Netop – VPN Survey

Deployed to Spiceworks Voice of IT panel
in February 2014; 192 respondents in the United States

Executive Summary

IN THIS REPORT

In February 2014, Spiceworks Voice of IT surveyed 192 IT pros in the US to learn how they manage VPN and the challenges experienced with their current solution. To qualify for the survey, they must be the person responsible for managing or supporting their organization's VPN solution.

Key findings of this report include:

- Roughly three-quarters of respondents have set up a VPN in the past year.
- The majority state their organization uses a firewall based service for their VPN solution, while 26% use a server based service. Further, most employ Internet Protocol Security (IPsec) (68%) and / or Transport Layer Security (SSL/TLS) (52%) for a VPN security protocol.
- Respondents are evenly split on whether they allow their vendors and / or trusted third parties VPN access to their organization's network. Nearly two-thirds of the respondents who allow VPN access state their vendors can access department-specific business applications (i.e. database software, accounting software).
- Three-quarters believe their VPN solution is very to extremely effective at providing employees remote access to their organization's intranet. Respondents also feel it's very to extremely effective at connecting multiple locations (63%) and pulling data for reports (47%).
- When asked about the greatest limitations of VPNs, nearly half state that the difficulty for employees to connect remotely is the greatest limitation. Other limitations are reliability of connection (35%), degree of expertise needed to configure (27%) and logging use (26%).
- When asked how interested they would be in a product that replicates the functions of a VPN (but is easier to use and maintain), 47% indicate they're somewhat interested, and 14% are very to extremely interested.

The following pages provide detailed findings for all questions in the study.
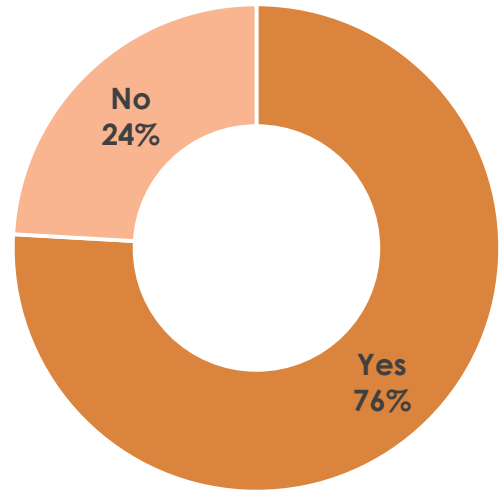

Configuring a New VPN

To qualify for the survey, respondents must be the person responsible for managing or supporting their organization's VPN solution.

Of those who qualified, roughly three-quarters (76%) state they've set up a VPN in the past year. However, 24% state they haven't set one up in the past year.
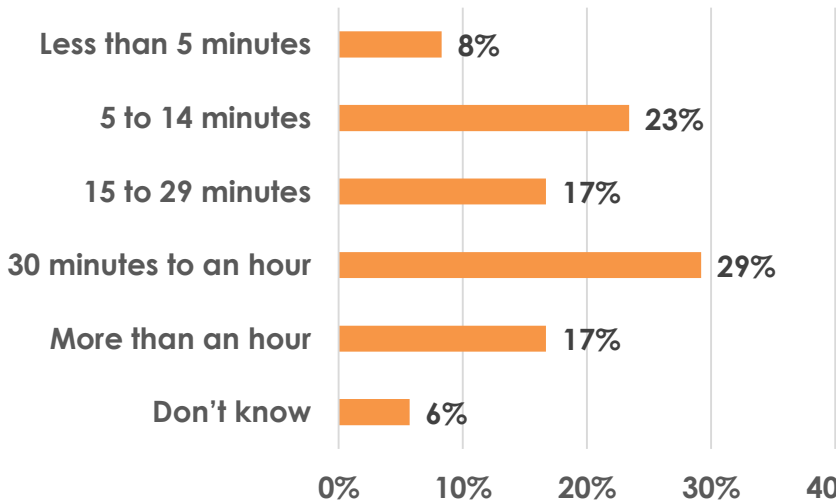
When asked how much time they estimate it would take to configure a new VPN, 31% believe it would take less than 15 minutes, 17% indicate 15 to 29 minutes, 29% indicate 30 minutes to an hour, and 17% indicate it would take more than an hour.

Have you set up a VPN in the past year?

No
24%

Yes
76%

How much time do you estimate it would take you to configure a new VPN?

Less than 5 minutes	8%
5 to 14 minutes	23%
15 to 29 minutes	17%
30 minutes to an hour	29%
More than an hour	17%
Don't know	6%

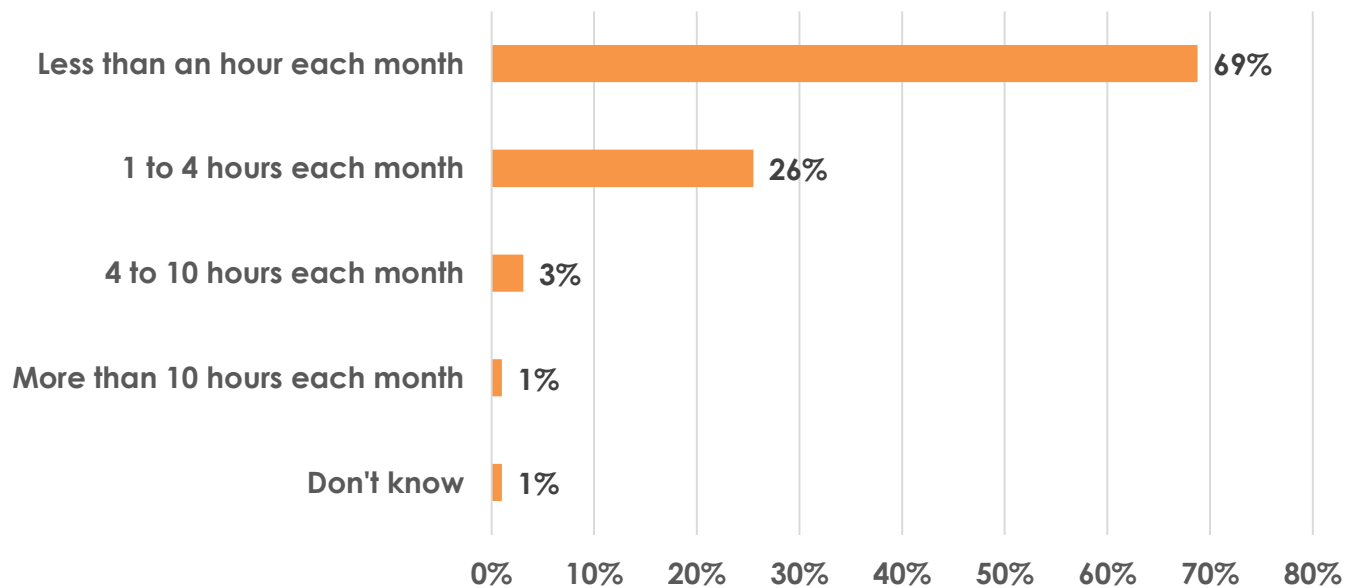0%   10%   20%   30%   40%

Respondents = 191

Respondents = 192

3

Time Spent Maintaining Existing VPNs

When it comes to maintaining existing VPNs and managing user rights pertaining to VPNs, more than two-thirds (69%) state it takes less than an hour each month, while 26% indicate one to four hours, and 4% indicate more than four hours each month.

How much time do you spend each month maintaining existing VPNs and managing user rights pertaining to VPNs?

| Category	Percentage
Less than an hour each month	69%
1 to 4 hours each month	26%
4 to 10 hours each month	3%
More than 10 hours each month	1%
Don't know	1%

Respondents = 192
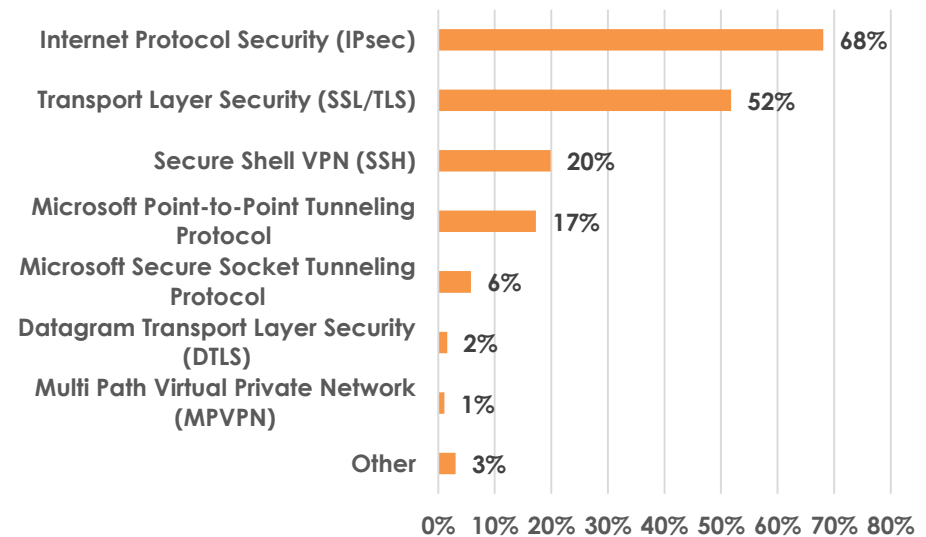
Type of VPN Solution

The majority of respondents (72%) state their organization uses a firewall based service for their VPN solution, while 26% use a server based service.

Most respondents state their organization uses Internet Protocol Security (IPsec) (68%) and / or Transport Layer Security (SSL/TLS) (52%). Other protocols used are Secure Shell VPN (SSH) (20%) and Microsoft Point-to-Point Tunneling Protocol (17%).

What type of VPN solution does your company use? (Select all that apply.)

Firewall based service	72%
Server based service	26%
External VPN Service Provider	7%
Other	6%
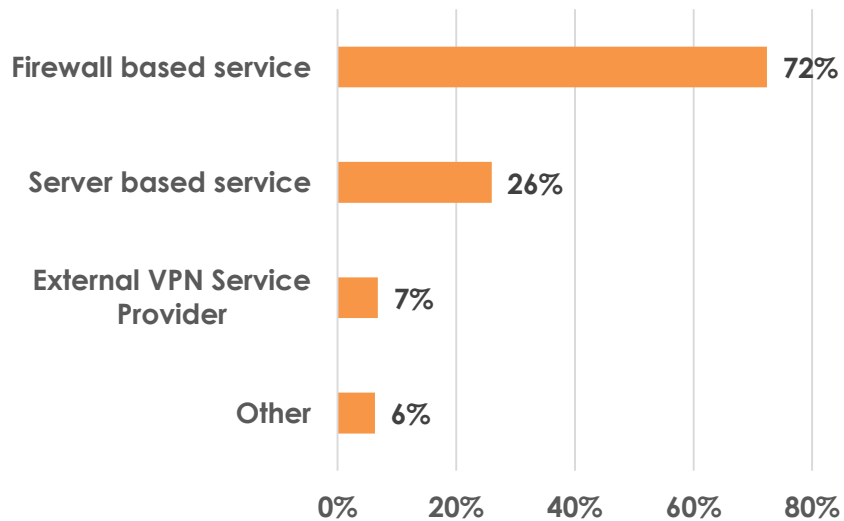
Respondents = 192

Which of the following VPN security protocols does your company employ? (Select all that apply.)

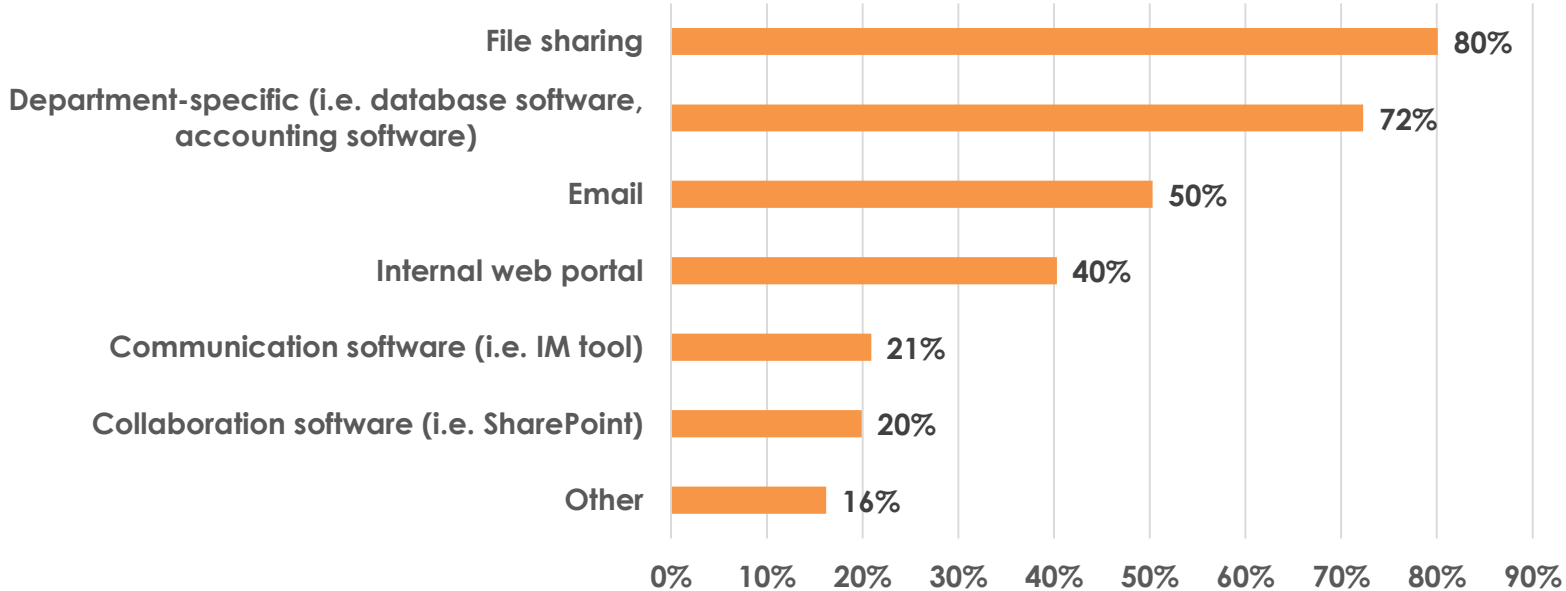|	
Internet Protocol Security (IPsec)	68%
Transport Layer Security (SSL/TLS)	52%
Secure Shell VPN (SSH)	20%
Microsoft Point-to-Point Tunneling Protocol	17%
Microsoft Secure Socket Tunneling Protocol	6%
Datagram Transport Layer Security (DTLS)	2%
Multi Path Virtual Private Network (MPVPN)	1%
Other	3%

Respondents = 191

Accessing Applications

The majority of respondents state their organization's employees use the VPN tunnel for file sharing (80%) and department specific (72%) applications. Other applications include Email (50%) and Internal web portal (40%). Sixteen percent indicate "other," and these verbatim responses are included in the Excel file provided.

**What applications do your employees use through your VPN tunnel?
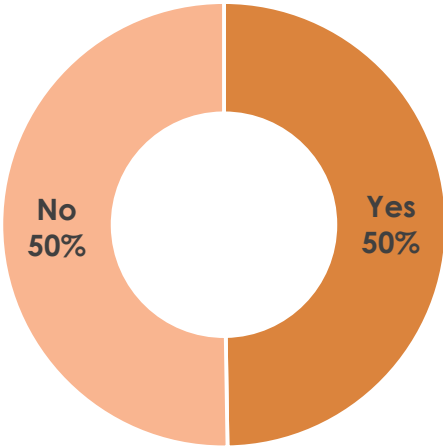(Select all that apply.)**

Application	Percentage
File sharing	80%
Department-specific (i.e. database software, accounting software)	72%
Email	50%
Internal web portal	40%
Communication software (i.e. IM tool)	21%
Collaboration software (i.e. SharePoint)	20%
Other	16%

Respondents = 191

Vendor Access to Network

Respondents are evenly split on whether they allow any of their vendors and / or trusted third parties VPN access to their organization's network.
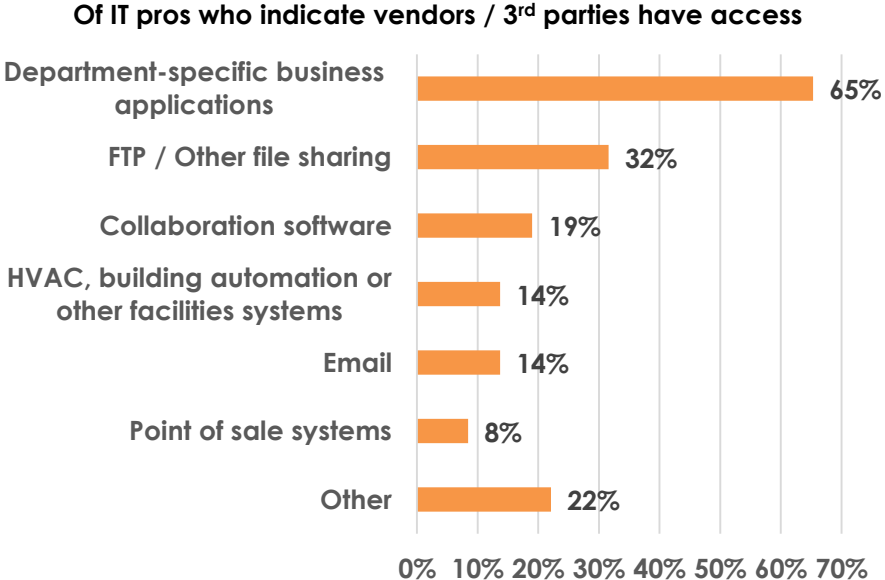
Of the 50% of respondents who allow VPN access, 65% allow vendors access to department-specific business applications (i.e. database software, accounting software). Other programs or systems are FTP / other file sharing (32%) and collaboration software (19%). Twenty-two percent indicate "other," and these verbatim responses are included in the Excel file provided.

Do you allow any of your vendors and/or trusted 3rd parties VPN access to your network?

No
50%

Yes
50%

What programs or systems are the vendors accessing? (Select all that apply.)

Of IT pros who indicate vendors / 3rd parties have access

Department-specific business applications	65%
FTP / Other file sharing	32%
Collaboration software	19%
HVAC, building automation or other facilities systems	14%
Email	14%
Point of sale systems	8%
Other	22%

0% 10% 20% 30% 40% 50% 60% 70%

Respondents = 192
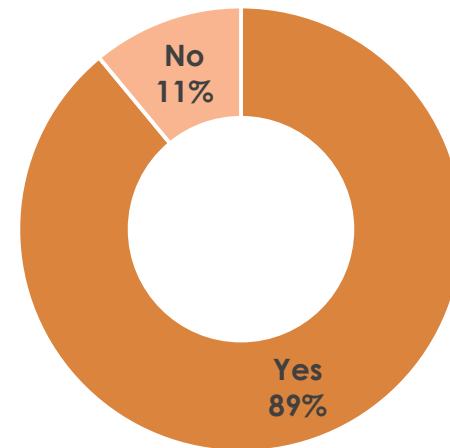
Respondents = 95

Types of Authentication

Nearly all respondents (93%) use passwords for authentication, while an additional 29% use two-factor authentication.

Further, the majority (89%) state this authentication is standardized across all VPNs in their organization.

What types of authentication do you use with VPN connections? (Select all that apply.)

Category	Percentage
Passwords	93%
Two-factor authentication	29%
Biometrics	1%
Other	3%
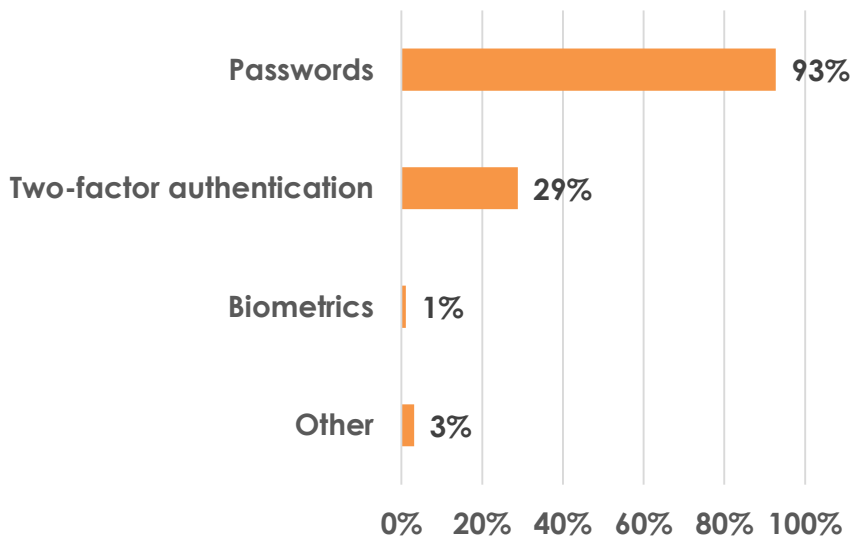
Respondents = 191

Is authentication standardized across all VPNs in your organization?

No 11%
Yes 89%

Respondents = 191

Number of Remote Devices Supported

When asked how many remote devices they support, three-quarters indicate they support one to 100 remote devices. However, 20% support more than 100 devices, and 4% indicate they don't support remote devices.

**How many remote devices do you and your team support?**
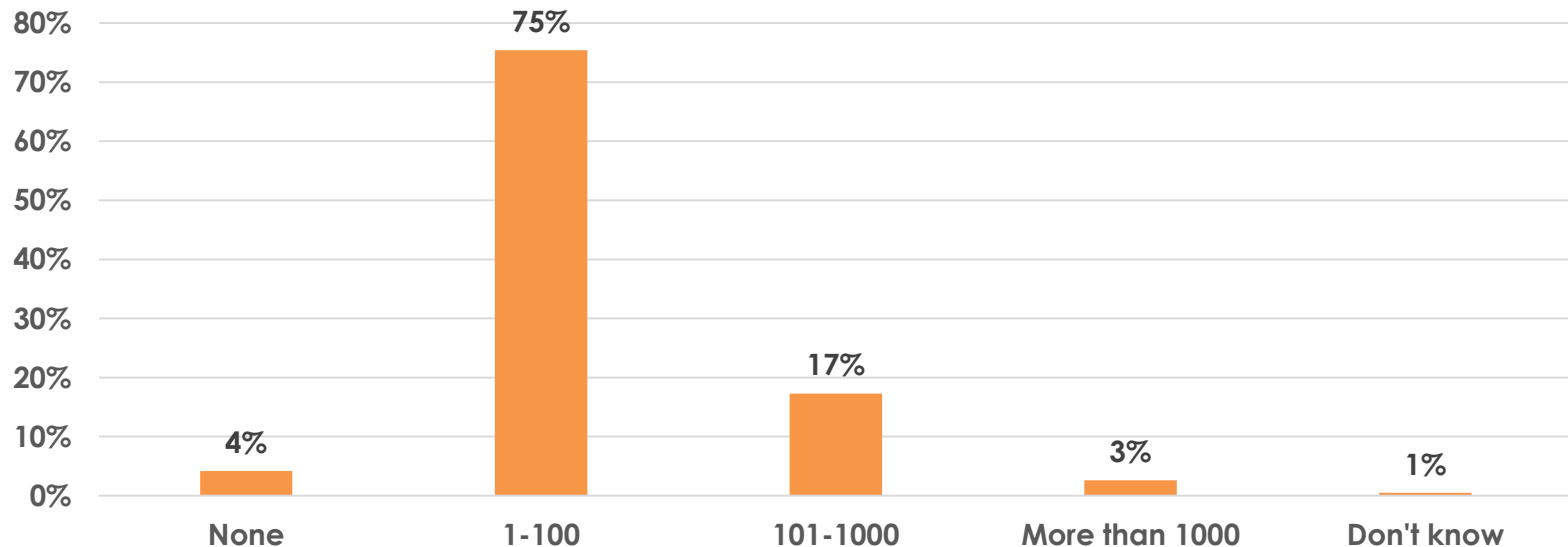
Respondents = 191

Effectiveness of Current VPN Solution

Three-quarters of respondents believe their VPN solution is very to extremely effective at providing employees remote access to their organization's intranet. Respondents also feel it's very to extremely effective at connecting multiple locations (63%) and pulling data for reports (47%).

Using a scale of 1 to 5, where 1 is not at all effective and 5 is extremely effective, please rank how effective your VPN solution is at the following:

Weighted Average
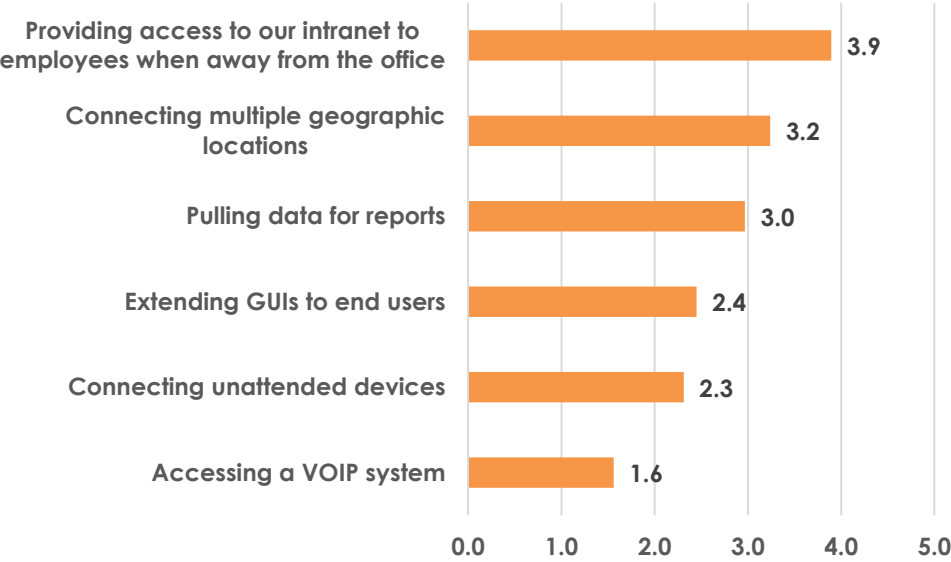
	Top Two (Very to extremely effective)	Bottom Two (Not very to not at all effective)	Not applicable
Providing access to our intranet to employees when away from the office	75%	3%	9%
Connecting multiple geographic locations	63%	5%	24%
Pulling data for reports	47%	14%	19%
Extending GUIs to end users	42%	10%	35%
Connecting unattended devices	34%	11%	35%
Accessing a VOIP system	23%	14%	52%

Weighted Average chart:
- Providing access to our intranet to employees when away from the office: 3.9
- Connecting multiple geographic locations: 3.2
- Pulling data for reports: 3.0
- Extending GUIs to end users: 2.4
- Connecting unattended devices: 2.3
- Accessing a VOIP system: 1.6

Scale: (1) Not at all effective, (2) Not very effective, (3) Somewhat effective, (4) Very effective, (5) Extremely effective

Respondents = 186-188

Limitations of VPNs

Nearly half (47%) state that the difficulty for employees to connect remotely is the greatest limitation of VPNs. Other limitations are reliability of connection (35%), degree of expertise needed to configure (27%) and logging use (26%).

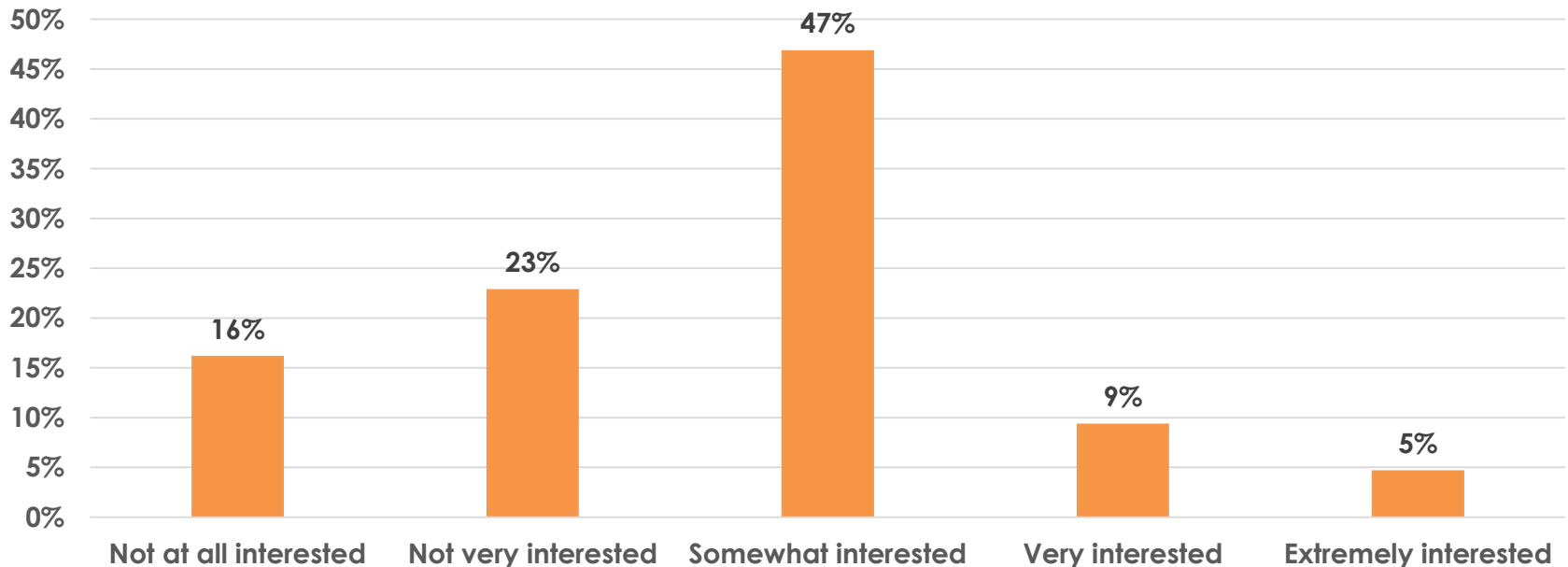**Which of the following do you consider to be the greatest limitation of VPNs? (Select all that apply.)**
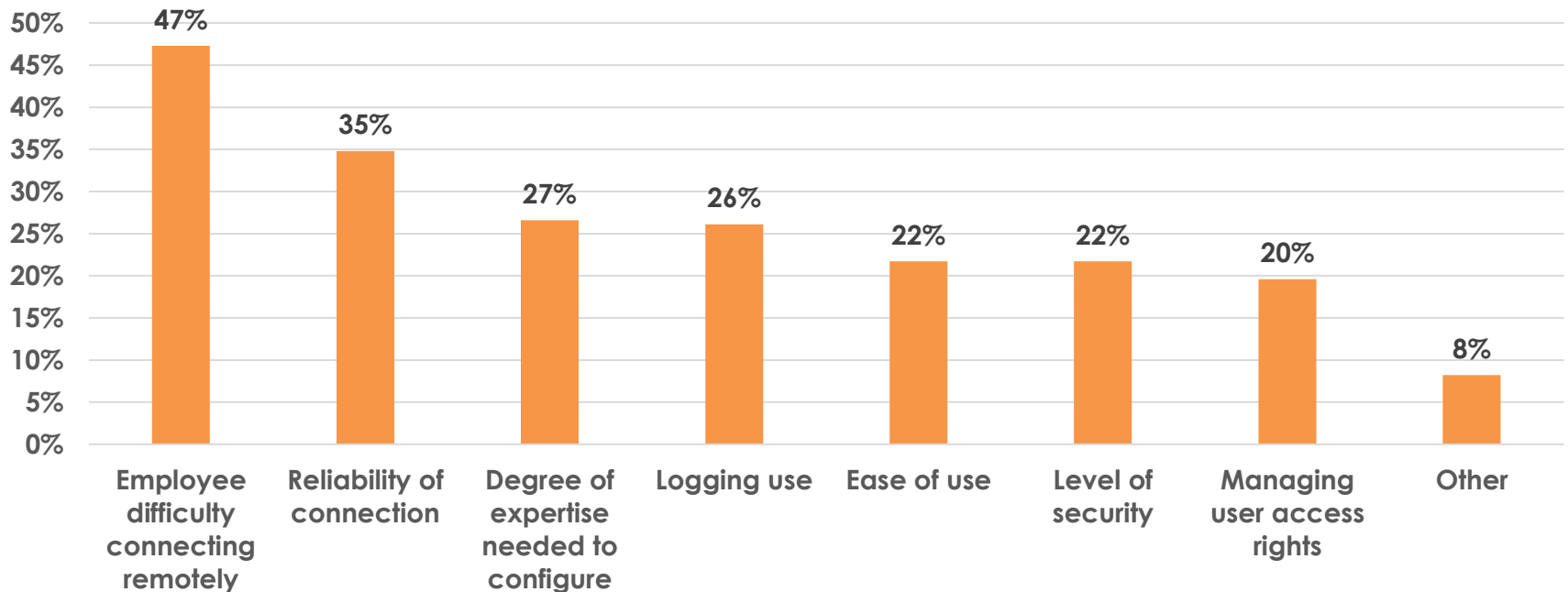
Respondents = 184

Interest in an Alternative VPN Solution

When asked how interested they would be in a product that replicates the functions of a VPN (but is easier to use and maintain), 47% indicate they're somewhat interested, and 14% are very to extremely interested. However, 39% indicate they're not at all to not very interested.

How interested would you be in a product that replicated the functions of a VPN but was easier to use and maintain and allowed port-specific access?

Respondents = 192

Respondent Profile

Company Size

Size	Percentage
1-19	14%
20-99	35%
100-249	30%
250-499	8%
500-999	8%
1000 or more	5%
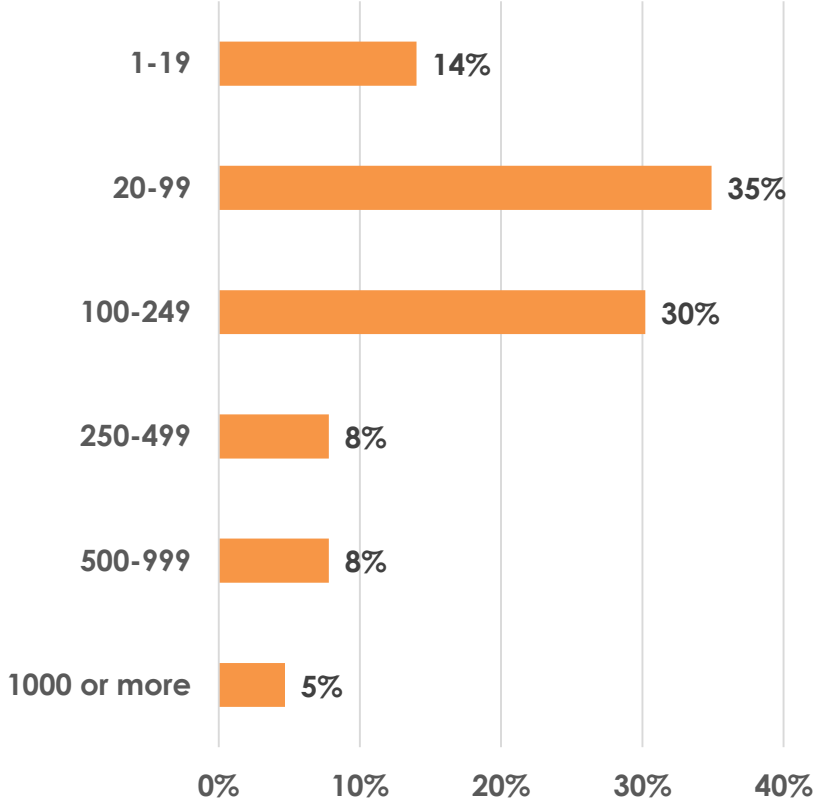
Industry

Top 16 industries are shown

Industry	Percentage
Manufacturing	16%
Healthcare	10%
IT service provider	9%
Non profit	7%
Government	7%
Finance	6%
Engineering	6%
Retail	5%
Education	5%
Legal	3%
Energy	3%
Consulting	3%
Software	3%
Construction	3%
Transportation	2%
Insurance	2%

Total = 192

Total = 192