PULSE FIREMON

Future of Network Security - RETAIL INSIGHTS -

With an increasing number of retail and consumer focused businesses taking steps toward digital transformation and transitioning more of their operations to the cloud, security is just as crucial to business survival as the need to transform.

Mega breaches make headlines and damage reputations, and in an era when trust and brand loyalty are critical factors of success, a single breach can strip away any benefits of transformation a retailer has managed to secure for its brand. In order to meet the needs of this evolving landscape these executives must consider the best path forward to maintain security and enable transformation.

Pulse and FireMon surveyed retail IT security leaders 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, 2020 - Jan. 21, 2021
Respondents: 139 Retail IT Security Leaders in North America and EMEA

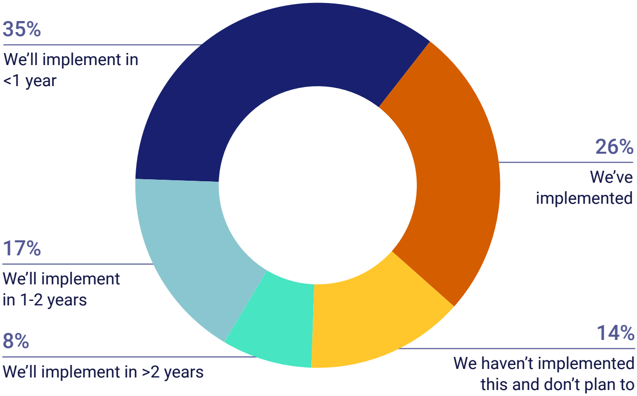
A.

Amping Up Automation

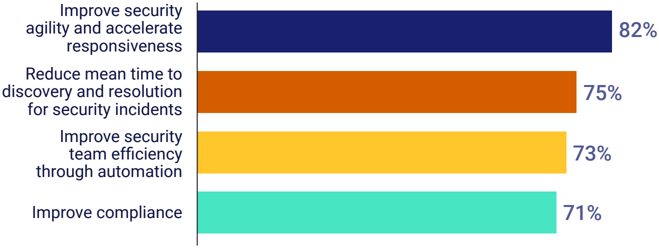
The need for speed is driving widespread investments in security

automation, with more than half of respondents (52%) saying they'll implement security orchestration and automation within 2 years and 98% of organizations having already automated security policies to some degree.

HAS YOUR ORGANIZATION IMPLEMENTED SECURITY ORCHESTRATION AND AUTOMATION?

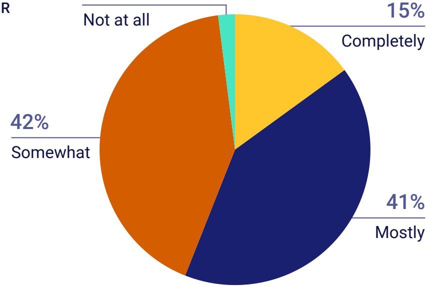


WHAT ARE THE TOP DRIVERS BEHIND YOUR ORGANIZATION'S DECISION TO IMPLEMENT SECURITY ORCHESTRATION AND AUTOMATION?



TO WHAT EXTENT HAS YOUR

ORGANIZATION AUTOMATED YOUR NETWORK SECURITY POLICIES?

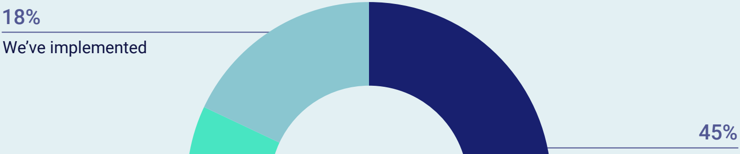


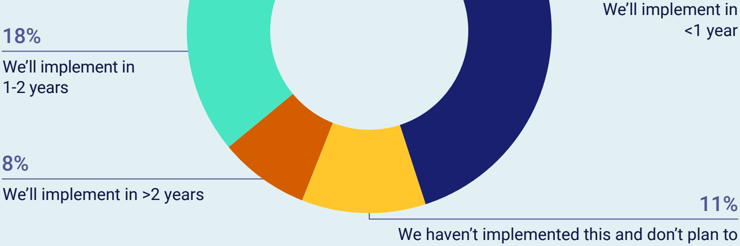
B.

Embracing Zero Trust

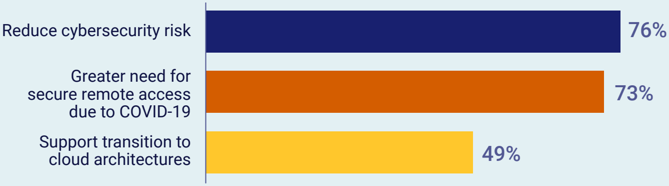
Fueled by the desire to reduce cybersecurity risks and an increasing reliance on cloud-based applications, 81% of respondents say their organizations have either implemented a Zero Trust architecture or plan to do so within 2 years.

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?

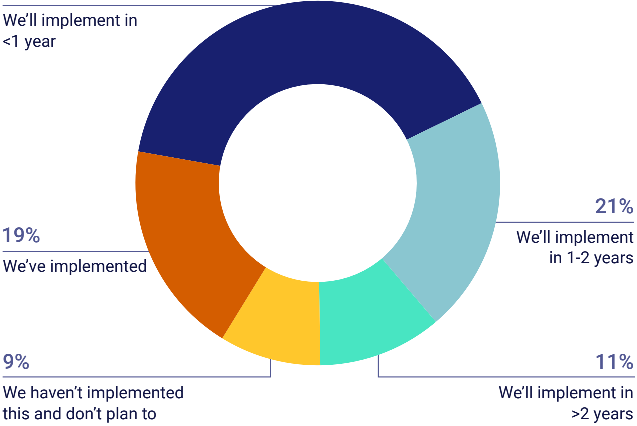


C.

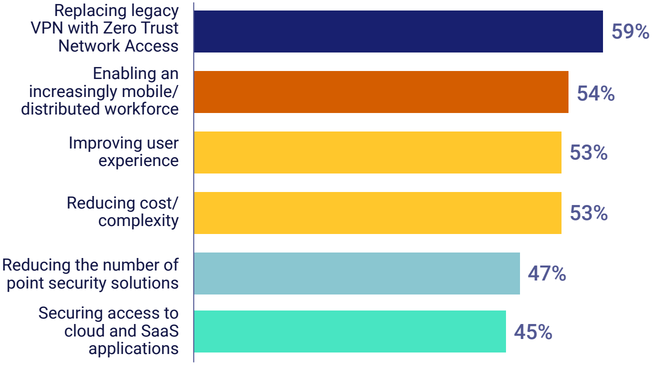
Implementing SASE

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 a predictable user experience.

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



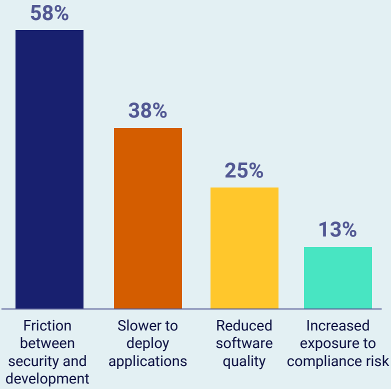
WHAT ARE THE TOP DRIVERS BEHIND YOUR ORGANIZATION'S DECISION TO IMPLEMENT A SASE PLATFORM?



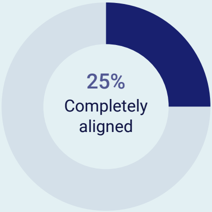
Addressing Security-Development Misalignment

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?

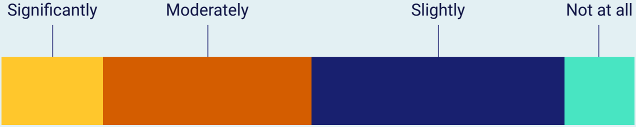


TO WHAT EXTENT ARE YOUR APPLICATION DEVELOPMENT AND DELIVERY PROCESSES ALIGNED WITH YOUR NETWORK SECURITY OPERATIONS?



OVER THE LAST 9 MONTHS, TO WHAT EXTENT HAS UNPLANNED DOWNTIME DISRUPTED ACCESS TO BUSINESS-CRITICAL OR CUSTOMER-FACING APPLICATIONS?

16% 33% 40% 11%

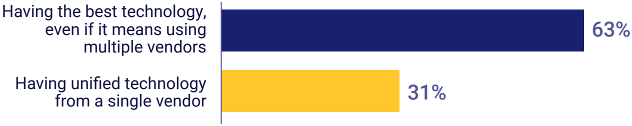


E.

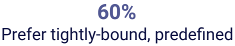
Managing Accelerating Heterogeneity

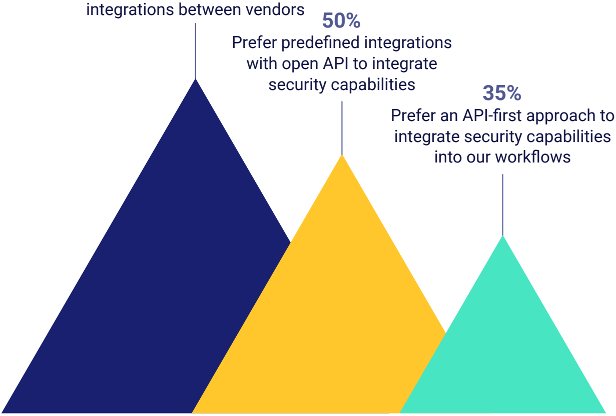
More than half of organizations place the highest importance on having the best technology, even if that requires using multiple vendors. Additionally, more than 8 in 10 will use network security tools with an open API to integrate security with development, deployment and IT, and tools and processes.

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



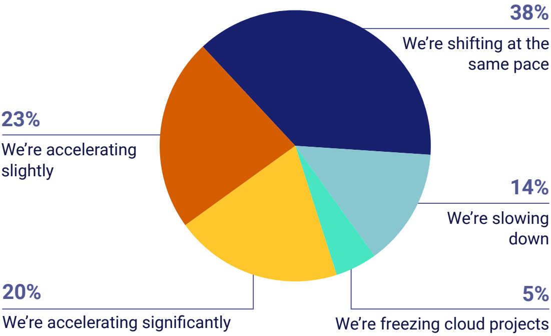
HOW WOULD YOU BEST DESCRIBE YOUR ORGANIZATION'S APPROACH TO INTEGRATING NETWORK SECURITY TOOLS IN YOUR IT ENVIRONMENT?



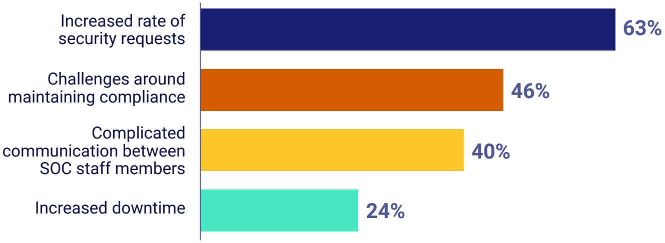


The pandemic has shifted market dynamics and consumer behavior, forcing many in the retail industry to ramp up their transition to the cloud—and face rising network security challenges.

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

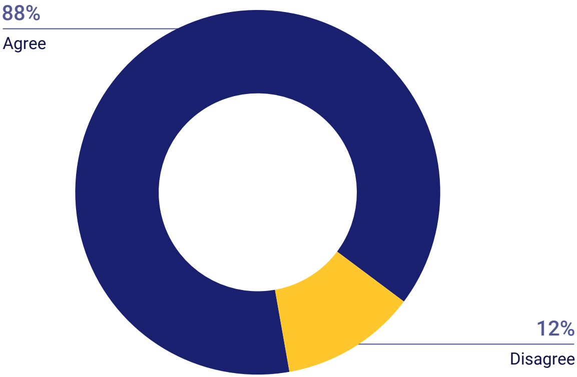


HOW HAS THE COVID-19 PANDEMIC NEGATIVELY IMPACTED YOUR NETWORK SECURITY PROCESSES AND INITIATIVES?

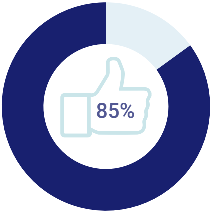


Network security policy management (NSPM) is considered by the majority of Retail's IT security community to be a strategic investment, one that over three quarters plan to invest in within the next year.

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



85% OF EXECUTIVE RESPONDENTS SAY THEIR ORGANIZATIONS PLAN TO INVEST IN NSPM WITHIN THE NEXT 12 MONTHS.

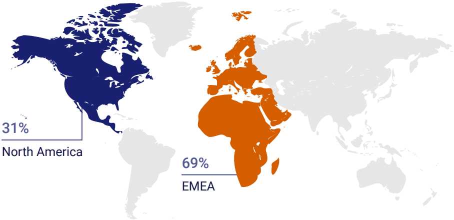


Learn how FireMon helps global enterprises protect their networks, ensure compliance, and increase security agility.

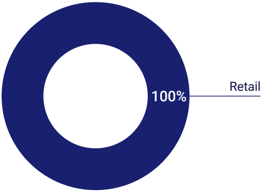
LEARN MORE

Respondent Breakdown

REGION

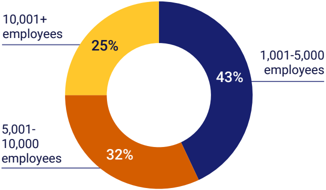


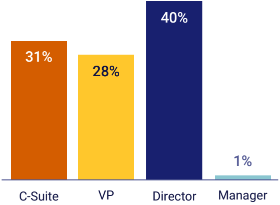
INDUSTRY



COMPANY SIZE

TITLE





Insights powered by PULSE