Top Networking and Security Challenges in the Enterprise

Planned Network Investments in 2017

Global Industry Report

November 2016

CATO

NETWORK + SECURITY
IS SIMPLE AGAIN

Contents

Survey Highlights

In the latest research initiative lead by the Cato Networks team, **Top Networking and Security Challenges In the Enterprise; Planned Network Investments in 2017**, over 700 networking, security and IT executives and professionals from around the globe, shared their biggest risks, challenges and planned investments related to network connectivity and security. This report examines the key findings and takeaways their feedback reveals.

Mobile and Cloud are Transforming Enterprise Networking and Security

Increasing workforce mobility and demand for real-time access to cloud applications and infrastructure across devices are redefining the network and security rules for the enterprise.

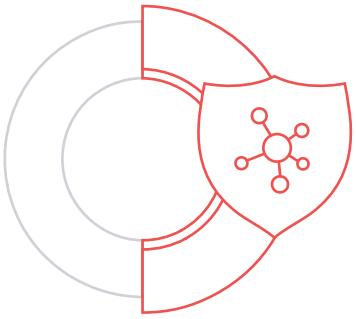
The networking and security architectures of the past were designed for well-defined, static, and location-bound businesses. Today, there is a growing chasm between these legacy technologies and the dynamic, cloud-centric and mobile-first businesses.

Identifying risks

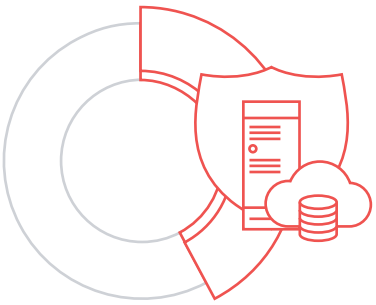
Gartner Research projects IT spending on public cloud-based infrastructure services to surpass US $24 billion in 2016, with associated management and security expected to exceed US $8 billion. Private cloud infrastructures, including server and network virtualization and software-defined networking (SDN), are transforming on-premises data centers into agile software-defined data centers (SDDC).

Yet, as the move towards the cloud continues with the goal of enabling real-time access to cloud applications for mobile workers, it poses new networking and security challenges for IT leaders.

50% identify network security as their top security risk, 38% identify integrating and securing cloud and physical datacenters as a top three network security risk.

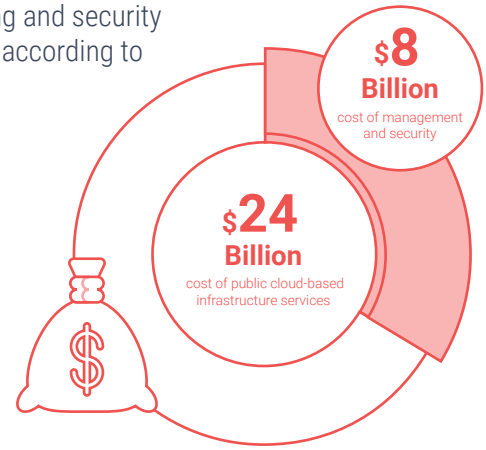


50%
of IT leaders identify **network security as their top security risk**



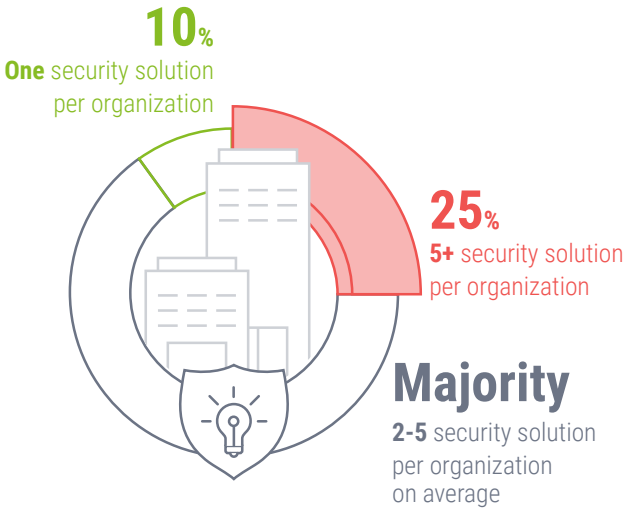
38%
of IT leaders identify **integrating and securing cloud and physical datacenters among their top three network security risks**

The cost of networking and security architectures in 2016 according to Gartner



Point Products and Skills Shortages Impact Security Posture

The difficulty in handling emerging threats and the need to enhance organizational defenses highlights the weakness in the underpinning legacy architectures built upon point products and dependent on hard-to-find skills.



Number of implemented security solutions

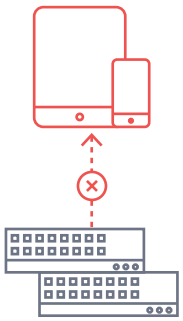
A majority of organizations are quoting between two and five solutions on average, while 25% report having over five solutions in place. Those respondents from organizations with more than 1,000 employees report a higher prevalence of multiple security solutions, with 39% managing five or more.

IT skills shortage

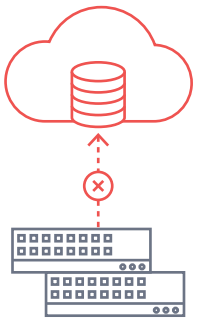
The IT skills shortage, recognized by Gartner in their 2016 CIO Agenda report as the single biggest issue preventing CIOs from achieving their objectives, is crippling IT leadership, cited as the third biggest security risk faced by organizations.

The dissolving perimeter

The prevailing appliance-based security is not only expensive to own but it is also incompatible with the cloud and mobility demands. Although the network security appliance economy has worked well for legacy appliance vendors (providing a recurring and dependable revenue stream through continuous upgrades and refreshes of dated and capacity-constrained equipment), it is taking its toll on businesses with 49% citing the capital and operational expenses associated with appliances as their biggest network security challenge. Appliances also do not extend well to cover mobility (48%) and cloud (35%) as these enterprise resources don't neatly fit into a defined perimeter.



For **48%** of organizations appliances do not extend well to cover mobility



For **35%** of organizations appliances do not extend well to cover cloud

Legacy Architectures Misaligned with Business Needs and Emerging Threats

Current networking and security architectures are crippling business' ability to defend against emerging threats as well as achieve cost-effective and secure connectivity.

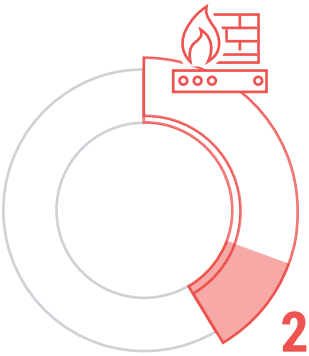
Top concern: Defending against ransomware and complexity of managing distributed appliances

Networking and security professionals are most worried about their ability to defend against emerging threats such as ransomware. More than 50% of IT professionals see defending against emerging threats such as ransomware as the number one priority over the next 12 months, across both networking and security.

50+% of IT professionals see defending against emerging threats such as ransomware as the number one priority

Current security practices require complex topology and expensive connectivity

42% of IT professionals state that they are using branch firewalls at every office to protect internet access, with 25% backhauling traffic to a datacenter. Both of these options represent tough trade-offs between increased complexity of managing distributed appliances, and wasteful use of expensive WAN resources (MPLS).



42% of IT professionals state that they are using branch firewalls at every office to protect internet access

25% backhauling traffic to a datacenter

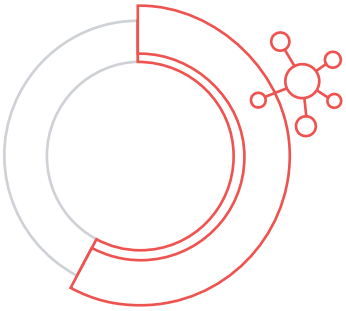
48% of organizations force their mobile users to connect using VPN

Challenges to securing mobile access

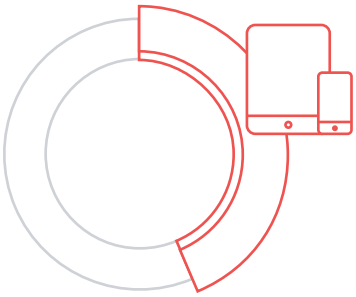
For mobile users, 48% of organizations force their mobile users to connect using VPN to an appliance in a specific location in order to gain access to public cloud applications. This is a very inefficient method that often results in poor user experience.

Mobile Risks Are a Blind Spot for Many Enterprises

Although network and mobile security are tied as the top two security risks (58% and 44% respectively), and despite the realization that close to 50% cannot fully enforce corporate security policies on mobile users (48%), most organizations do not have comprehensive threat protection in place.

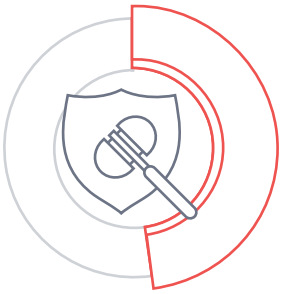


58%
of IT professionals see **Network Security** as their top security risks



44%
of IT professionals see **Mobile Security** as their top security risks

Most organizations are challenged by three aspects of keeping their company, IP and users productive and safe:



48%
Enforcing corporate security policy on mobile users

49%
Cost of buying and managing security appliances and software

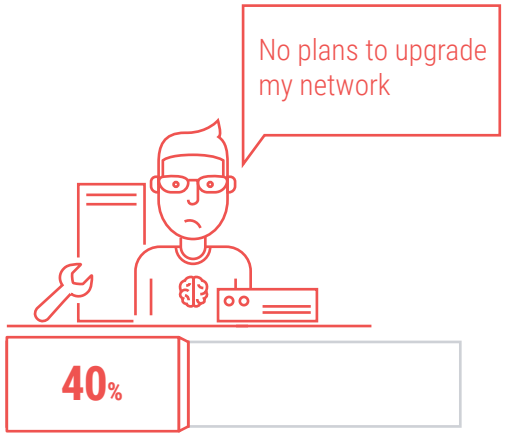
35%
Integrating and securing cloud and physical data centers

Cost of Complexity of Network and Security Impact Investments

Complexity and cost of managing hybrid (on-premises and cloud/mobile) network connectivity and security result in either paralysis or sub-optimal investments.

Complexity stifling progress

Complexity is pushing 40% to do nothing, with no plans to upgrade their network, likely due to lack of ROI on existing approaches claiming to solve for the cost and complexity conundrum.



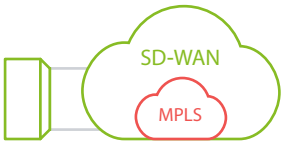
No Holistic Architectural Approach

The wide range of challenges for network and security teams leads to the continued deployment of point solutions to address point problems that further drive cost and complexity. As opposed to embracing a holistic approach, most are addressing fragments of the cost and complexity challenge through incremental fixes, which in turn lead to more complexity and IT skill shortage, such as:

20%
Direct internet access for branch offices

18%
Reduce branch appliance footprint
(FWs, UTMs, etc.)

15%
Migrate from MPLS to internet last-mile connectivity



15%
SD-WAN to augment MPLS

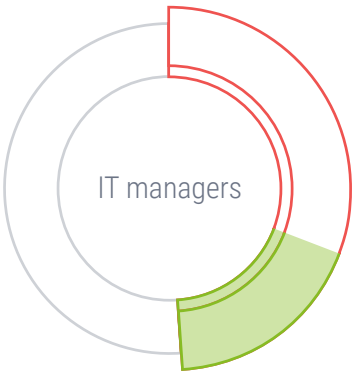
IT professionals clearly recognize the shortfalls of existing networking and security architectures - from the cost of buying and managing appliances and using high latency public internet connectivity to save costs, to deploying multiple point solutions and the struggle to find the people to run them. However, with a “this is how things are done” mentality, and even more point solutions to address specific parts of the problem, the pace of transformation is slow.

Distributed and Fragmented Point Solutions Impose Substantial Load on IT

Managing multiple security solutions can waste valuable IT resources as too much time is spent managing the "as-is state."

Cost of current practices

Despite many IT managers' realization that they are paying a premium to buy and manage security appliances and software (49%), only 18% are planning to reduce branch appliance footprint of Firewalls (FWs) and Unified Threat Management (UTM) systems.



49% of IT managers' realize that they are paying a premium to buy and manage security appliances and software

18% are planning to reduce branch appliance footprint of FWs and UTMs

Considering new WAN solutions

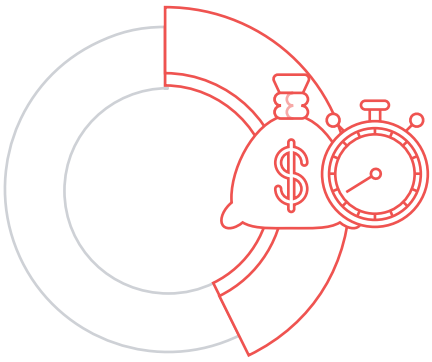
Those looking to managed WAN solutions – a quarter of the respondents – will alleviate their IT skills shortage but will not see a reduction in cost; they will simply transfer cost from Capex to Opex.

Adoption of transformational network strategies takes time to evolve and mature. The higher the aggregate potential return, the faster the transformation. It is likely that many point approaches do not offer a compelling value on a standalone basis to get customers to take actions en masse.

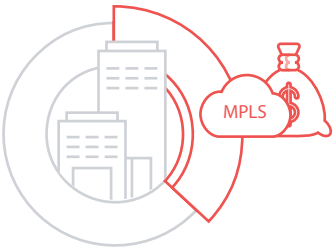
25% of IT managers are looking to managed WAN solutions

Existing Approaches to Transforming Offer Limited Fix

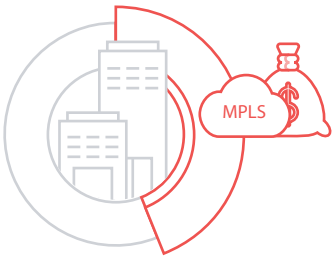
High quality and affordable WAN connectivity is hard to find; partial fixes provide limited return, leading to paralysis:



43% of responders cite high latency in remote locations and cost of managing appliances as their biggest WAN challenges



37% of organizations **with less than 1000 employees** cite MPLS cost as their biggest challenge

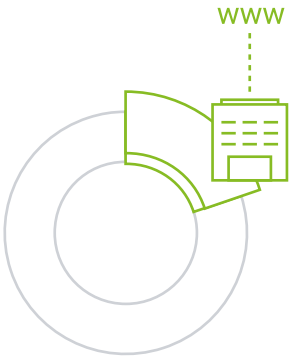


44% of organizations **with more than 1000 employees** cite MPLS cost as their biggest challenge

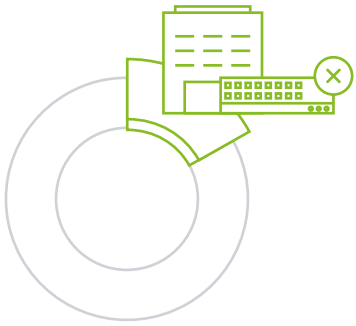
This is an indication that securely connecting the business is a tough trade-off between cost, complexity and performance. Many organizations don't see a resolution to this trade-off as evidenced by 40% planning no changes to their network.

Some are taking a targeted approach to address parts of the problem.

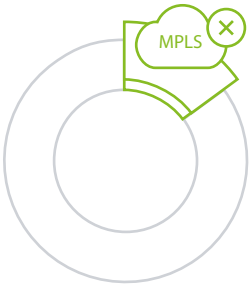
26% of IT managers consider managed WAN connectivity solutions to augment their skills



20% will deploy direct internet access to eliminate MPLS capacity waste



18% will reduce branch office appliance footprint to address cost and management complexity



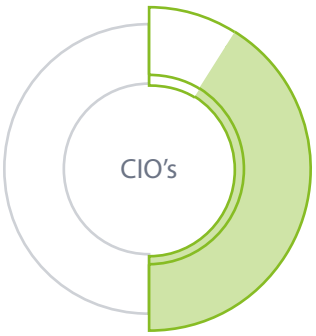
15% will eliminate or augment MPLS with Internet links that can provide affordable and reliable WAN connectivity for specific cloud traffic

Converged Cloud-Based Network and Security Will Cut Costs/ Complexity, Improve Security

The industry is bound to embrace simplification, convergence and a holistic approach to making security more agile and dynamic in 2017.

Appliance elimination

39% on average, and over 50% of CIOs, plan to eliminate hardware appliances in the coming year, while 41% see Firewall as a Service (FWaaS) as the most promising infrastructure protection technology.



50+% of CIOs, plan to eliminate hardware appliances in 2017,

41% see **Firewall as a Service** (FWaaS) as the most promising infrastructure protection technology

Using the cloud to continuously transform IT

Amazon AWS alleviated the server and storage lifecycle management complexity and overhead, enabling 62% of IT professionals to plan the elimination of server hardware and 52% to eliminate storage hardware in 2017.

62%
of IT professionals to plan to eliminate server hardware in 2017

52%
of IT professionals to plan to eliminate storage hardware in 2017

The cloud will be the platform to re-architect networking and security in a way that eliminates the cost, complexity and architectural challenges associated with appliance-based networking and security.

Detailed Survey Results

Q1

What type of WAN connectivity does your organization use?
(Check all that apply)

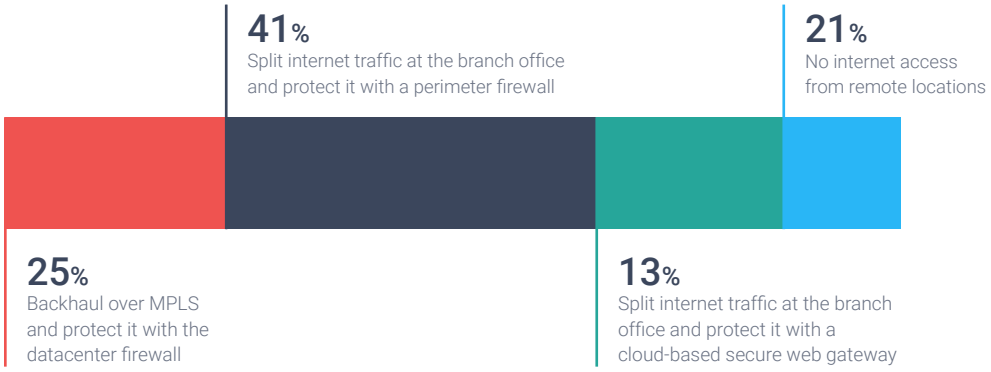
72%
VPN tunnels over the internet

38%
MPLS

31%
SD-WAN
(MPLS and internet)

Q2

How does your organization secure internet access from remote locations?



41%
Split internet traffic at the branch office and protect it with a perimeter firewall

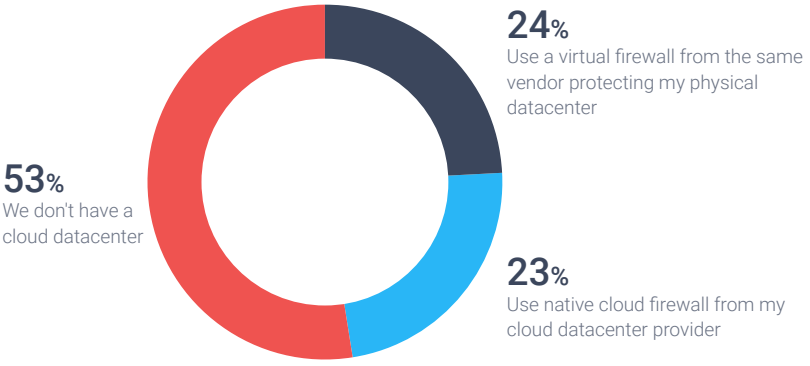
21%
No internet access from remote locations

25%
Backhaul over MPLS and protect it with the datacenter firewall

13%
Split internet traffic at the branch office and protect it with a cloud-based secure web gateway

Q3

How do you protect your cloud datacenter?



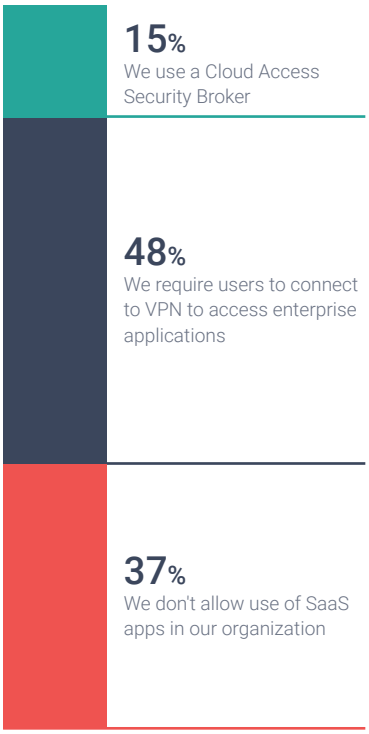
24%
Use a virtual firewall from the same vendor protecting my physical datacenter

53%
We don't have a cloud datacenter

23%
Use native cloud firewall from my cloud datacenter provider

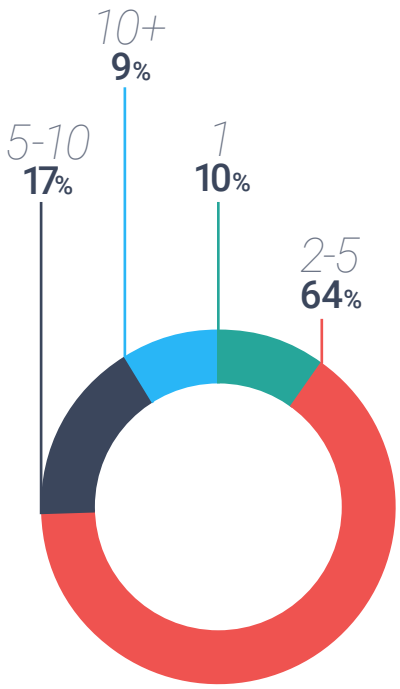
Q4

How do you secure Public Cloud (SaaS) access by mobile users?



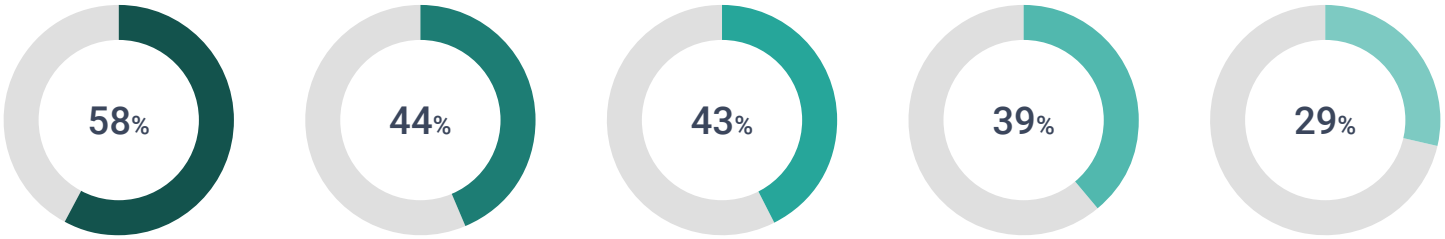
Q5

How many different security solutions do you use across your physical, cloud and mobile environments?



Q6

Relative to your existing capabilities, which of the following areas represent the biggest risk for your organization?
(check all that apply)



Q7

What are your biggest challenges when it comes to WAN?

(check all that apply)

43%
Latency in remote locations

43%
Cost of buying and managing appliances

37%
Cost of MPLS

35%
Mobile VPN access to the network

19%
Onboarding new locations

Q8

What is your biggest challenge when it comes to network security?

(check all that apply)

49%
Cost of buying and managing security appliances and software

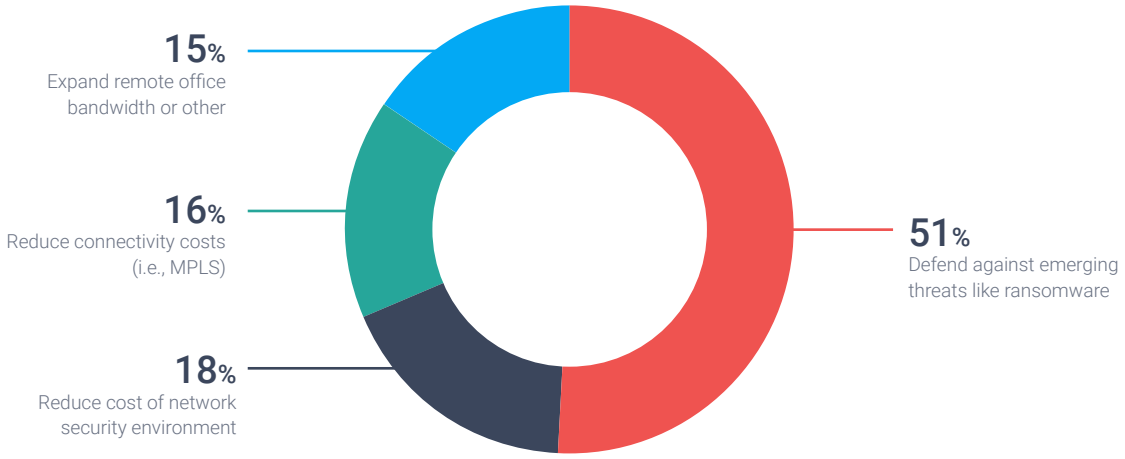
48%
Enforcing corporate security policy on mobile users

35%
Integrating and securing cloud and physical datacenters

32%
Providing secure direct internet access for branch locations

Q9

Over the next 12 months, what is your highest networking and security priority?



Q10

How do you plan to upgrade your network over the next 12 months?
(check all that apply)

15% Migrate from MPLS to internet last-mile connectivity

15% SD-WAN to augment MPLS

20% Direct internet access for branch offices

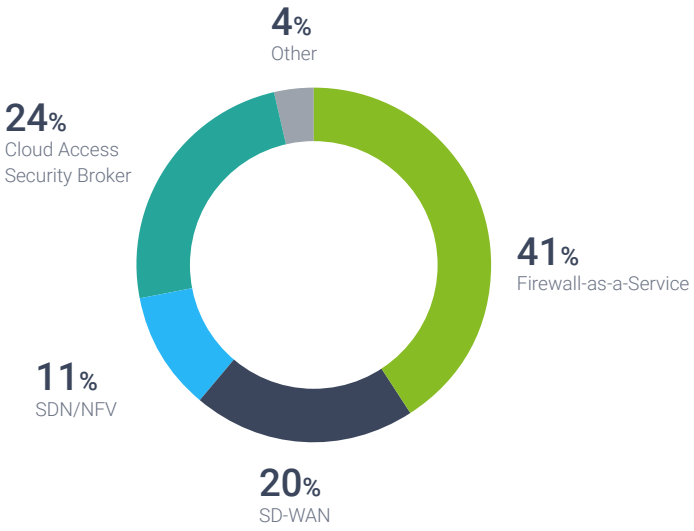
26% Managed global WAN connectivity solution

18% Reduce branch appliance footprint (FWs, UTMs, etc.)

40% I do not plan to upgrade my network over the next 12 months

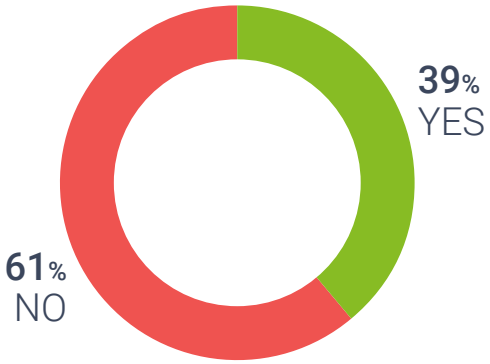
Q11

What do you see as the most promising emerging technology for infrastructure protection?



Q12

Do you plan to eliminate any on-premise hardware over the next 12 months?



Q13

What type of on-premise hardware do you expect to eliminate over the next 12 months?
(check all that apply)

34% Security

36% Networking

52% Data storage

62% Servers

Q14

What is your role?

- **10%** CIO/VP IT
- **22%** IT Director
- **10%** Network Architect
- **15%** Network Analyst
- **21%** Security Architect/Analyst
- **22%** Other

Q15

What is the size of your company?

- **32%** 1-99 employees
- **31%** 100-999 employees
- **13%** 1,000-2,499 employees
- **11%** 2,500-10,000 employees
- **13%** 10,000+ employees

Q16

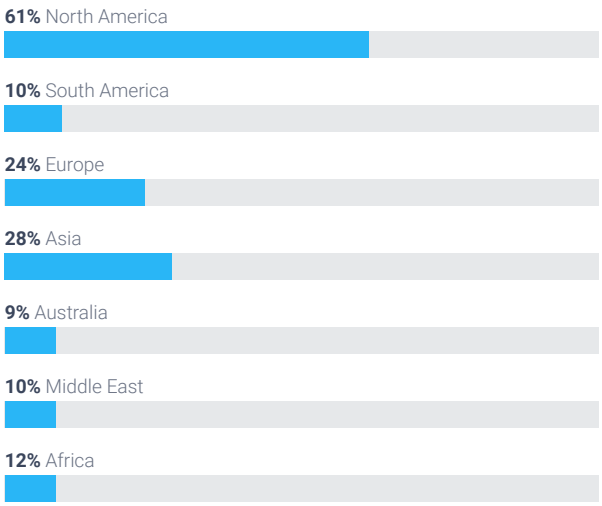
What industry does your company belong to?

- **7%** 1-99 employees
- **6%** 100-999 employees
- **13%** 1,000-2,499 employees
- **11%** 2,500-10,000 employees
- **13%** 10,000+ employees
- **32%** 1-99 employees
- **31%** 100-999 employees
- **13%** 1,000-2,499 employees
- **11%** 2,500-10,000 employees
- **13%** 10,000+ employees
- **13%** 10,000+ employees
- **13%** 10,000+ employees

Q17

Where is your company located?

(check all that apply)



- **61%** North America
- **10%** South America
- **24%** Europe
- **28%** Asia
- **9%** Australia
- **10%** Middle East
- **12%** Africa

About Cato

Cato Networks provides organizations with a software-defined and cloud-based secure enterprise network. Cato delivers an integrated networking and security platform that securely connects all enterprise locations, people and data.

The Cato Cloud reduces MPLS connectivity costs, eliminates branch appliances, provides direct, secure internet access everywhere, and seamlessly integrates mobile users and cloud infrastructures to the enterprise network.

Based in Tel Aviv, Israel, Cato Networks was founded in 2015 by cybersecurity luminary Shlomo Kramer, who previously cofounded Check Point Software Technologies and Imperva, and Gur Shatz, who previously cofounded Incapsula.

Network+Security is Simple Again

For more information:

www.CatoNetworks.com

@CatoNetworks