WEBROOT®
Smarter Cybersecurity™

2017 MSP Cybersecurity Trends

Introduction

Technology continues to advance at an almost alarming rate, bringing new ways for cybercriminals to attack endpoints and networks every day. As a result, many managed service providers (MSPs) are faced with an increasing number of challenges when it comes to protecting their clients. In turn, the trust between an MSP and its clients is regularly tested.

One of the biggest and most destructive threats MSPs and their clients have faced in recent years is ransomware. Nearly 70% of managed service providers (MSPs) are not completely confident their clients' endpoints are secure against future ransomware attacks.

/ˈransəm,wer/ | noun.

Ransomware is a virus that encrypts files and more and holds them hostage until businesses pay. Even if you pay the ransom, there's no guarantee that your files will be returned. For small businesses, this type of attack can be devastating, and can even lead to bankruptcy.

According to the FBI, cybercriminals were expected to collect over $1 billion[1] in ransoms during 2016. It's quite likely that actual losses suffered were even higher, given the disruption of productivity and business continuity, as well as a general reluctance to report successful ransomware attacks.

Currently, there are well over 120 separate ransomware families, and Webroot has seen a 3,500% increase[2] in cybercriminal internet infrastructure for launching attacks since the beginning of 2016. Unfortunately, these trends show no signs of slowing down.

We surveyed 500 MSPs to learn their thoughts on the MSP market and the state of ransomware as it pertains to their business, clients, and profits.

[1] CNN.com. Cyber-extortion losses skyrocket, says FBI. (April 2016)

[2] Webroot Inc. The Quarterly Ransomware Report. (Oct 2016)

Survey Background

Of the group surveyed, nearly half manage more than 500 endpoints, and 37% earn over $1 million in managed services revenue per year.

Number of endpoints under management

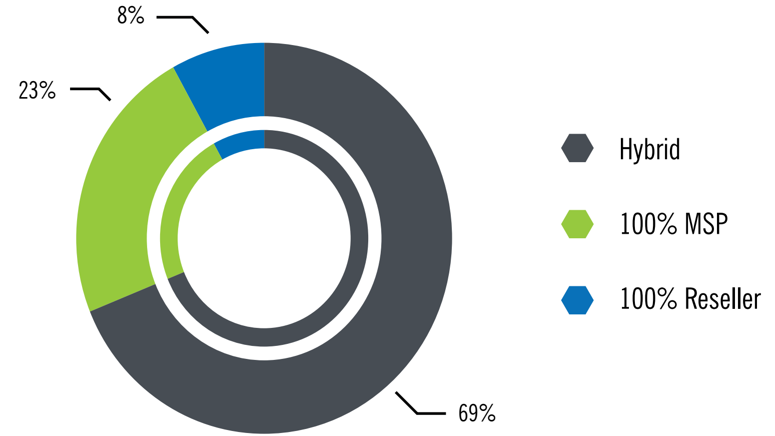
25%	27%	22%
1-100	101-500	501-1000
18%	5%	3%
1001-2500	2501-5000	5000+

Annual managed services revenue

63%	22%	9%
Less than a million	1-5 million	5-10 million
3%	3%	
10-25 million	Over 25 million	

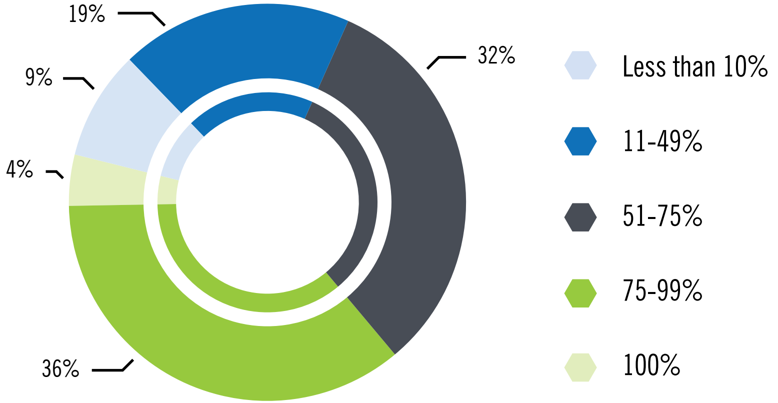
Of the MSPs surveyed, the majority reported they use a hybrid MSP/reseller business model.

Business Model



However, among the respondents, 40% classify their business as 75-100% services based.

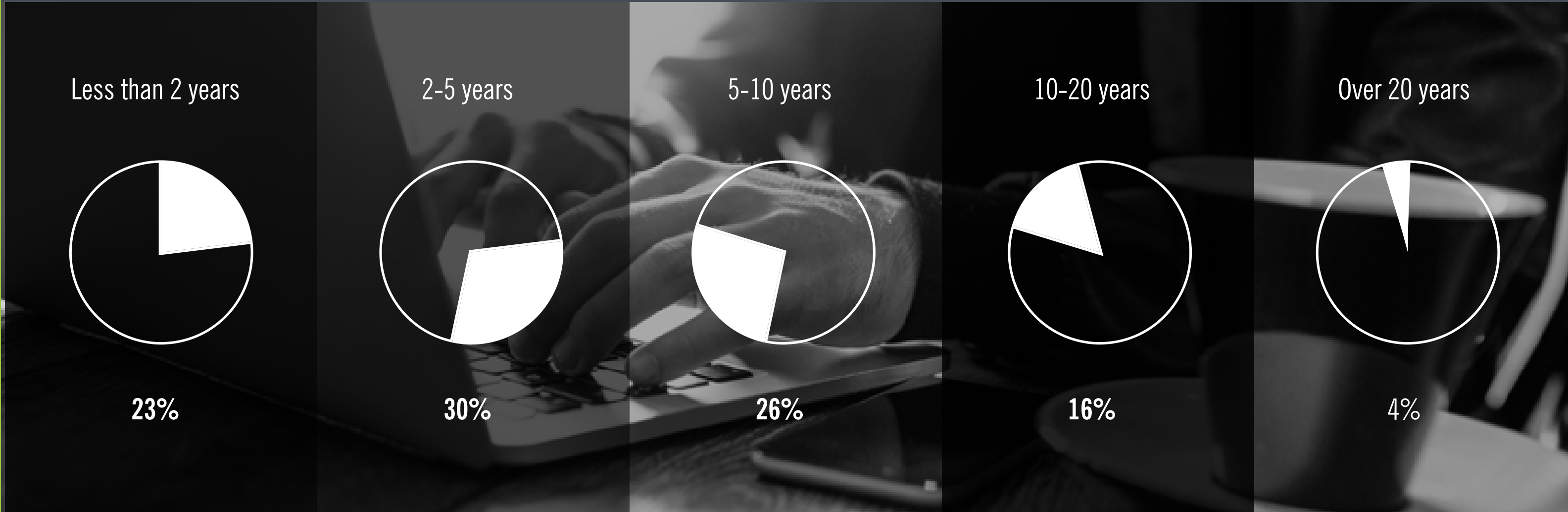
Percentage of business that is services based



MSP Business Trends

Among service providers, 53% have been in business fewer than 5 years, while 20% have been providing services for 10 years or longer. This indicates a shift from a resale-based business to a managed services model.

How long survey respondents have offered managed services:



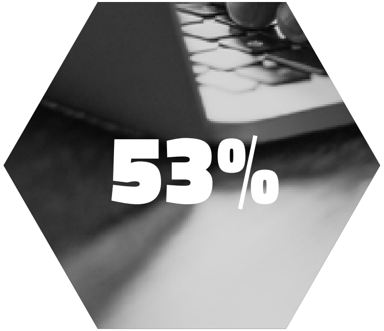
36% use remote monitoring and management (RMM) services, while over half use professional services automation (PSA) tools

RMM users

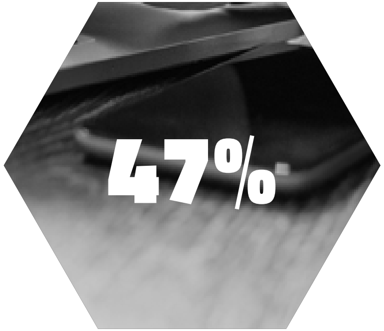
Yes

No

PSA users

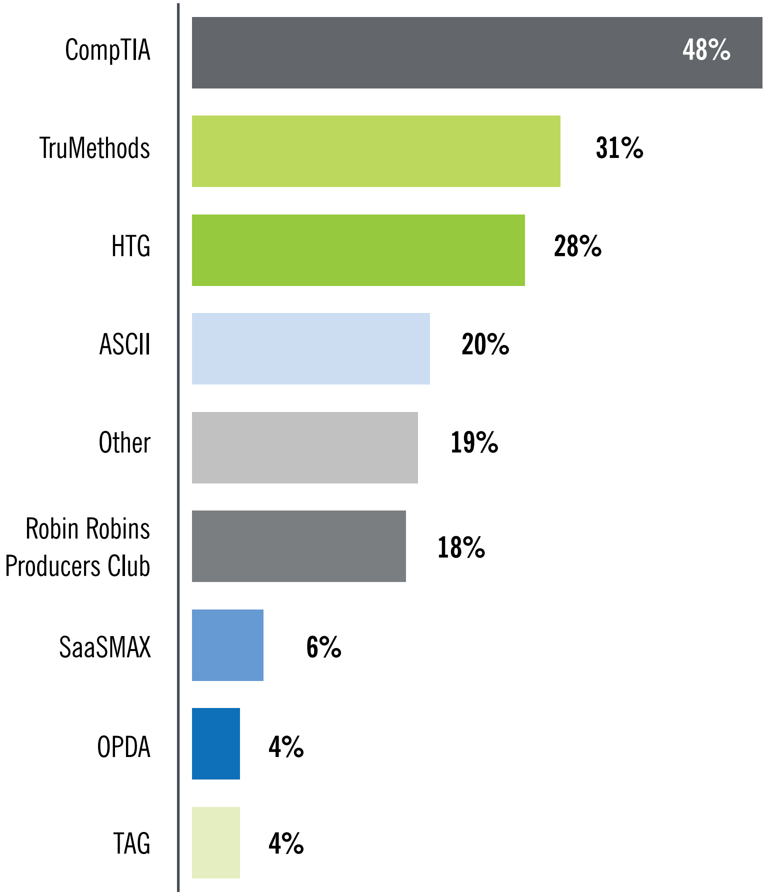


Yes



No

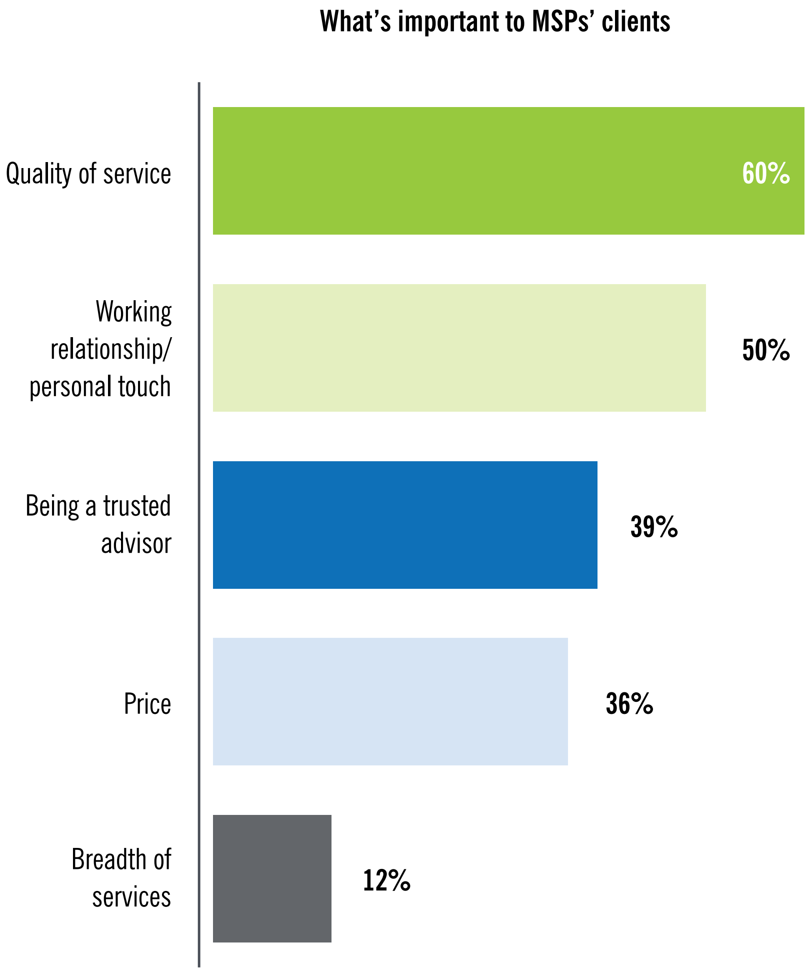
Breakdown of peer group affiliation



One quarter of respondents belong to peer groups, underscoring the importance of peer experience, word of mouth, and personal recommendations within the MSP space. In fact, many survey respondents were members of more than one group.

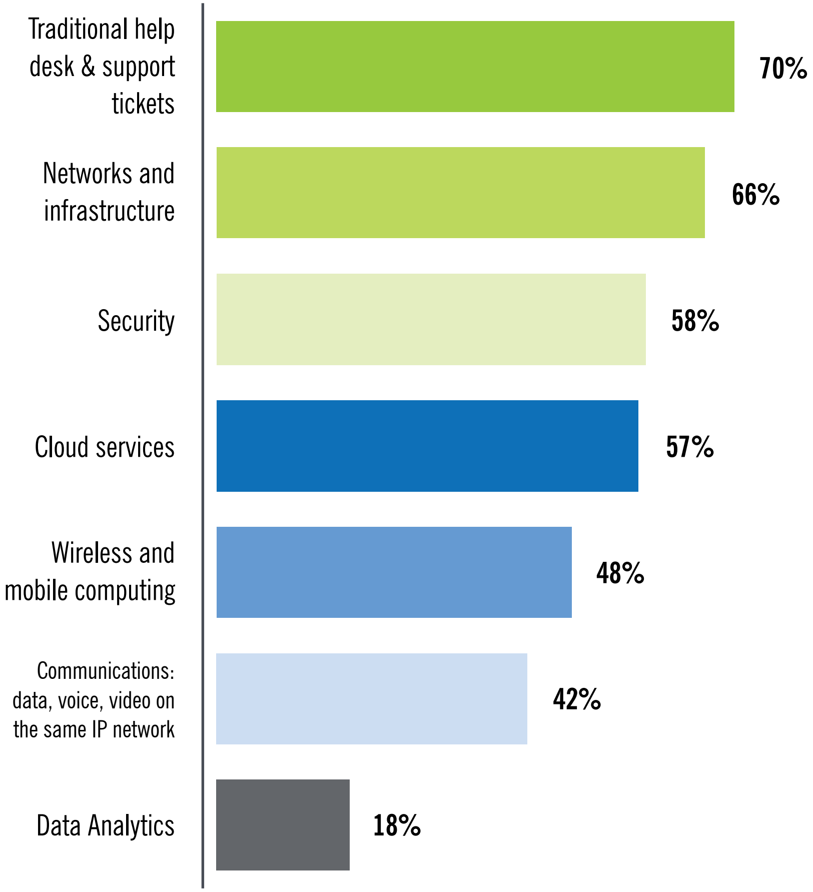
What Matters to End Clients

We asked respondents to check all that apply in this case. Overwhelmingly, the key takeaways from this data are that clients not only expect a certain level of quality in the services they receive, but also place a great deal of importance on the individual working relationship. Clients want to know that they're being taken seriously as people, and are being served by MSPs who understand their needs on a personal level. It's worth noting that the variety of services offered is considered to be at the bottom of their list of considerations when choosing an MSP.



The majority of service providers offer numerous services to their clients, often in a standardized bundle. This helps maintain consistency of quality and costs for both the clients and their MSP.

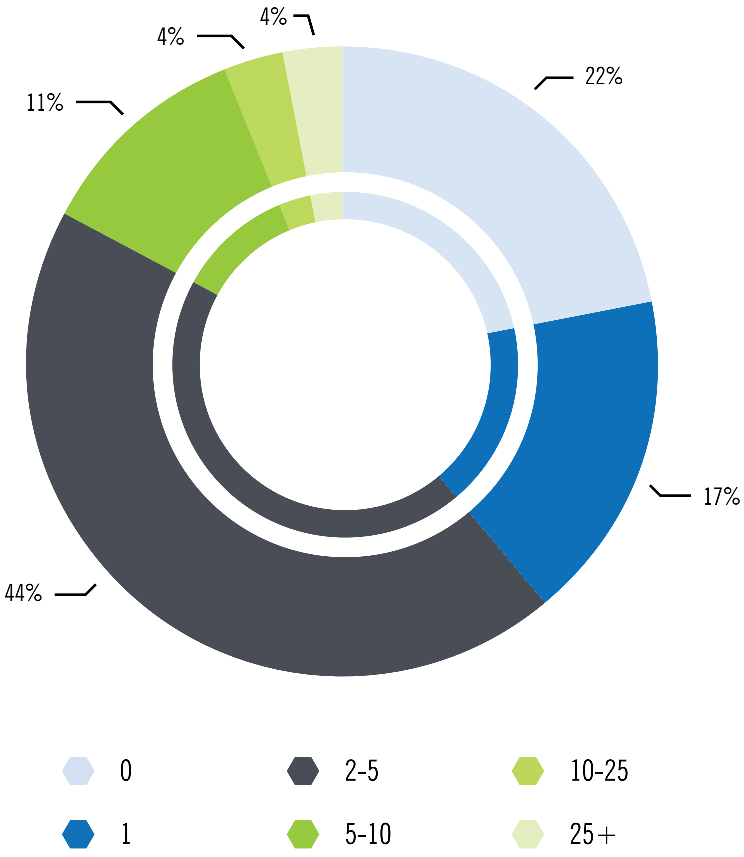
Types of services offered



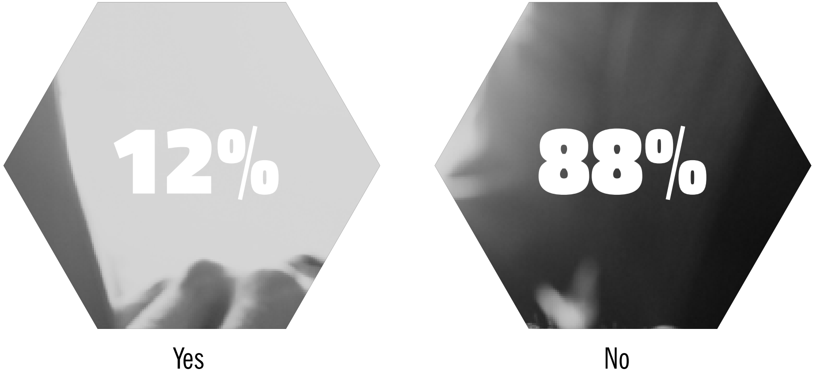
The Ransomware Problem

The moment you've all been waiting for: nearly 90% of MSPs surveyed reported that their clients had been hit by ransomware in the last year.

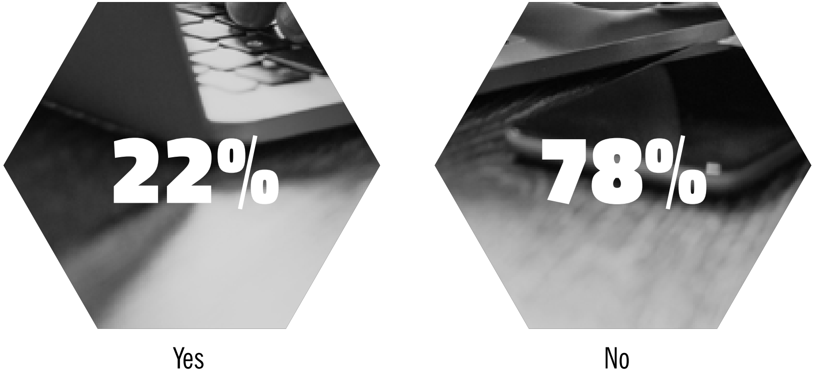
Number of clients hit by ransomware in the last 12 months.



MSPs who have paid the ransom for their clients' data



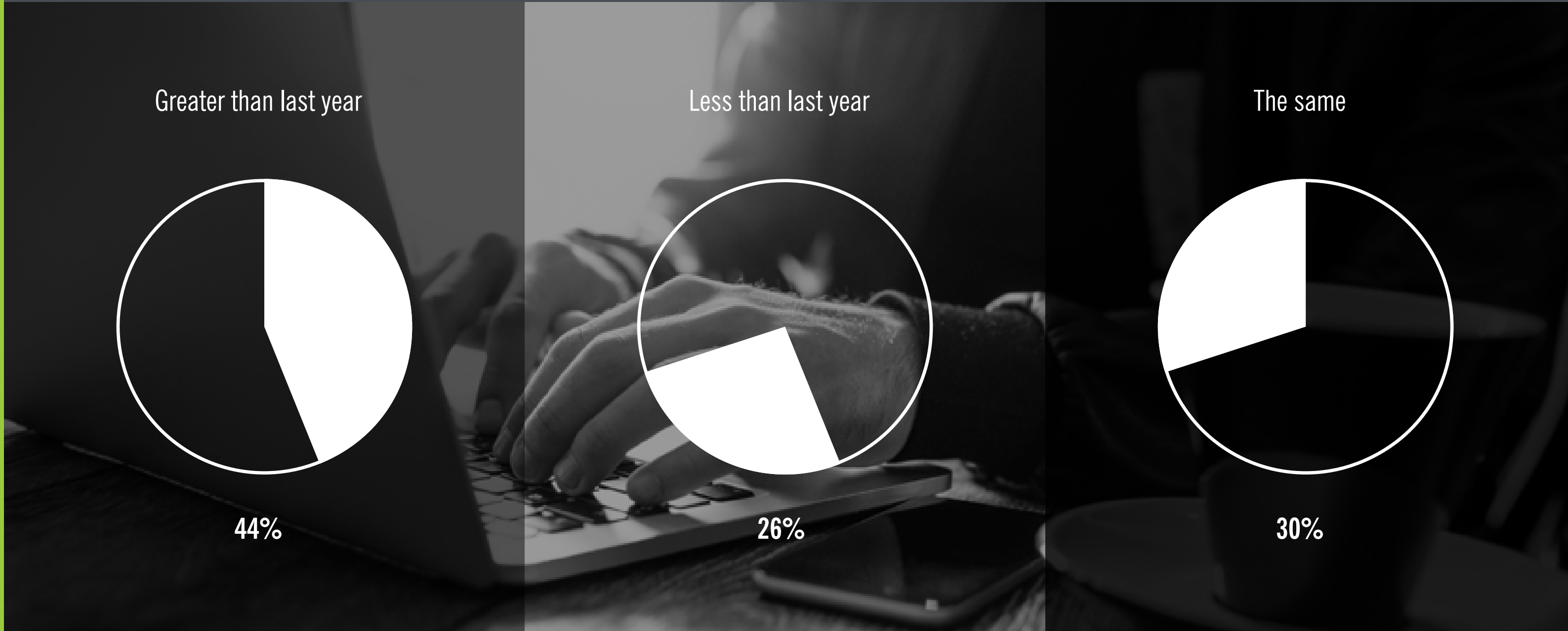
MSPs who are prepared to pay the ransom



Unfortunately, a ransomware attack can also be costly for MSPs. 1 in 8 MSPs reported having paid the ransom themselves, while nearly 1 in 4 answered that they were fully prepared to do so, should the need arise.

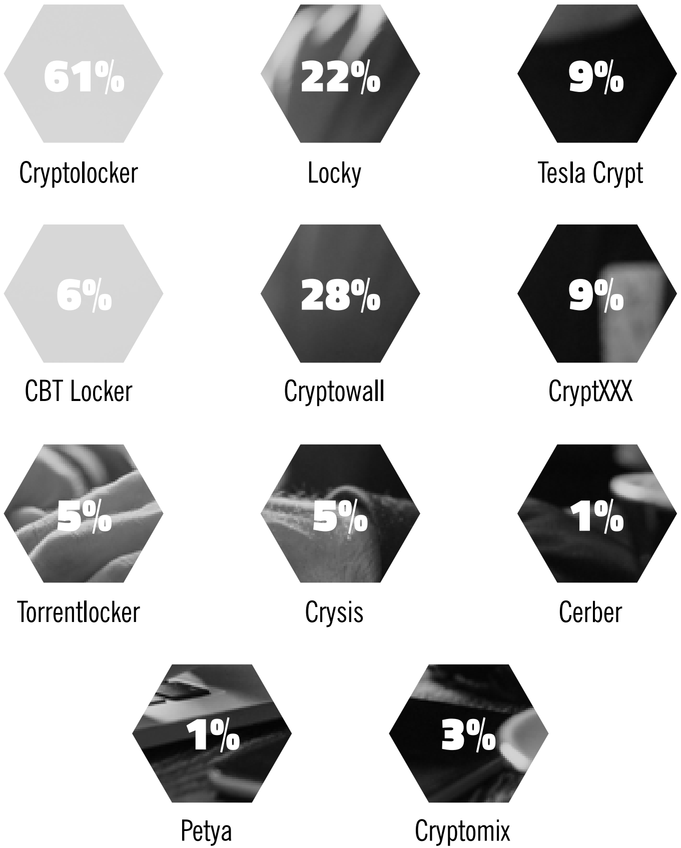
When it comes to ransomware, Webroot's own threat research shows that the trend won't be slowing down any time soon. It's far too effective and lucrative right now, and, with the advent of Ransomware-as-a-Service, it's easier than ever for criminals to take advantage of unsuspecting users.

Feelings about ransomware prevalence over the last 12 months, compared with the previous year:



Due to the repeated success of polymorphic ransomware, many MSPs have seen multiple variants making the rounds through their customer base.

Variety of ransomware types that have affected MSPs' clients

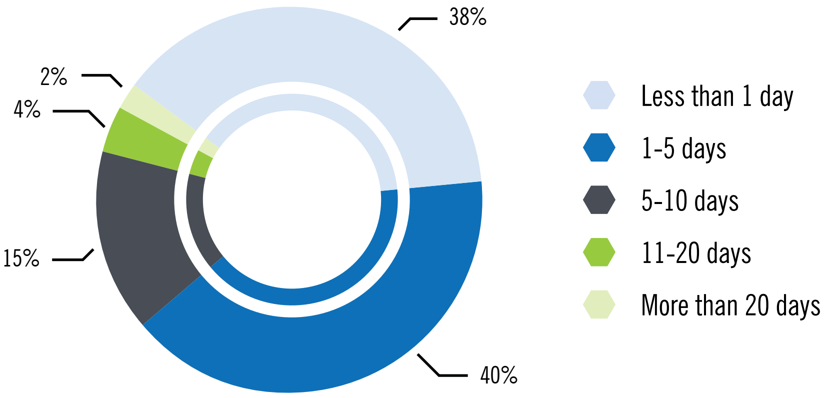


In addition to potential monetary cost, over 60% of MSPs have had to spend multiple days remediating the fallout of a ransomware attack in the last 12 months.

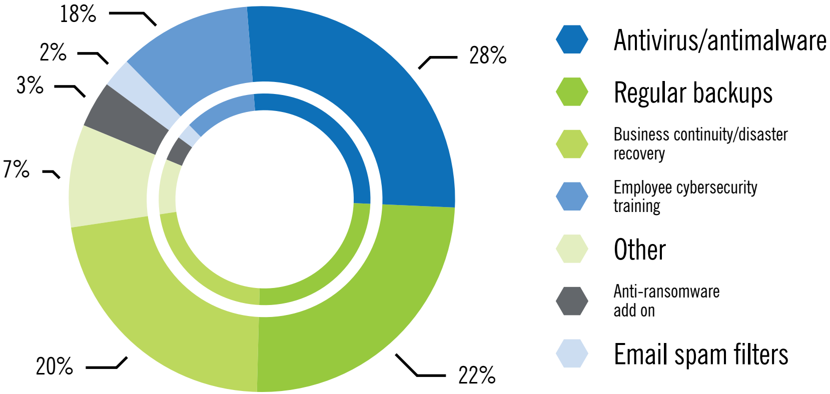
Survey respondents considered antivirus and antimalware software to be a crucial component of a ransomware defense strategy. However, the numbers indicate that MSPs believe regular backups and business continuity/disaster recovery planning are of nearly equal importance.

In response to the ransomware problem, many cybersecurity vendors have released so-called “anti-ransomware add-ons”. Judging by the data, however, today’s MSPs aren’t convinced of their value or effectiveness. Also worth noting is that user education remains a valuable part of a solid security setup.

Amount of time spent remediating ransomware in the past 12 months

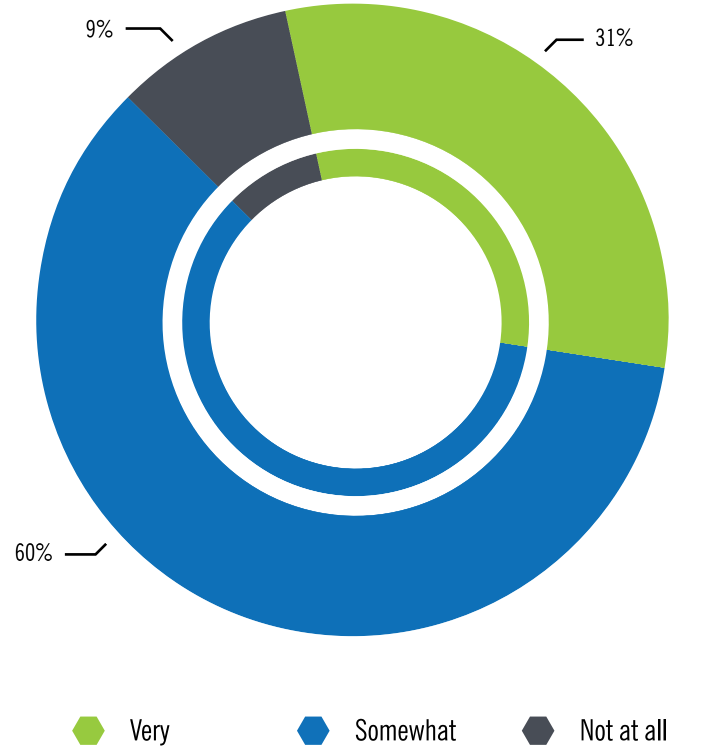


Ransomware protection strategies, in order of efficacy



Overall, nearly 70% reported a lack of confidence that their clients' endpoints are secure against a future ransomware attack.

Level of confidence that endpoints are protected against future ransomware attacks



RECOMMENDATIONS

To date, ransomware appears to be the most profitable malware type in history. Our threat research team expects that it will only become more destructive and more capable of self-replication, until it's able to hold entire networks hostage.

The sad truth is that ransomware authors are winning right now. As long as security infrastructure as a whole is weak, network hygiene practices are lacking, and organizations lean solely on their endpoint security for protection, they will continue to win. MSPs need to implement appropriate mitigation strategies and continue educating their users about cyberattacks and security best practices.

Here are 4 tips to protect your clients.

1

Educate Users *Teach them…*

a. Not to open emails from unknown senders with attachments or URLs
b. Not to open the attachments or URLs, even if they open the emails
c. How to spot suspicious emails, even when they appear to be from reputable contacts

2

Maintain Multi-Vector Protection

a. Implement reliable cloud-based antimalware, web filtering, and firewalls
b. Patch applications regularly, such as Adobe Reader, Java, and other plugins
c. Prevent user error with ad and pop-up blockers

3

Put Your OS to Work

a. Set up Windows® OS policy restrictions
b. Block VSS and disable Windows Script Hosting (VBS)
c. Filter executables (.exe) from emails whenever possible

4

Back up, Back up, Back up

a. Use a secure, cloud-based backup service regularly
b. Set up offline air gap backups with multiple copies of each file
c. Maintain up-to-date business continuity and disaster recovery

Finally, one of the most important steps an MSP can take to protect clients is to stay up-to-date on the latest ransomware developments. As malware in general continues to evolve, the best defense you can offer your clients is good information and solid cybersecurity practices.

WEBROOT®
Smarter Cybersecurity™

About Webroot

Webroot delivers next-generation network and endpoint security and threat intelligence services to protect businesses and individuals around the globe. Our smarter approach harnesses the power of cloud-based collective threat intelligence derived from millions of real-world devices to stop threats in real time and help secure the connected world. Our award-winning SecureAnywhere® endpoint solutions, BrightCloud® Threat Intelligence Services, and FlowScape® network behavioral analytics protect millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more, Webroot is headquartered in Colorado and operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity™ solutions at www.webroot.com.

385 Interlocken Crescent   Suite 800   Broomfield, Colorado   800.870.8102   webroot.com