# Table of Contents

Introduction .......................................................................................................................... 3

Chapter 1:  
What IT Pros Think about Network Security ................................................................. 4

Chapter 2:  
Key Challenges with Managing WAN Connectivity ...................................................... 8

Chapter 3:  
Exploring the Benefits of Network Security Solutions ............................................. 11

Conclusion .......................................................................................................................... 13
Today’s cybersecurity threats are more advanced and persistent than ever, and organizations of all sizes are at risk. In fact, 62% of all cyberattacks target SMBs.¹

Mid-sized businesses have the same type of information commonly found at global companies, and it’s usually less secure. They often have limited IT staff to maintain proactive security measures and guard against insider threats, while also supporting day-to-day operational issues.

To keep their businesses safe and secure, IT decision-makers (ITDMs) are searching for solutions that can enhance network connectivity, improve security, and strengthen infrastructure in a world of increasing threats. These solutions must also make the most of limited time and resources.

A recent Spiceworks survey of 250 IT decision-makers for mid-sized business revealed deep insights into how IT pros view network security, as well as the challenges, benefits, and drivers of deploying comprehensive network security solutions. This report explores the survey results.
In our data-driven world, companies are having to reframe their approach to network security. As security threats increase in size and sophistication, the growing use of cloud-based applications and services connected to public-facing networks—combined with the use of personal devices for business—has exposed more data to attack. At the same time, businesses need to share more data in more places with customers and employees, which proportionately increases the risk of that data being compromised.

As a result, ITDMs are being pulled in multiple directions, often during the same day. Security is a key priority, as IT pros work to meet end-user demands for anytime, anywhere access, while desperately trying to stay ahead of increasingly sophisticated attacks from malicious hackers. Government mandates like the General Data Protection Regulation (GDPR) are setting new standards for information security and data privacy compliance, creating an urgent need for advanced security expertise.

A majority of ITDMs surveyed said they worry about the possibility of unknown security breaches, the impact of those breaches on their business, and the time and skills required to fend off existing and potential threats. Meanwhile, they often have to fit network security solutions into an already tight IT budget, making the cost of those solutions a top challenge (66%). Day-to-day pain points, including the complexity of monitoring logs, lack of time to address security issues, and the fear of unintentional human error were also top of mind.

### Challenges when Deploying Network Security Solutions

- **Cost of solutions**: 66%
- **Monitoring logs/potential threats**: 48%
- **Limited time/resources to properly secure the network**: 46%
- **Inadequate budget for security solutions**: 45%
- **Increased management/operational complexity**: 44%
- **Difficulty keeping up with new threats/protection techniques**: 40%
Most of the surveyed ITDMs reported deploying an average of seven different network security capabilities—led by anti-virus, anti-malware, anti-spam, and URL filtering/blocking—to protect their network from security threats. This is especially challenging because 79% of these organizations manage their network security challenges in-house.

### Top security threats experienced in the past year

<table>
<thead>
<tr>
<th>Threat</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>73%</td>
</tr>
<tr>
<td>Malware</td>
<td>36%</td>
</tr>
<tr>
<td>Spyware</td>
<td>28%</td>
</tr>
<tr>
<td>Ransomware</td>
<td>20%</td>
</tr>
<tr>
<td>Web application attacks</td>
<td>16%</td>
</tr>
<tr>
<td>Denial of Service attacks (DoS/DDoS)</td>
<td>6%</td>
</tr>
</tbody>
</table>
82% of survey respondents reported experiencing at least one type of security threat in the past year.

In spite of deploying multiple layers of network protection, 82% of respondents reported experiencing at least one type of security threat in the past year. And the fallout of a security breach can be devastating. An overwhelming majority of survey respondents (80%) singled out costs associated with time and resources as the biggest casualty, followed by reduced employee productivity, loss of revenue, and damages to brand and reputation.

<table>
<thead>
<tr>
<th>Experienced/Expected Results of Security Threat/Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="chart.png" alt="Chart showing percentages of IT pros' expectations" /></td>
</tr>
</tbody>
</table>
When asked about the network security and management concerns that keep them up at night, IT pros responded:

“I’m only human and can miss something. There’s always someone else smarter than me out there.”

“I worry that my knowledge is a mile wide but an inch deep.”

“Crypto haunts my dreams.”

“We are a small org with not many virus attacks, but what keeps me up is the one that eventually gets through, taking out the network and the company.”

It’s clear that cyber-threats have climbed to the top of IT pros’ worry lists for fear that a data breach could cause serious damage or even take down their businesses. With new risks emerging daily and traditional “protect the perimeter” technology strategies proving insufficient, IT pros are struggling with the lack of know-how and resources to make effective network security decisions.
Companies everywhere are seeking to modernize their infrastructure to achieve better operational efficiencies and drive business growth. For organizations today, it’s critical to ensure that the network isn’t the “weak link” in their digital strategy. Tasked with supporting new bandwidth requirements driven by the rise of IoT and BYOD trends, IT pros are seeking new ways to provide the best possible performance and access to resources across the wide-area network.

The Spiceworks survey revealed that organizations use multiple WAN services. Most respondents use an average of three different WAN services—led by fiber/carrier ethernet (72%), broadband (55%) and wireless LAN (49%)—to connect employees and workflows.
Managing and securing the corporate WAN is a top priority for IT pros. With organizations deploying new cloud, mobile, and IoT initiatives, they’re more reliant on the network than ever. The volume of applications and workloads on the network is growing rapidly, along with the demands for fast, reliable access. IT teams need to be able to count on end-to-end network solutions that are reliable, extensible, and simple to operate, so they have more time to focus on other strategic activities.

Tasked with managing an enterprise WAN that’s more expansive and complex, IT pros are faced with an array of challenges. The vast majority of surveyed IT pros said that network availability, security, and performance are the most critical factors to consider when deploying current WAN services.

**Factors of Importance When Deploying WAN Services/Solutions**

- **Availability/reliability (uptime)**: 92%
- **Performance (bandwidth, throughput)**: 78%
- **Security**: 82%
- **Quality of Service (QoS)**: 54%
- **Capacity**: 52%

It’s critical to ensure that the network isn’t the “weak link” in the organization’s digital strategy.
When the WAN runs smoothly, businesses can communicate effectively and data is free-flowing. But when WAN performance issues do occur, productivity can be hindered and collaboration with coworkers and customers can come to a screeching halt. Surveyed ITDMs cited a variety of challenges with managing WAN connectivity, most notably around providing network failover and security. These challenges are driving companies to consider network security solutions to help them better protect their networks, meet compliance and reporting requirements, and reduce the burden on in-house security management teams.

<table>
<thead>
<tr>
<th>Challenges with Managing WAN Connectivity</th>
<th>42%</th>
<th>40%</th>
<th>33%</th>
<th>32%</th>
<th>29%</th>
<th>29%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Providing network failover</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost of WAN connectivity/backbone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Troubleshooting problems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unreliable connection/low bandwidth</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability/reliability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Spiceworks survey revealed that IT pros are extremely interested in comprehensive network security solutions that can help them with the areas that they perceive as most critical—security (71%), availability (67%), and performance (66%).

Top Benefits of Deploying Network Security Solutions

- Improved security
- Simplified IT operations
- Centralized management
- Time to drive key initiatives
- Access to security experts
By deploying comprehensive network security solutions, organizations can benefit from reduced capital expenditures, while effectively balancing the productivity of their IT resources. Survey respondents indicated that they expect these solutions to improve security, centralize network management, and free up time for IT to focus on other key initiatives.

So, what’s holding ITDMs back from deploying the right network security solutions? Cost (76%) is the top concern, along with worry about the risk of relying on a third-party (65%), lack of control (61%), and uncertainty about the ROI (54%).

| The areas where IT pros believe network security solutions can make the biggest difference: |
|---------------------------------|-----------------------------|
| Security                        | 71%                         |
| Availability/reliability (uptime)| 67%                         |
| Performance (bandwidth, throughput) | 66%                      |
| Deployment/management           | 62%                         |
| Quality of Service (QoS)        | 62%                         |

“There aren’t enough hours in the day for a multi-role admin in a medium-sized business to catch everything.”

—IT professional, survey respondent
Conclusion

While improving security, performance, and agility are top priorities for all organizations, it’s up to individual ITDMs to make sure it happens in most mid-sized businesses. By partnering with a single vendor that offers a holistic approach for protecting networks—actively preventing, mitigating, and responding to attacks—organizations can simplify network management, reduce the need for multiple providers, and trim administration costs.

CenturyLink works with growing businesses seeking to digitize their operations. These companies count on CenturyLink as a single-source provider with deep expertise, state-of-the-industry equipment, and flexible, fully integrated IT services. CenturyLink supports their expansion to new sites, manages bandwidth and equipment upgrades, and resolves complex network issues so that their in-house IT teams can focus on strategic initiatives and drive business growth.

As the threat landscape becomes more complex and destructive, companies need greater insights to avoid losing valuable data and sensitive information. To help you stay ahead of evolving threats and gain the insights you need to proactively secure your network, CenturyLink leverages its expansive global network to see farther and deeper, allowing you to react in time and prevent a devastating breach. CenturyLink goes beyond data analysis and combines critical insights, artificial intelligence, and human-machine interaction to define the best path of protection for all your information assets.

From adaptive network security that filters data requests from devices to providing round-the-clock visibility into potential threats and easy access to security professionals, CenturyLink empowers businesses with an efficient and cost-effective ecosystem of solutions to secure people, data, and things.

Ready to take the next step?
Learn more about CenturyLink Network Security Solutions.

Download the How-To Guide

About the Survey

In May 2018, Spiceworks surveyed IT decision-makers in the U.S. in an online research panel on behalf of CenturyLink. All 250 respondents were from organizations with 11 to 500 employees, and they were required to have influence on network connectivity and security solution purchases by their organizations.

This document is provided for informational purposes only and may require additional research and substantiation by the end user. In addition, the information is provided “as is” without any warranty or condition of any kind, either express or implied. Use of this information is at the end user’s own risk. CenturyLink does not warrant that the information will meet the end user’s requirements or that the implementation or usage of this information will result in the desired outcome of the end user. This document represents CenturyLink’s products and offerings as of the date of issue. Services not available everywhere. Business customers only. CenturyLink may change or cancel products and services or substitute similar products and services at its sole discretion without notice. ©2018 CenturyLink. All Rights Reserved.