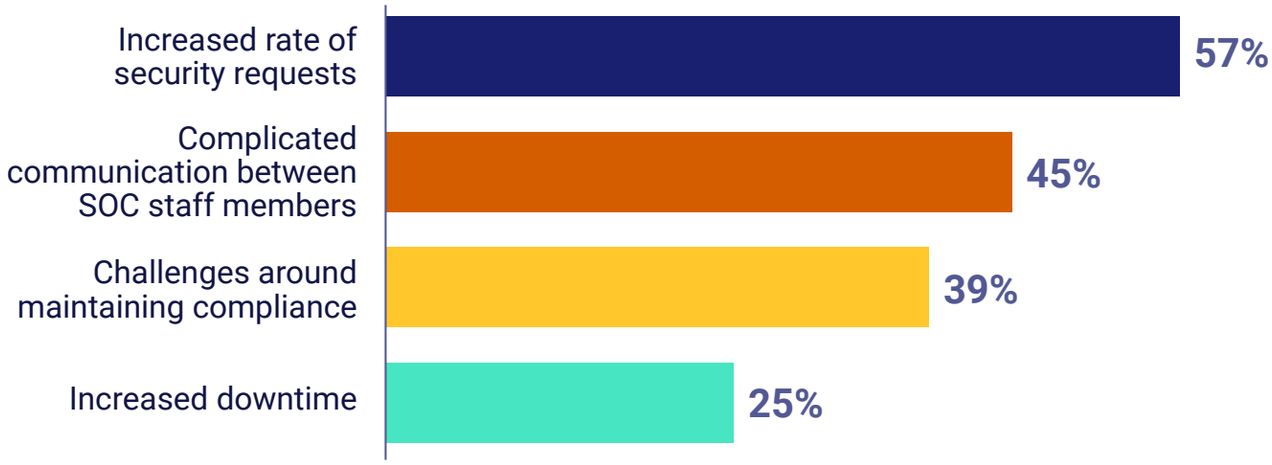
As distributed work continues, so does the cloud transition—as well as rising network security challenges

DUE TO THE COVID-19 PANDEMIC, TO WHAT EXTENT HAS YOUR COMPANY ACCELERATED ITS IT INFRASTRUCTURE TRANSITION TO THE CLOUD?



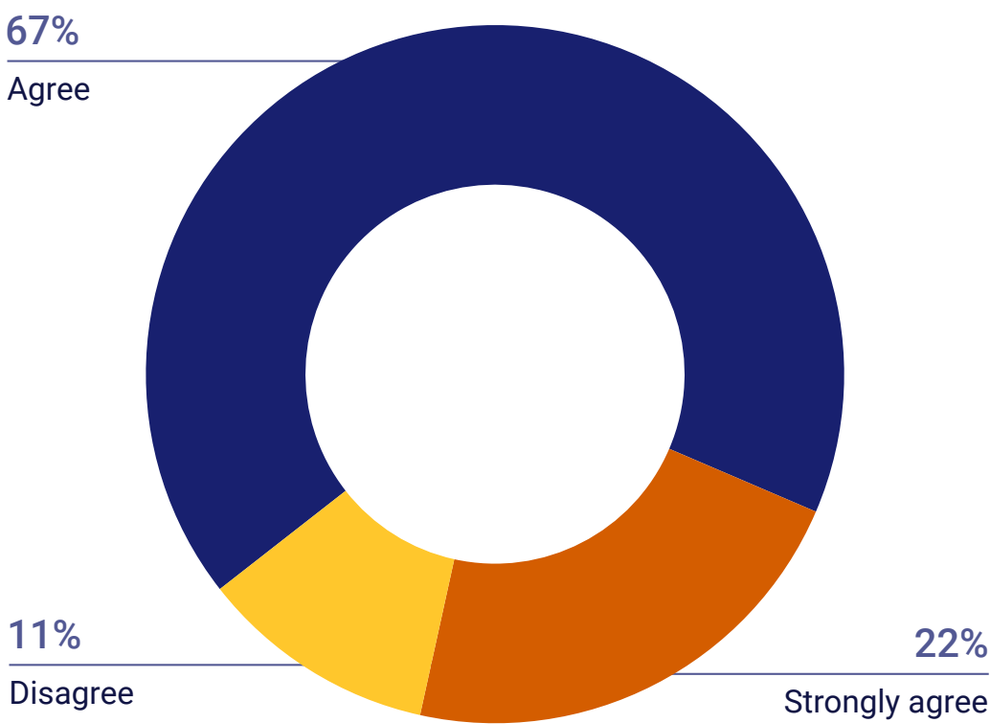
HOW HAS THE COVID-19 PANDEMIC NEGATIVELY IMPACTED

YOUR NETWORK SECURITY PROCESSES AND INITIATIVES?

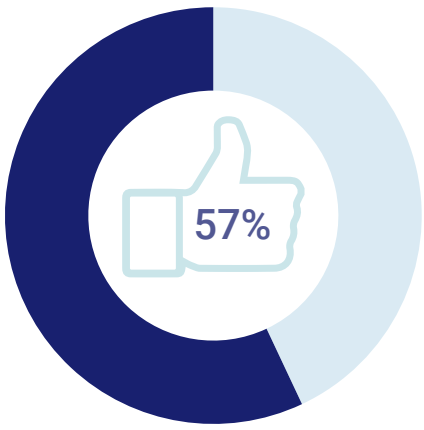


Network security policy management (NSPM) is considered by the majority of the IT security community to be a strategic investment, one that over half plan to invest in within the next year.

TO WHAT EXTENT DO YOU AGREE THAT NSPM IS A STRATEGIC INVESTMENT FOR ORGANIZATIONS WHO WANT TO MOVE FASTER AND BE MORE RESPONSIVE?



57% OF EXECUTIVE RESPONDENTS SAY THEIR ORGANIZATIONS PLAN TO INVEST IN NSPM WITHIN THE NEXT 12 MONTHS.

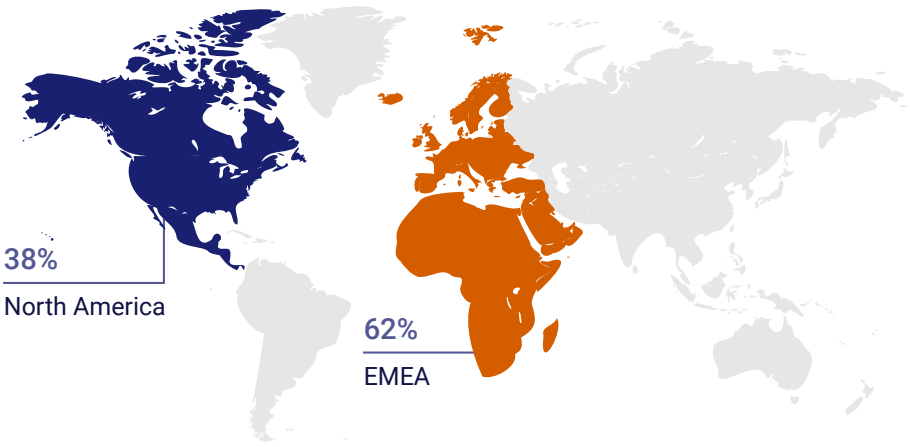


Learn how FireMon helps global enterprises protect their networks, ensure compliance, and increase security agility.

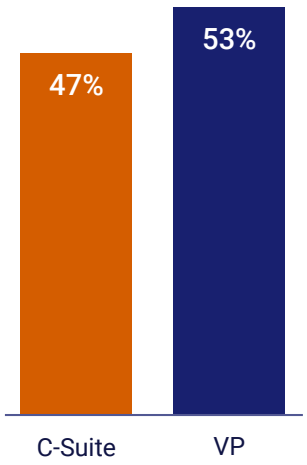
LEARN MORE

Respondent Breakdown

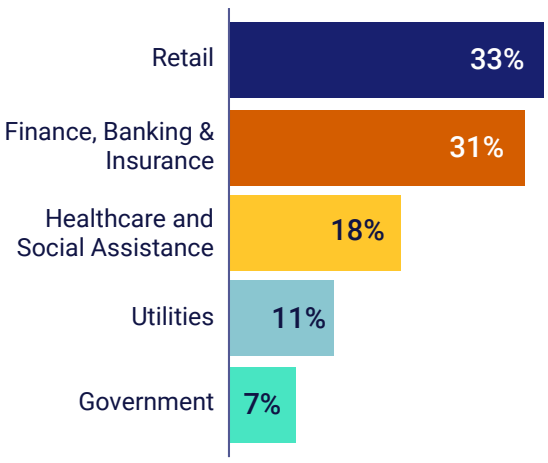
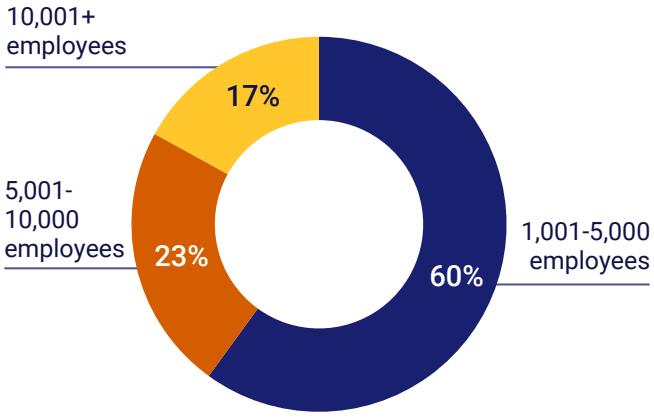
REGION



TITLE



INDUSTRY



COMPANY SIZE