



untangle<sup>®</sup>

# VOICE OF THE CHANNEL AND 2020 PREDICTIONS

REPORT



A handwritten signature in black ink that reads 'Steve Young'.

**Steve Young**  
Channel Marketing Manager

## INTRODUCTION

---

I am delighted to share Untangle's second annual Voice of the Channel Report and 2020 Predictions.

Untangle prides itself on building lasting and beneficial relationships with our Channel Partners who provide network security solutions to small and midsize businesses (SMBs) and organizations all over the world. Our Channel Partners help protect the networks of more than 40,000 customers in a variety of industries. Nonetheless, they continue to experience similar barriers SMBs face in the cybersecurity market - budget constraints and resource limitations. Channel Partners, by nature of their role in helping source solutions, inherit the barriers that SMB's face in the Cybersecurity market and need to work within the budgets allocated. To combat these barriers, Channel Partners continue to deploy scalable solutions to meet the needs of their clients today and in the future.

For this annual report, we surveyed Channel Partners, both locally and internationally, to understand current cybersecurity trends the channel is seeing, as well as their predictions for 2020. We've compiled the survey data on IT trends, current service portfolios, customer threats, and on how these trends shape strategic business decisions for their organizations moving forward.

In 2019, our Channel Partners reported an increase in malware and phishing attacks, and unfortunately believe this trend will continue in 2020. However, as cyber criminals have increased their attack tactics, Channel Partners have also increased their security service offerings to meet these emerging threats. Most Channel Partners have foundational cybersecurity products in their portfolios that provide them with a variety of solutions to fit the needs of their clients for today's and tomorrow's threats.

As the industry looks forward to 2020, Channel Partners anticipate ransomware and phishing will continue to be the biggest threat to their clients, and working with vendors who provide a robust network security solution to address these threats will be key.

Untangle is committed to providing enterprise-grade network security solutions, management, and advanced networking solutions at price points that help our Channel Partners meet their clients' needs.

## CURRENT CHANNEL IT TRENDS

2019 was a challenging year for network security professionals. Cyber criminals targeted government, business and personal data at breakneck speeds. Attacks were made on government systems in Baltimore, IT infrastructures at 49 school districts, multiple instances of personal data being stolen such as credit card information and dental records.

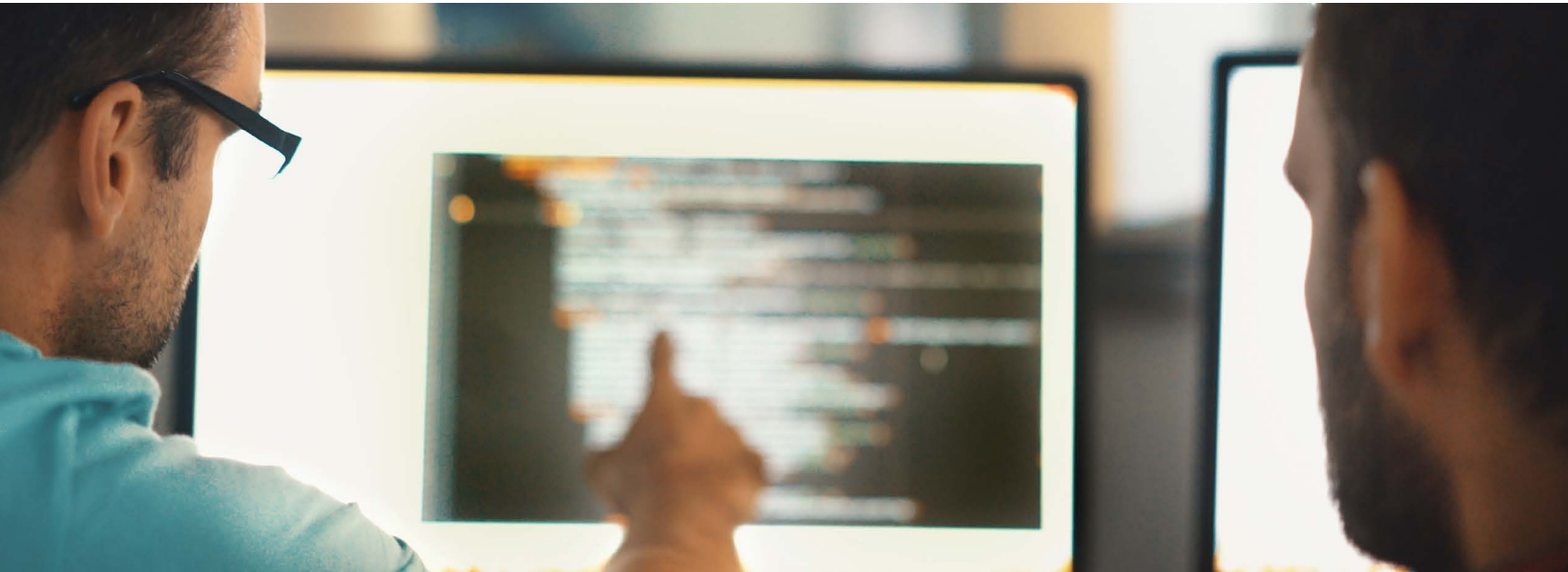
Channel Partners, IT security professionals who assist SMBs and organizations with network security deployment, were integral in 2019's battle against cyber attack. As cybercriminals shifted their target to weaknesses within business supply chains to gain entry into the network, these security service professionals were on hand to mitigate and help customers recover from these attacks.

# 23%

of channel partners identify limited solutions knowledge as a top barrier in cybersecurity

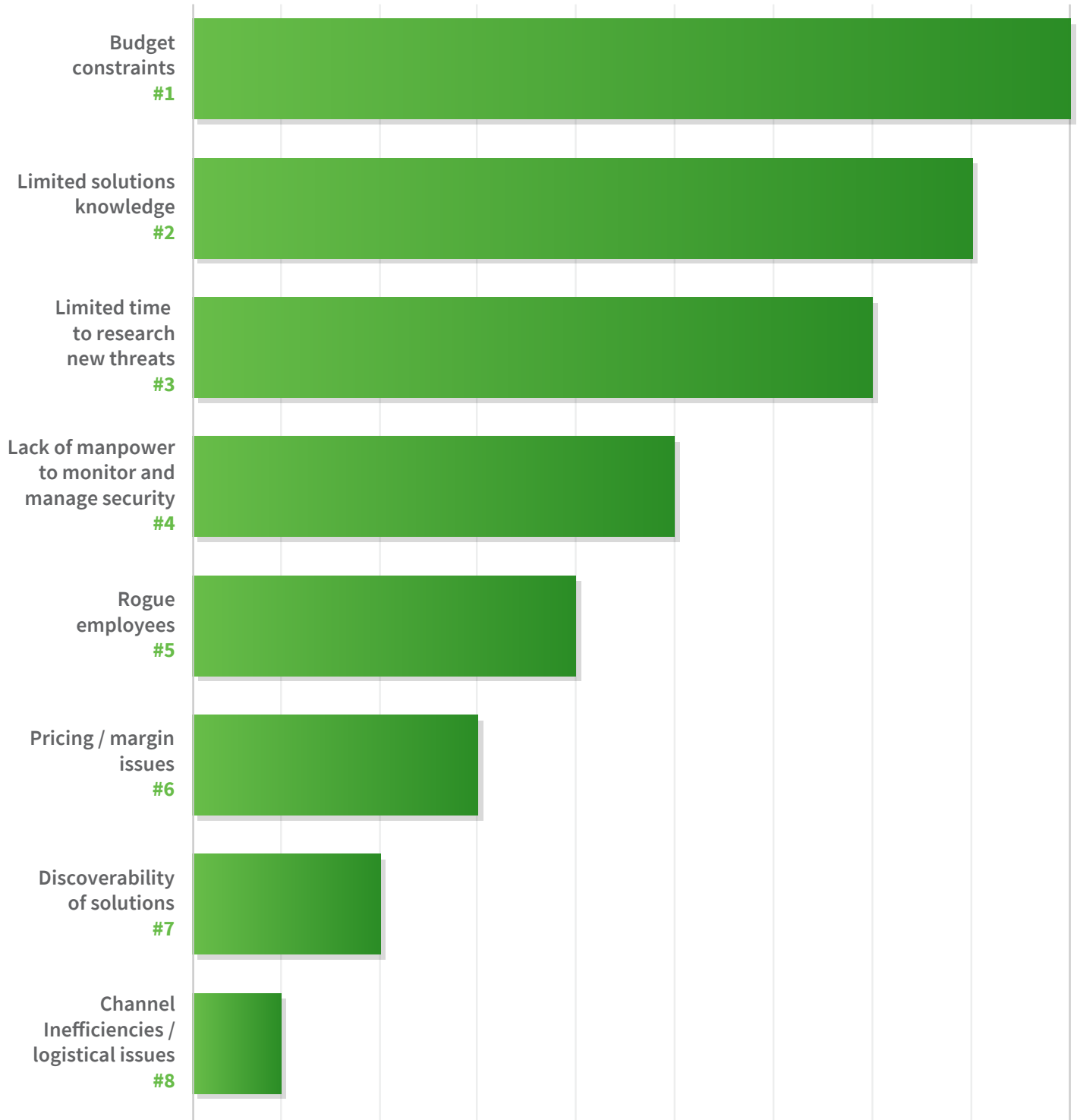
# 22%

of channel partners identify budget constraints as a top barrier in cybersecurity



Channel Partners, however, are not without their own barriers. 23% of Channel Partners surveyed identify lack of customer knowledge as the top barrier in cybersecurity, followed by customer budget constraints (22%), and limited time to research and understand new threats (13%). Channel Partners showcase that they can be the first, and sometimes the only line of defense against a cyber attack, but without customers understanding that they are risk, they are often called upon after an attack has already occurred.

# Top Barriers the Channel Experiences in the Cybersecurity Market



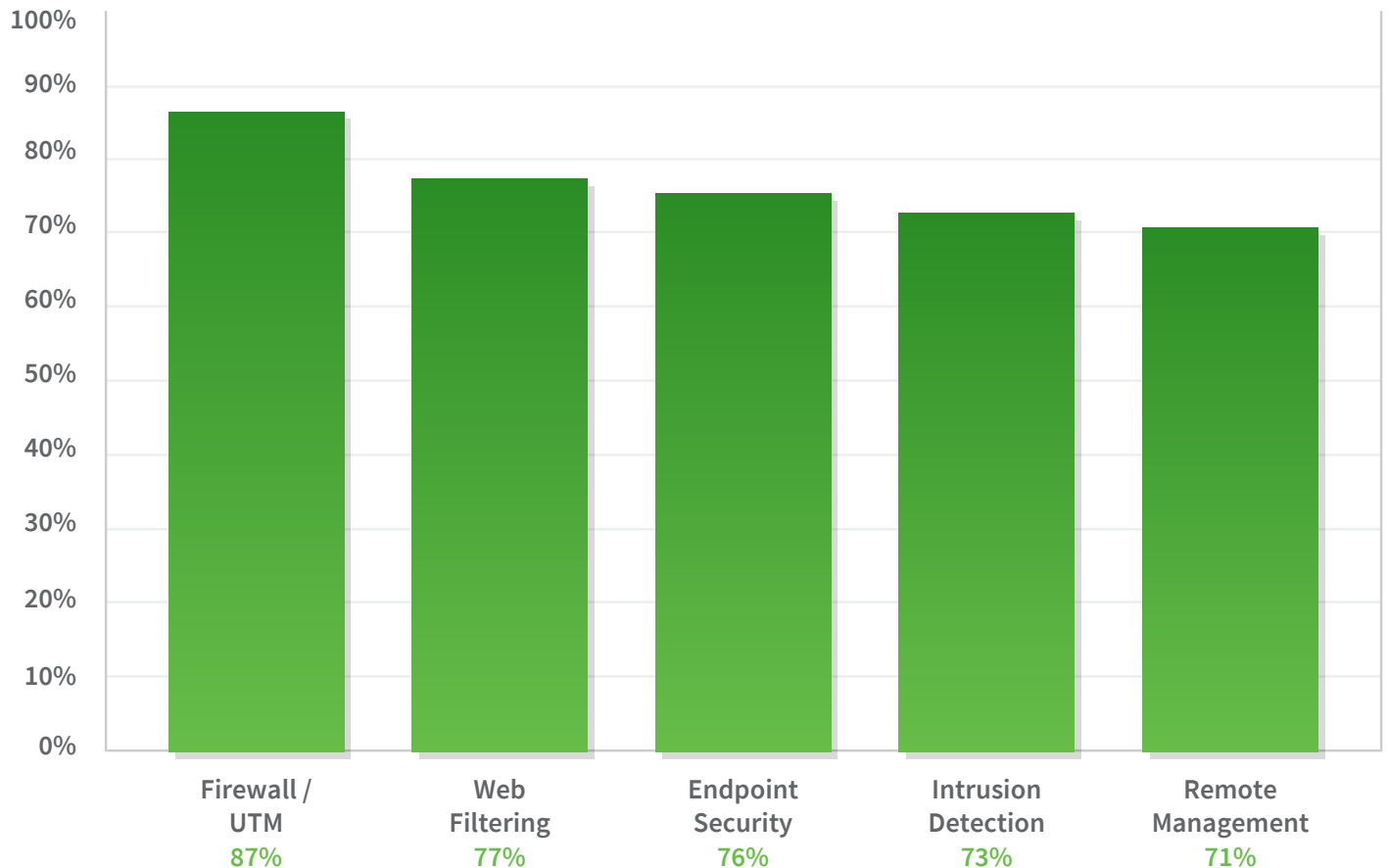
## ROBUST SERVICE OFFERINGS

A majority of respondents provide a variety of services and solutions for clients looking to outsource their IT needs.

As cybersecurity has become a cornerstone of any business or organization's yearly planning, service providers have increased their service portfolio. A majority of Channel Partners already have foundational cybersecurity products in their portfolios, like firewall/UTM (87%), web filtering (77%), endpoint security (76%), intrusion detection and prevention (73%), remote monitoring and management (71%), and data loss prevention (50%), that provide them with a variety of solutions to fit the needs of their clients.

In 2018, 77% of respondents stated that cybersecurity was less than 30% of their overall business, in 2019, this increased to over 50%, which indicates a growing awareness of the need to put preventative measures in place.

### *Top 5 Product Offerings from Channel Partners*



## CYBERATTACKS

2019 saw an increase of cyberattacks, with Channel Partners identifying their clients were specifically targeted by phishing (84%), malware(84%), and ransomware (63%) attacks.



In many cases, budget restrictions or other limitations, such as not having dedicated IT Staff, are a driving factor for SMB vulnerability. Of those Channel Partners who responded, 44% identified that their clients still fell victim to malware attacks after they hired a third-party security vendor.

### *How can this be?*

In many cases, this is a result of budget limitations from the client side. A clear example of this is Landry's Restaurant, as they fell victim to a security breach for a second time in 2019. The initial security breach, in May 2015, affected several restaurants in the Landry's portfolio targeting point-of-sale systems at the restaurants and stealing customer information. To address this system vulnerability, Landry's implemented an encrypted endpoint security system on all point-of-sale devices across more than 500 properties.

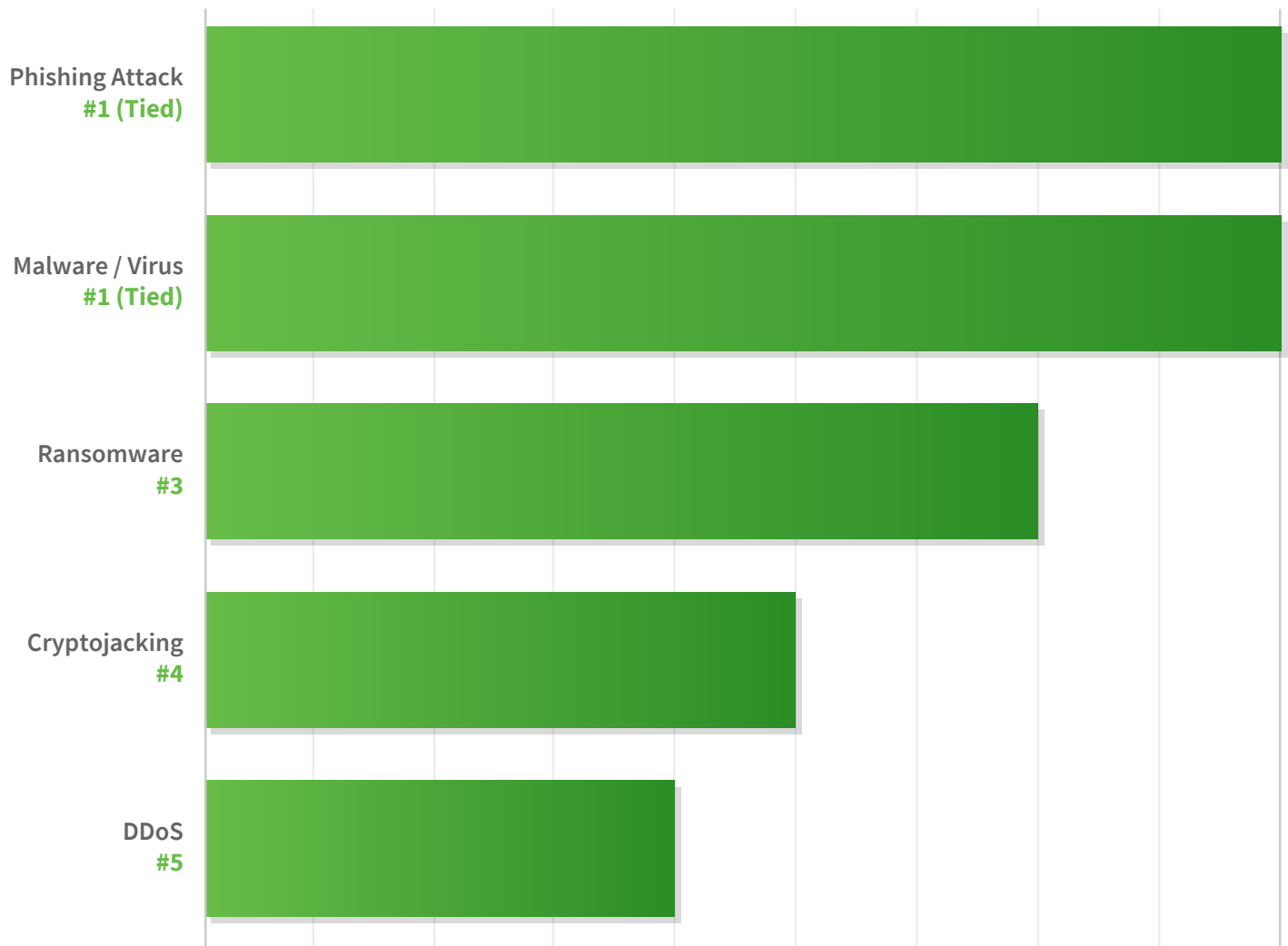


Fast forward to December 2019, Landry's announced a second data breach affecting customers' payment cards. This data breach was the result of employees not actually using the encrypted endpoint security systems. Employees had multiple options for processing payments, not all of which had the same level of encryption. Even after having made the investment in the encrypted endpoint security system, employees were not using it for every transaction.

The budget limitations to support all card-reading devices and a lack of time and resources spent on employee training created the perfect storm. While Landry's had invested in adding encryption to their endpoint security system, this only provided part of a robust protective layer around processing payments, leaving other components of their systems vulnerable.

There is light at the end of the tunnel, however. Due to SMBs and organizations contracting with Channel Partners, they are becoming more aware of how to identify suspicious emails and abnormal network traffic. According to our survey, clients reported ransomware (43%), phishing (42%) and malware (40%), after a breach occurred. This indicates that clients are becoming better at identifying cyberattacks and taking proactive steps to continue educating employees and report attempts before they can cause damage.

## *Top 5 Cyberattacks Channel Partners Customers Were Victims of in 2019*

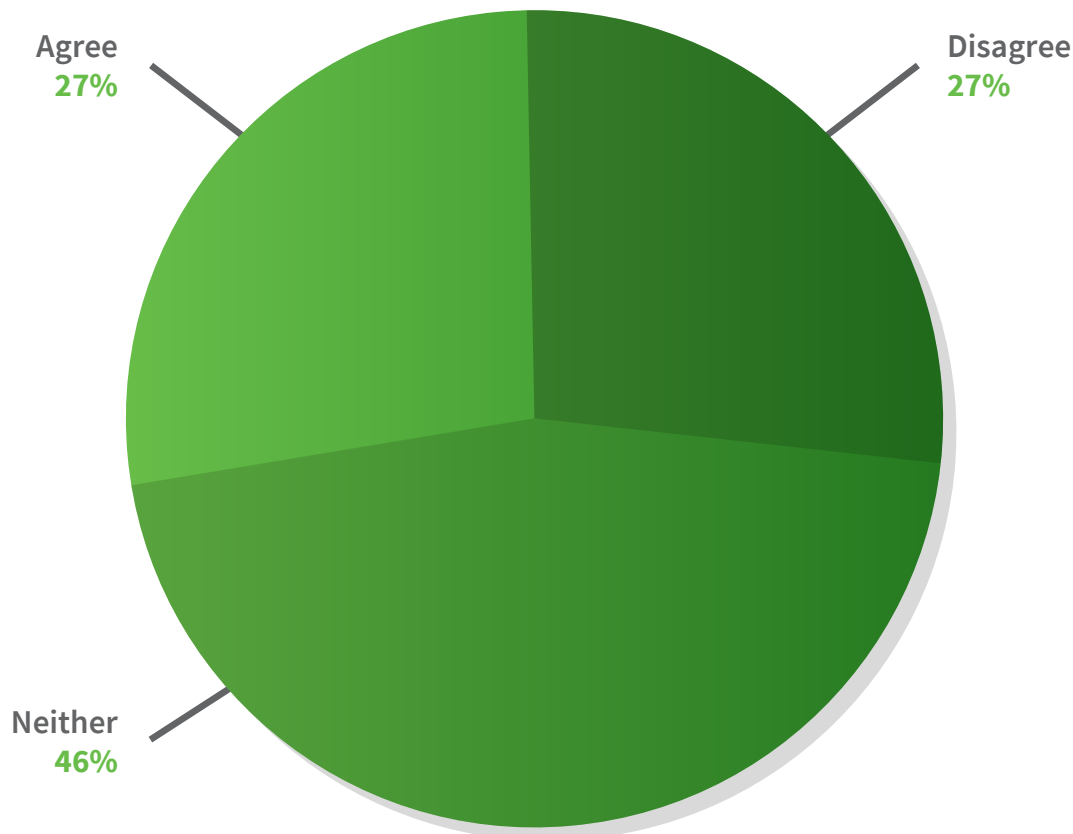


## CLIENTS REMAIN SKEPTICAL ABOUT CLOUD ADOPTION

As businesses continue to look for innovative ways to streamline workflows, connect branch offices and remote employees, while reducing capital expenses, many have turned to cloud-based applications. However, there is still skepticism about security within the cloud.

Price (36%), limited experience (26%) and lack of trust (20%) are the top barriers the channel experiences when their clients begin or consider adopting cloud security solutions. Many clients worry about entrusting their business or customer data on a server that belongs to someone else. The lack of education and experience with the cloud along with news of large scale data breaches, such as Quest Diagnostics (11.9 million records), CapitalOne (100 million records), Facebook (540 million records), and CafePress (23 millions records), creates an uphill battle for Channel Partners looking to transition their client's legacy deployments into the modern age.

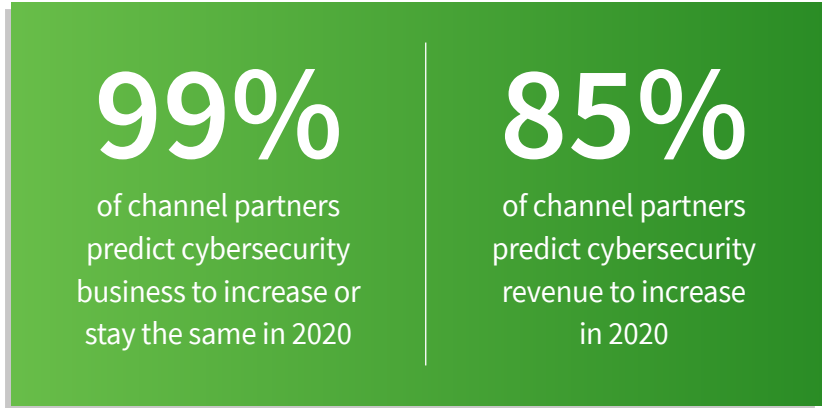
*Do you believe that moving your data/network traffic to the cloud offers better security?*





# 2020 CYBERSECURITY PREDICTIONS

99% of Channel Partners indicated that cybersecurity, as an overall part of their business, will increase or stay the same in 2020, while 85% believe that their cybersecurity revenue will increase in 2020. This is in line with IDC's latest Worldwide Semiannual Security Spending Guide, that indicated global spending on security-related hardware, software and services will grow at a compound growth rate of 9.2% between 2018 and 2022, to a total of \$133.8 billion in 2022.<sup>1</sup>



Currently, 77% of respondents offer managed services to their clients, with an additional 10% actively considering adding this service in 2020. This reflects the broader channel trend of value-added-resellers moving towards adding recurring revenue through an MSP model.



When asked about the largest threats the channel expects to encounter in 2020, ransomware (46%) and phishing (25%) were top ranked choices. BYOD, cryptojacking and rogue insiders were also concerns, but ranked considerably lower.

Many Channel Partners are also looking into expanding their service portfolio. Future product offerings include Compliance-as-a-Service for clients who require additional reporting and regulation, such as schools, libraries, financial institutions and government offices.

<sup>1</sup> <https://www.idc.com/getdoc.jsp?containerId=prUS44935119>

# UNTANGLE PARTNER PROGRAM

Channel Partners play a key role in providing network security solutions to SMBs with limited resources and budget. With the number of cyberattacks expected to increase in 2020, the channel must stay ahead of emerging threats by providing effective network security solutions that are affordable and easy to manage. When considering vendors to partner with, researching and testing out solutions is key to finding the right one for your business.



The Untangle Partner Program provides resellers, managed service providers, and distributors the ability to sell our award-winning products that lead the industry in terms of ease-of-use for both partners and end users. Unique deployment options provide our partners with many choices based on their clients' budgets.

*Join the Untangle Partner Program*

[CLICK HERE TO LEARN MORE](#)

Known industry-wide for its ease-of-use and comprehensive reporting, NG Firewall is the number one choice of small-to-medium businesses and distributed organizations. NG Firewall is seamlessly integrated with Untangle's cloud services, including ScoutIQ™ threat intelligence and Command Center centralized management. Command Center lets partners manage their deployments with ease and convenience from any browser without requiring any on-premise footprint.

# UNTANGLE NETWORK SECURITY FRAMEWORK

The Untangle Network Security Framework, comprised of our award-winning NG Firewall, Untangle SD-WAN Router, and centralized management platform, Command Center, is a comprehensive approach to network security orchestration. This framework offers a suite of cloud-managed security and connectivity options that work together to fit the needs of small-to-medium businesses and distributed enterprises. This integrated approach provides IT teams with the ability to ensure protection, monitoring and control across devices, applications, and events, enforcing a consistent security posture over the entire digital attack surface. Untangle puts IT back in control of dispersed networks, hybrid cloud environments, and IoT and mobile devices.



## ADVANCED SECURITY

- Protection, encryption, control & visibility anywhere
- NG Firewall, IPS, VPN & more
- Onboard security for small network appliances & IoT devices
- Full security processing on-premises or in the cloud

## INTELLIGENT SD-WAN

- Secure, WAN-optimized connectivity for every location
- Seamless scalability
- Patent-pending Predictive Routing™ technology for first packet, dynamic path selection
- Manage one or many appliances from Command Center

## CLOUD MANAGEMENT AT SCALE

- Zero touch deployment
- Configure & push policies
- Advanced alerting & reporting
- Visibility across globally dispersed networks & endpoints



**Untangle, Inc.**

25 Metro Drive, Ste. 210

San Jose, CA 95110

[www.untangle.com](http://www.untangle.com)

**For sales information, please contact us by phone in the US at +1 (866) 233-2296 or via e-mail at [sales@untangle.com](mailto:sales@untangle.com).**

©2020 Untangle, Inc. All rights reserved. Untangle and the Untangle logo are registered marks or trademarks of Untangle, Inc. All other company or product names are the property of their respective owners.