Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **February 2021**
Sponsored by **Infoblox**

The Global Quest for Sustainable Work-From-Anywhere Security

Executive Summary

This report discusses the results of an in-depth survey on security issues conducted for Infoblox during the fourth quarter of 2020. The focus of the survey was to understand how endpoint security has evolved over the past 12 to 18 months and its acceleration from the COVID-19 pandemic, and how this is shaping the future of security. Conducted globally, the goal of the survey was to understand the long-term shifts in security strategies that are being undertaken to keep pace with the work-from-anywhere transformation that is a key element in the "new normal".

KEY TAKEAWAYS

Here are the key takeaways from the research:

- **Work from anywhere is here to stay**
  Our research found that the proportion of employees working from home increased nearly five-fold during the early days of the pandemic. Despite some employees moving back to an office environment since that time, work from anywhere remains at historically high levels and is expected to remain well above pre-pandemic levels over the long term.

- **Key business and security capabilities suffered during the pandemic**
  Some important capabilities have suffered during the pandemic. Most noteworthy among them were the ability to maintain access to existing services and the ability to expand digital transformation projects. Other key areas suffered, as well, including compliance with privacy obligations and the ability to report security readiness to boards of directors. Organizations in EMEA had significantly more problems in maintaining existing services than their counterparts in North America or the APAC region.

- **Most organizations were forced to make security changes**
  More than nine out of ten organizations made changes to their endpoint security following the commencement of the pandemic, and some organizations made major changes to their overall security posture as they equipped employees to work exclusively from home.

- **The shift to cloud security has accelerated**
  More than seven out of 10 organizations increased their use of cloud security to some degree, some doing so dramatically. Only five percent of organizations reported that they decreased their use of security in the cloud. Despite the increase, there is some level of opposition to cloud-based security, including its perceived higher-than-acceptable cost and some IT and security departments preferring the use of on-premises infrastructure.

- **The result is that security has improved**
  The overall security posture for in-office, work-from-home and traveling/remote employees has improved compared to their pre-pandemic levels. Security for work-from-home has improved the most, although it's important to note that this was the least secure environment for most organizations before the pandemic began. At the same time, security policies have also improved from their pre-pandemic levels.

- **VPN use grew dramatically**
  The use of VPN nearly doubled early in the Pandemic as teams looked to existing solutions for relief – from 37 percent of remote and traveling employees pre-pandemic to 65 percent in the early days of the lockdowns. And, use of VPN remains at nearly the same level several months later. Even after the pandemic has passed, IT and security decision makers anticipate that use of VPN will remain higher than it was before the pandemic.

More than seven out of 10 organizations increased their use of cloud security to some degree, some doing so dramatically.

- **VPN's problems were exposed and alternatives are being considered**
  Only 41 percent of IT and security decision makers agree or strongly agree with the notion that "VPN works well for us". As a result, most organizations are using or considering alternatives to VPN, including endpoint antivirus, DNS Security, and identity and access management solutions, among others. The research found that nearly three-fourths of IT and security decision makers consider DNS to be important to their overall security efforts and activities.

- **Remote worker visibility improved**
  Not surprisingly, with increased use of VPN, and greater focus on a growing remote worker population, the overall level of visibility that IT and security departments have into the activities of remote workers has grown. Prior to the pandemic, only seven percent of organizations had what they considered to be very good or excellent visibility into remote workers and devices. However, this more than doubled early in the pandemic and more than doubled again several months later. The most commonly used tools to gain visibility are log files, identity asset management solutions and Active Directory.

- **Few will roll back to previous practices**
  About three out of five organizations plan to maintain the changes they made to their security infrastructure after the pandemic started, but some will revert back to their old manner of doing things. The organizations that are more likely to retain the level of security changes they made are those with larger numbers of employees and/or those with a higher proportion of employees who will continue working from home.

ABOUT THE SURVEY

Osterman Research conducted an in-depth survey on behalf of Infoblox during October and November 2020:

- A total of 405 surveys were conducted with individuals who are involved in recommending, choosing or implementing their organizations' security solutions, practices and technologies.

- Surveys were conducted in three regions: North America (199 surveys); Europe, the Middle East and Africa (EMEA, 100 surveys); and Asia-Pacific (APAC, 106 surveys).

- The surveys were conducted with larger organizations: the minimum size of the organizations surveyed was 2,000 employees (1,000 in APAC). The median size of the organizations surveyed was 3.400 employees overall (4,000 in North America, 2,450 in EMEA, and 3,300 in APAC).

- A wide range of industries were included in the survey, most notably manufacturing (15 percent), business services (11 percent), energy and utilities (8 percent), financial services (8 percent) and biotech/pharma (8 percent).

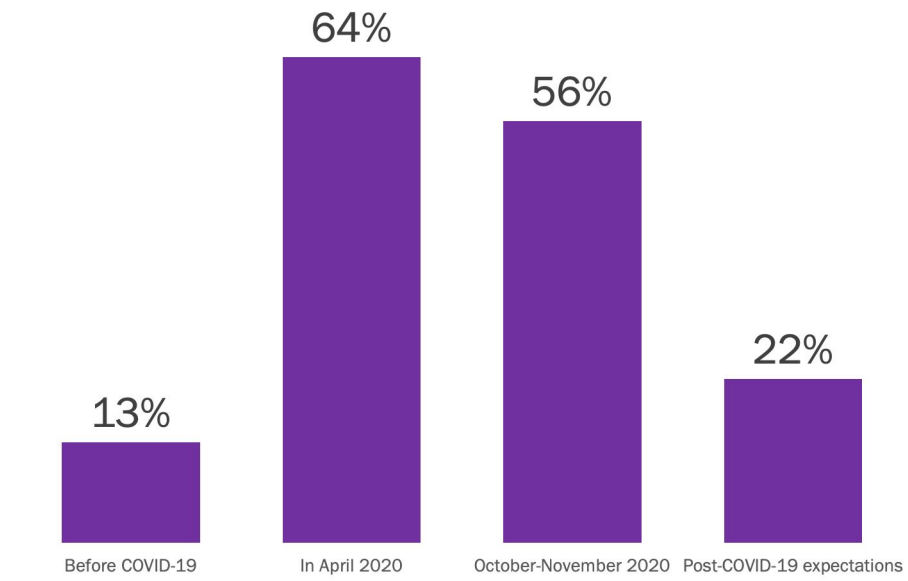
Nearly three-fourths of IT and security decision makers consider DNS to be important to their overall security efforts and activities.

Survey Findings

THE PANDEMIC WAS A CATALYST FOR MAJOR CHANGES

The various government lockdowns that were imposed in the early stages of the COVID-19 pandemic drove major changes in how employees work. As shown in Figure Q4, 13 percent of employees were working remotely prior to the pandemic, but this increased nearly five times to 64 percent in April 2020. At the time of the survey, some employees had moved back to their offices, but the vast majority (56 percent) were still working from home or otherwise remotely.

Figure Q4
Employees Working Remotely or From Home Before, During and After the COVID-19 Pandemic



Source: Osterman Research, Inc.

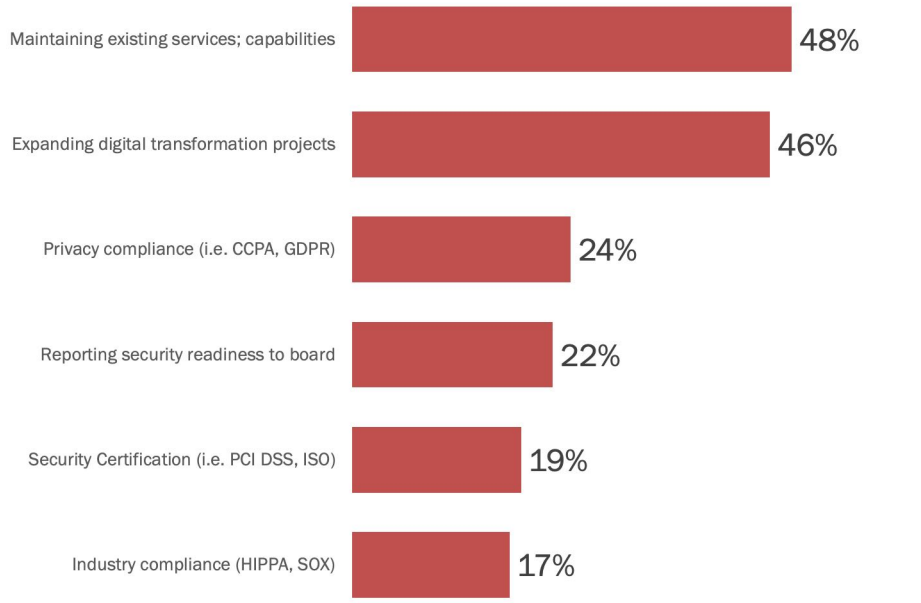
Interestingly, decision makers anticipate that 22 percent of employees will continue working from even after the pandemic has passed – significantly more employees working from home than prior to the pandemic. While many employees will simply want to remain at home even after the pandemic is long past, the work-at-home paradigm has proven popular as many employers look to reduce their costs of operations by leasing less office space, paying for less infrastructure to support employees, and so forth. The research found that long-term work-from-home will be more popular in North America (25 percent of employees will continue working from home post-pandemic) than in EMEA (16 percent) or APAC (20 percent). What we're seeing from this data is that there will be a net increase of 41 percent more employees working from home post-pandemic compared to pre-pandemic levels.

The various government lockdowns that were imposed in the early stages of the COVID-19 pandemic drove major changes in how employees work.

MANY CAPABILITIES SUFFERED DURING THE PANDEMIC

As shown in Figure Q9a, nearly one-half of organizations reported that their ability to maintain existing services and capabilities, and their ability to expand digital transformation projects, suffered significantly or a great deal as a result of the pandemic and the resulting lockdowns. Particularly with regard to digital transformation projects and initiatives, many of these were put on hold as IT and security teams scrambled to address the immediate needs of outfitting workers suddenly thrust into an at-home work environment, securing their access to corporate systems, and so forth.

Figure Q9a
Extent to Which Various Capabilities Suffered Following the COVID-19 Pandemic and the Increase in Remote Employees
Percentage responding "significantly" or "a great deal"



Source: Osterman Research, Inc.

Nearly one-half of organizations reported that their ability to maintain existing services and capabilities suffered significantly or a great deal.

THERE WERE SIGNIFICANT DIFFERENCES IN WHERE CAPABILITIES SUFFERED

We also discovered some significant differences in the extent to which various capabilities suffered during the pandemic in the different regions we surveyed. For example, as shown in Figure Q9b, there was a significantly greater impact in maintaining existing services in EMEA, as well as on digital transformation projects, than in the other two regions. However, there was much less difficulty in EMEA than in North America or APAC in terms of satisfying industry compliance requirements.

Figure Q9b
Extent to Which Various Capabilities Suffered Following the COVID-19 Pandemic and the Increase in Remote Employees, by Region
Percentage responding "significantly" or "a great deal"

Capability	Overall	North America	EMEA	APAC
Maintaining existing services; capabilities	48%	43%	67%	41%
Expanding digital transformation projects	46%	39%	60%	45%
Reporting security readiness to board	22%	22%	16%	28%
Privacy compliance (i.e., CCPA, GDPR)	24%	21%	18%	35%
Industry compliance (HIPPA, SOX)	17%	22%	8%	17%
Security Certification (i.e., PCI DSS, ISO)	19%	17%	18%	22%

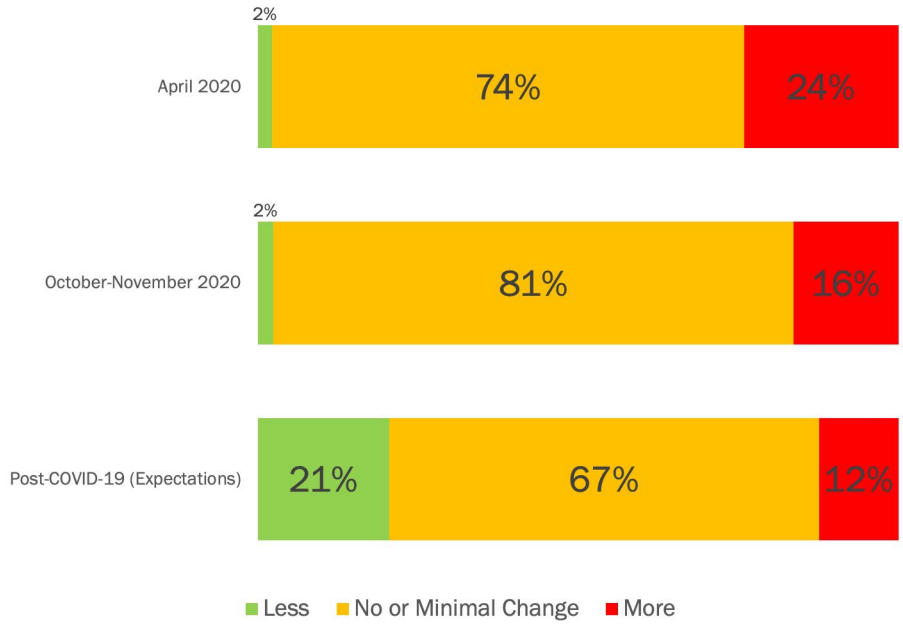
Source: Osterman Research, Inc.

We also discovered some significant differences in the extent to which various capabilities suffered during the pandemic.

INCIDENTS SPIKED EARLY DURING THE PANDEMIC

Compared to their pre-pandemic experience, 24 percent of IT and security decision makers reported that the number of security incidents worsened early on, while most of the remaining organizations felt that not much changed, as shown in Figure Q23. Six months later, those reporting that things were worse in the midst of the pandemic was still high – 16 percent – but a larger proportion reported that the number of security incidents was more in line with their pre-pandemic experience. Long-term, however, IT and security decision makers anticipate that the number of security incidents will fall substantially, growing from just two percent of organizations in 2020 to 21 percent.

Figure Q23
How the Number of Incidents Have Changed During and After the COVID-19 Pandemic



Source: Osterman Research, Inc.

Compared to their pre-pandemic experience, 24 percent of IT and security decision makers reported that the number of security incidents worsened early on.

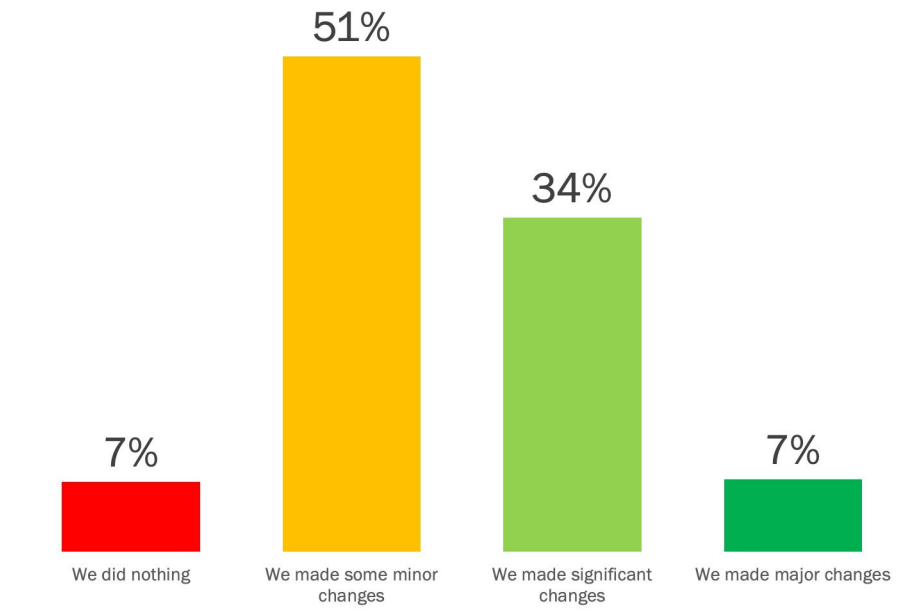
This data points to the fact that organizations made significant improvements to their security infrastructures – as discussed later in this report – which helped to mitigate increased activity among bad actors.

North American organizations are the least optimistic among those in the three regions we surveyed in the context of how things will improve post-pandemic. We found that while 29 percent of organizations in APAC and 23 percent of organizations in EMEA believe they will experience fewer security incidents post-pandemic compared to pre-pandemic, only 15 percent of North American organizations anticipate a reduction.

MOST ORGANIZATIONS MADE SECURITY CHANGES

As shown in Figure Q7, the vast majority of the organizations that we surveyed made changes to improve endpoint security after the pandemic began, with about two in five organizations making either significant or major changes to their infrastructure. Given that about five times more knowledge workers were now working from home or otherwise remotely than before the pandemic, IT and security teams were forced into making key changes in endpoint security practices and technologies with little time to make these changes.

Figure Q7
Efforts to Improve Endpoint Security After the COVID-19 Pandemic Began



Source: Osterman Research, Inc.

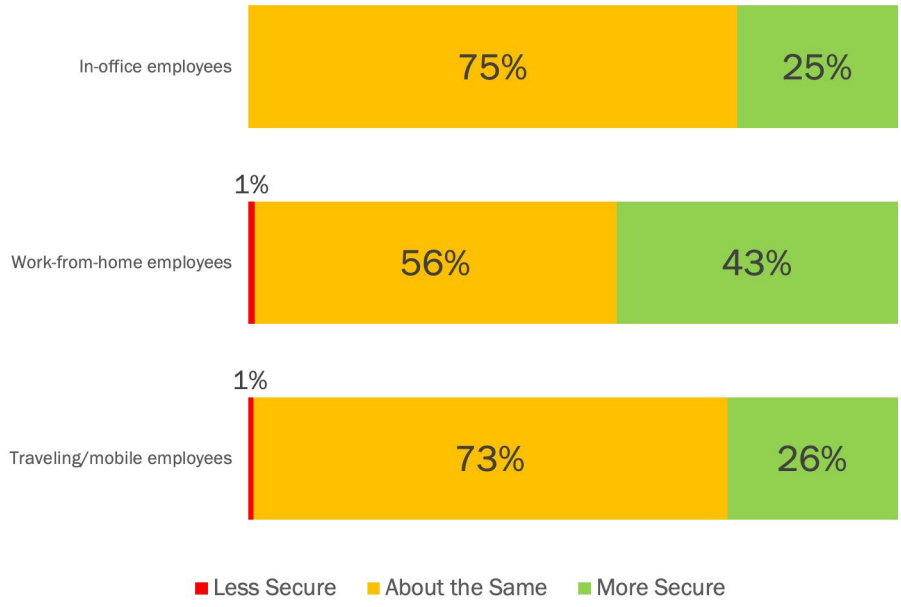
Interestingly, we found very little variability in the data shown above by region – all three were surprisingly consistent across the four categories of change.

IT and security teams were forced into making key changes in endpoint security practices and technologies with little time to make these changes.

HAS SECURITY IMPROVED SINCE THE PANDEMIC?

Immediately following the lockdowns that began in the March-April 2020 timeframe, IT and security departments struggled to outfit employees with the infrastructure they needed to work from home. However, their efforts have paid off handsomely in many cases: as shown in Figure Q5, many security decision makers believe that their security posture has actually improved as of the October-November 2020 timeframe compared to the pre-pandemic situation. This is particularly true for work-from-home employees, but we also found significant improvements in security for in-office and traveling/mobile employees.

Figure Q5
Current User Security Compared to Pre-COVID-19 Security



Source: Osterman Research, Inc.

Immediately after the lockdowns started, security suffered.

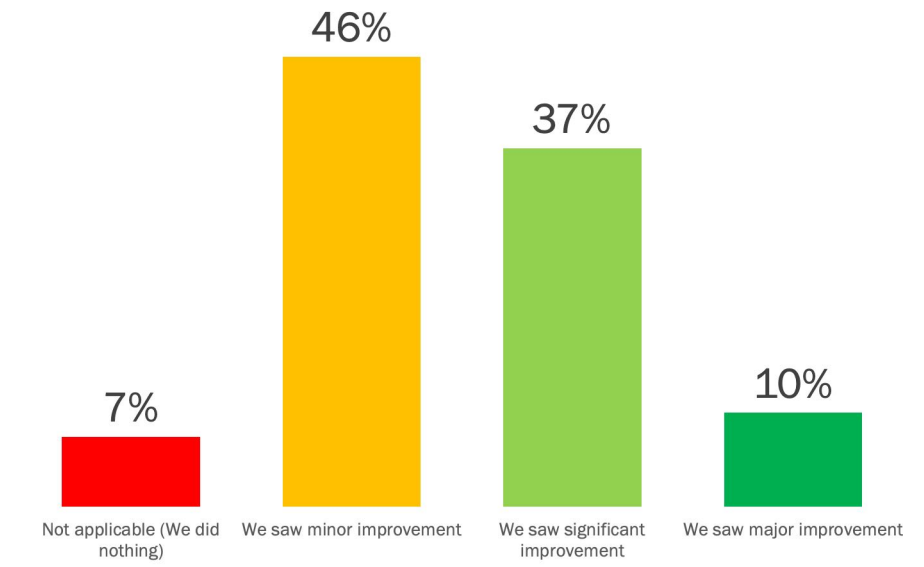
We did not find significant differences across the three regions we surveyed.

It's important to note that immediately after the lockdowns started, security suffered. An April 2020 Osterman Research survey found that both compliance and security capabilities dropped during the early days of the work-from-home phenomenon. For example, while 64 percent of organizations reported that they agree with the idea they were doing an excellent at job maintaining compliance with their various obligations before the pandemic, that level of agreement fell to 56 percent in April 2020. Similarly, while 56 percent were in agreement that they were doing an excellent job at blocking security threats prior to the pandemic, that figure dropped to 49 percent in April 2020.

HOW EFFECTIVE WERE THE CHANGES IN ENDPOINT SECURITY?

The changes that were made in an attempt to improve endpoint security paid off, as shown in Figure Q8. While 46 percent of organizations saw minor improvements as a result of the changes, 37 percent saw significant improvements and one in ten saw what they consider to be major improvements.

Figure Q8
Effectiveness of Changes at Improving Endpoint Security



Source: Osterman Research, Inc.

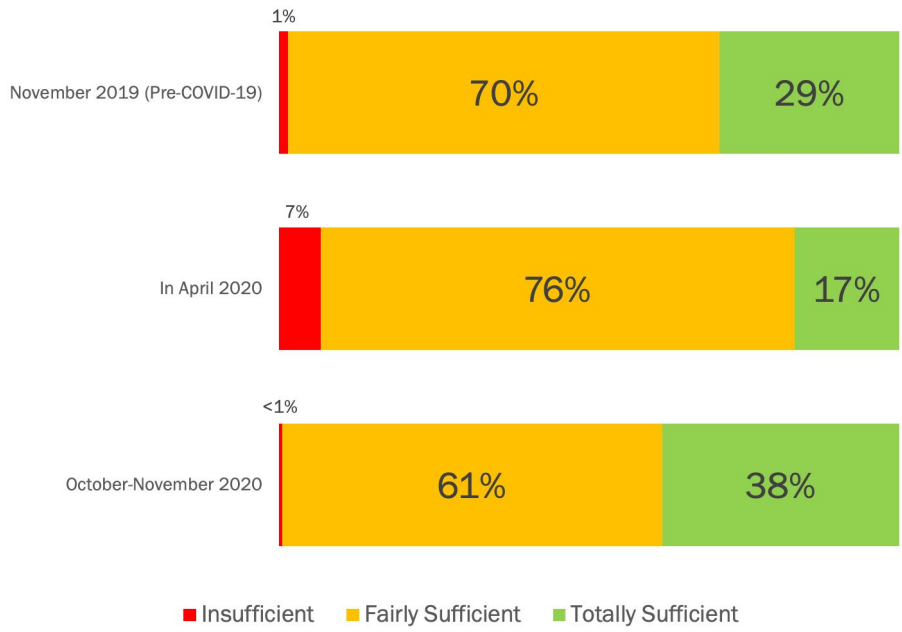
We did discover some differences between the regions in terms of how effective their changes to endpoint security were: the percentage of organizations in North American that experienced major improvements to endpoint security totaled eight percent, while in EMEA it was nine percent, but a much more impressive 14 percent in APAC.

The changes that were made in an attempt to improve endpoint security paid off.

SECURITY POLICIES HAVE IMPROVED

Not surprisingly, the sufficiency of corporate security policies took a fairly serious nosedive during the early days of the pandemic and the ensuing lockdowns. As shown in Figure Q6, while 29 percent of decision makers prior to the pandemic considered that their security policies were totally sufficient or nearly so, this dropped significantly to only 17 percent in April 2020, shortly after the pandemic was in full swing. Six months later, however, security policies have improved to the point where they are perceived as actually better than they were prior to the pandemic.

Figure Q6
Sufficiency of Security Policies Before and During the COVID-19 Pandemic



Source: Osterman Research, Inc.

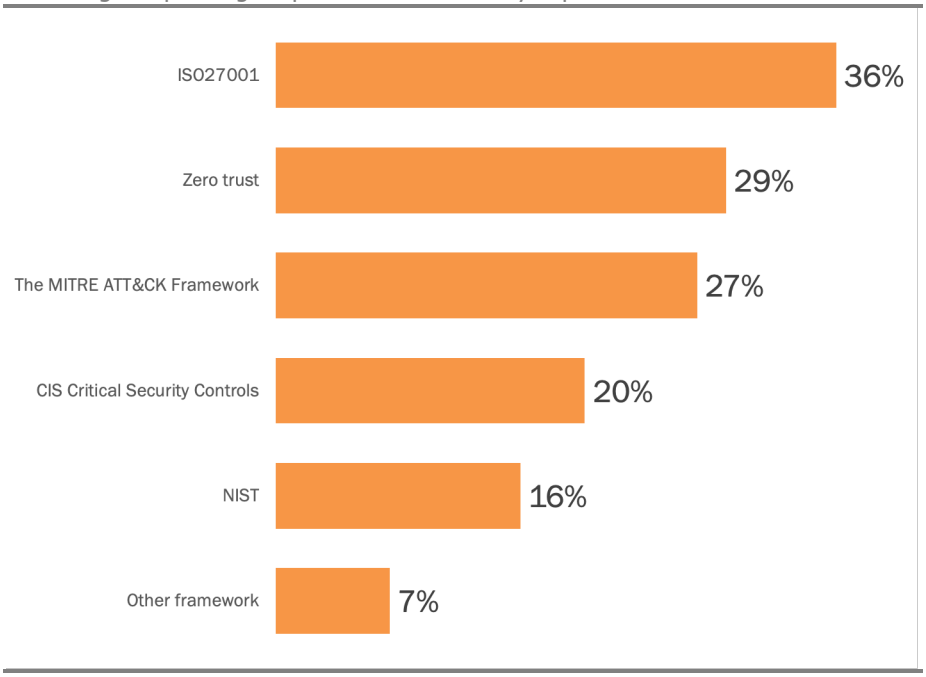
We found some differences among the three regions that were surveyed in terms of the percentages of decision makers that considered their security policies to be sufficient during the three time periods shown in the figure. However, we found the same pattern across all three regions: a significant drop in the perception that security policies were adequate from November 2019 to April 2020, followed by a rebound in the October-November 2020 timeframe that exceeded the levels from a year earlier.

The sufficiency of corporate security policies took a fairly serious nosedive during the early days of the pandemic and the ensuing lockdowns.

ISO 27001 AND ZERO TRUST ARE IMPORTANT

ISO 27001 and Zero Trust initiatives are considered to be important or extremely important by more than one-third of the organizations surveyed, as shown in Figure Q10. Other capabilities, including the MITRE ATT&CK Framework, CIS Critical Security Controls and NIST requirements are considered as less important.

Figure Q10
Importance of Various Capabilities
Percentage responding "important" or "extremely important"



Source: Osterman Research, Inc.

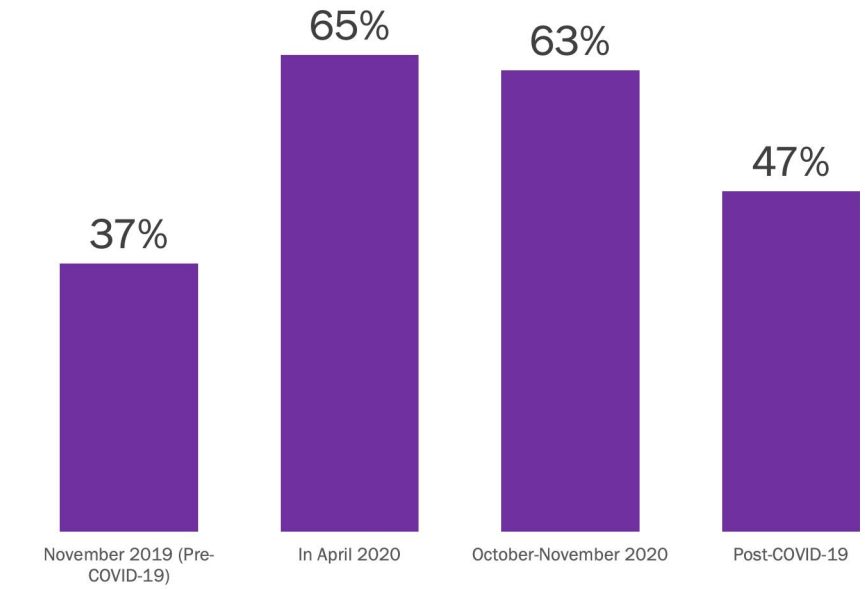
As we expected, there were significant differences among the regions surveyed in terms of the importance of these capabilities. For example, while NIST compliance is considered important or extremely important to 28 percent of North American organizations, these figures drop to three and four percent, respectively, in EMEA and APAC. While ISO 27001 is more consistently important across all three regions, Zero Trust is not: the latter is considered to be important or extremely important to 35 percent of the organizations surveyed in North America, compared to only 24 percent in APAC and 18 percent in EMEA.

ISO 27001 and Zero Trust initiatives are considered to be important or extremely important by more than one-third of the organizations surveyed.

VPN USE HAS GROWN SIGNIFICANTLY

As a tested and well understood technology, we verified that the use of VPN grew significantly by remote (mostly work-from-home) and traveling employees shortly after the pandemic started, increasing from 37 percent of the workforce in November 2019 to 65 percent by April 2020, as shown in Figure Q11. Six months later, use of VPN was still much higher than it was pre-pandemic, nearly at the same level as it was shortly after the lockdowns began. Long term, use of VPN is expected to be higher than it was pre-pandemic, but significantly lower than it was in the fourth quarter of 2020.

Figure Q11
Percentage of Remote and Traveling Workforce Using VPN During Various Periods



Source: Osterman Research, Inc.

We did not find major differences across the three regions that we surveyed in terms of how many remote and traveling employees use VPN, although we did find that the pre-pandemic use of VPN was highest in North America (42 percent) and lowest in EMEA (28 percent). Use of VPN by remote and traveling employees in April and October-November 2020 across the regions was fairly consistent, although use is falling faster in EMEA than in the other two regions. Later areas of the survey were able to shed light on why VPN does not appear to be a long-term viable solution for many.

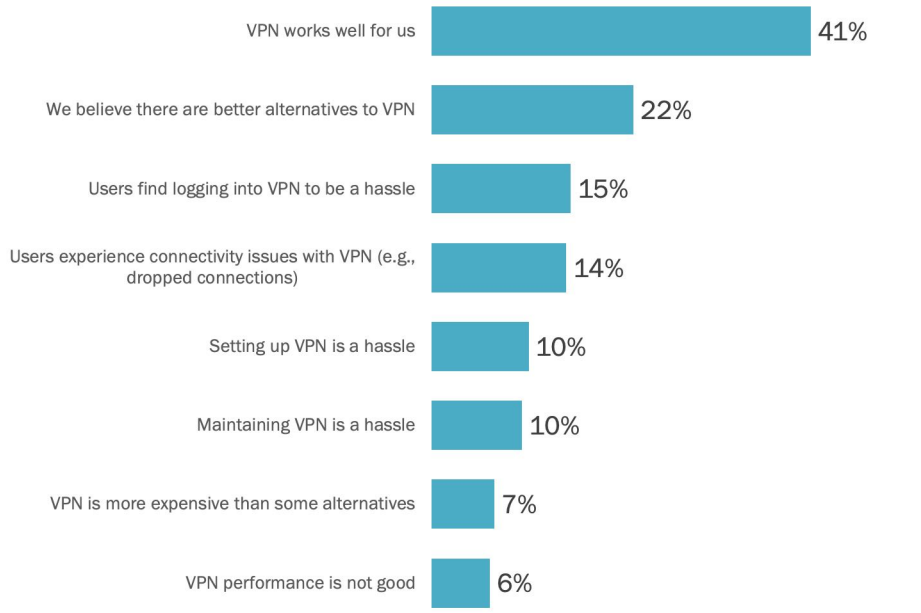
As a tested and well understood technology, we verified that the use of VPN grew significantly by remote (mostly work-from-home) and traveling employees.

OPINIONS ABOUT VPN VARY WIDELY

As shown in Figure Q12, two in five decision makers agree or strongly agree that VPN works well for their remote and traveling employees, while 22 percent agree to this extent that there are better alternatives to the current use of VPN.

That said, we found a fairly significant proportion of decision makers who consider VPN to be a less than optimum solution: for example, 15 percent of those surveyed agree or strongly agree that users find logging into VPN to be a "hassle" – when we add in those who mildly agree with that statement, the figure jumps to 46 percent. Similarly, when we add in those who mildly agree with the statement that users experience connectivity issues with VPN, the total increases to 48 percent of those surveyed.

Figure Q12
Agreement With Various Statements About VPN
Percentage responding "agree" or "strongly agree"



Source: Osterman Research, Inc.

We found a fairly significant proportion of decision makers who consider VPN to be a less than optimum solution.

We discovered some interesting regional differences in the perception of VPN. For example, while 48 percent of the North American respondents agree or strongly agree that VPN works well for them, this figure is only 38 percent in APAC and 28 percent in EMEA. Decision makers in North America and EMEA are more likely to agree or strongly agree that there are better alternatives to VPN – 21 percent and 25 percent, respectively – than their counterparts in APAC (19 percent).

THERE ARE NUMEROUS CONSIDERATIONS FOR REDUCING USE OF VPN

The research found that there are numerous solutions that are being used, or could be used, to reduce the use of VPN, including endpoint security solutions, DNS security, and identity and access management solutions, as shown in Figure Q13-15. Moreover, among the solutions that will be acquired or deployed by the fourth quarter of 2021, the leading solutions are Cloud Application Security Brokers (32 percent), DNS security (26 percent), and next-generation firewalls (22 percent).

Figure Q13-15
Technologies That are or Could be Used to Reduce Usage of VPN, to Support the Current Security Posture, and That Will be Deployed or Expanded During the Next 12 Months

Technology	To Reduce Reliance on VPN to Secure Remote Workers	Currently Used to Support Security Posture	To be Acquired/ Deployed or Expanded
Anti-virus or anti-malware solution installed on endpoints	64%	65%	13%
DNS Security	56%	61%	26%
IAM (Identity Access and Management)	45%	33%	14%
NGFW (Next-Gen Firewall)	39%	26%	22%
SEG (secure email gateway)	37%	32%	11%
SWG (Secure web gateway)	32%	23%	10%
CASB (Cloud Application Security Broker)	32%	22%	32%
Server/host protection solutions	30%	28%	17%
Web application security solutions	28%	19%	17%
Web application firewall (WAF)	25%	18%	11%
EDR solution	24%	13%	12%
SIEM	23%	18%	9%
Threat Sandboxing	20%	15%	12%
Host-based intrusion protection system	20%	17%	10%
Threat intelligence feeds/blocklists	18%	15%	12%
DLP	15%	11%	8%
Host-based runtime application self-protection	13%	10%	8%
SOAR	10%	4%	4%

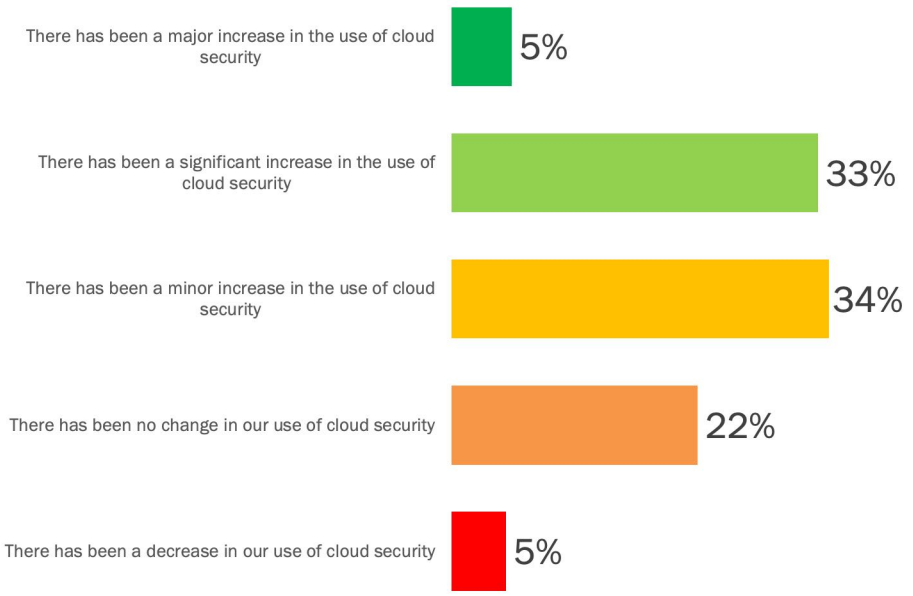
Source: Osterman Research, Inc.

There are numerous solutions that are being used, or could be used, to reduce the use of VPN.

USE OF CLOUD SECURITY HAS GROWN SIGNIFICANTLY

As shown in Figure Q16, more than seven in 10 organizations surveyed increased their use of cloud security solutions during the pandemic compared to before the pandemic began. In fact, nearly two in five organizations increased their use of cloud security solutions significantly or more so during the pandemic.

Figure Q16
Current Use of Cloud Security Compared to Before the COVID-19 Pandemic



Source: Osterman Research, Inc.

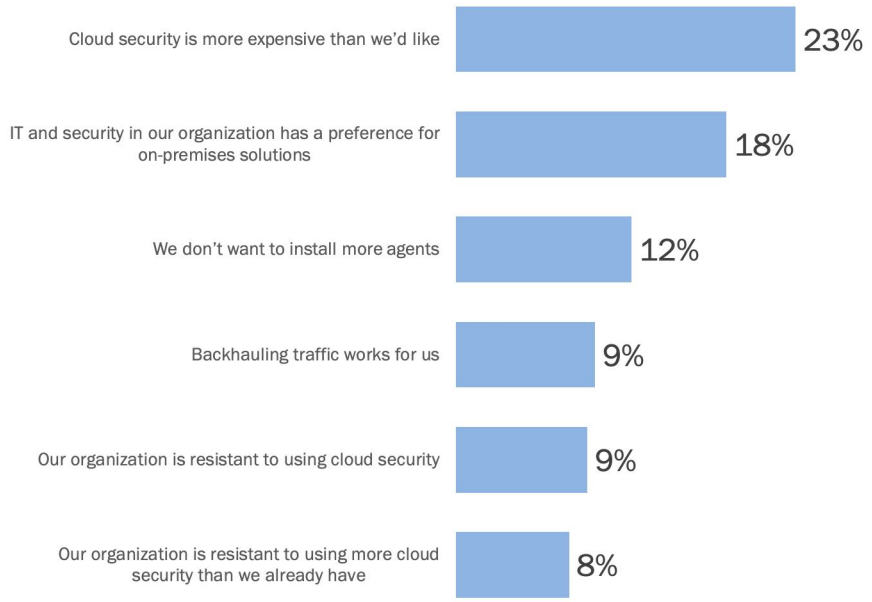
Organizations in APAC and EMEA adopted additional cloud security capabilities at a greater rate than their North American counterparts. For example, 45 percent of organizations in APAC saw either a significant or major increase during the pandemic as compared to 43 percent in EMEA and only 33 percent in North America.

Nearly two in five organizations increased their use of cloud security solutions significantly or more so during the pandemic.

THERE IS SOME RESISTANCE TO CLOUD SECURITY

Our research discovered that there is resistance to the use of cloud security on the part of some decision makers. As shown in Figure Q17, 23 percent of those surveyed agree or strongly agree that cloud security is too expensive, and 18 percent have a preference for on-premises security solutions.

Figure Q17
Agreement With Various Statements About Security Issues
Percentage responding "agree" or "strongly agree"



Source: Osterman Research, Inc.

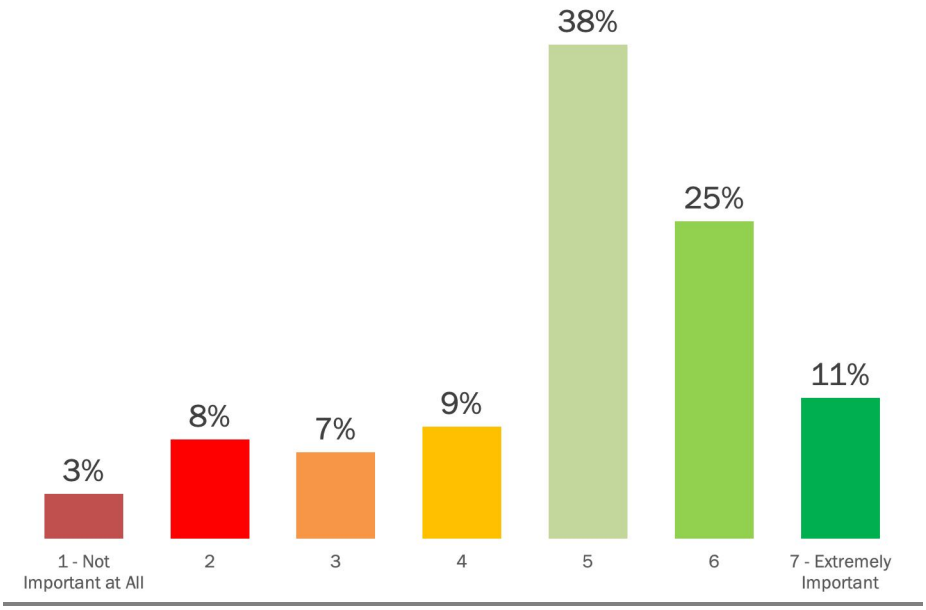
There is resistance to the use of cloud security on the part of some decision makers.

One explanation for the more modest increase in the use of cloud security in North America following the pandemic may be the higher level of resistance to its use. For example, while 11 percent of decision makers in North America agree or strongly agree that their organizations are resistant to the use of cloud security, these figures are only nine percent and five percent in EMEA and APAC, respectively. Interestingly, however, there is more preference for on-premises solutions in EMEA and APAC than in North America: while only 15 percent of North American decision makers agree or strongly agree that their organization has a preference for on-premises solutions, these figures are 19 percent in APAC and 25 percent in EMEA.

DNS IS CONSIDERED IMPORTANT

Seventy-four percent consider DNS to be important to their overall cybersecurity efforts. As shown in Figure Q18, 38 percent consider DNS to be modestly important, while 25 percent consider it to be important and 11 percent consider it to be extremely important.

Figure Q18
Importance of DNS to Overall Cybersecurity Efforts and Activities



Source: Osterman Research, Inc.

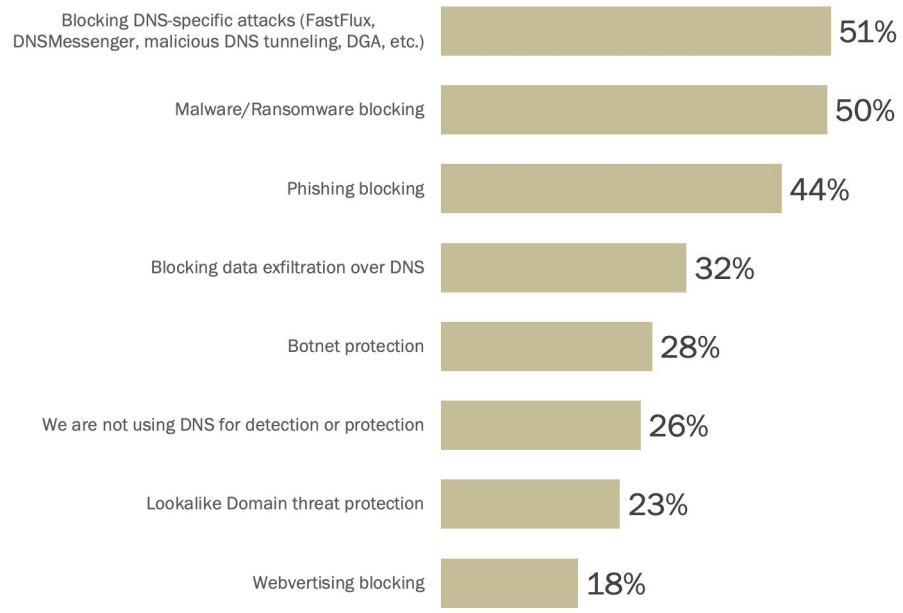
While 36 percent overall consider DNS to be important or extremely important, this figure was slightly higher in North America at 38 percent, and slightly lower in APAC and EMEA, at 36 percent and 30 percent, respectively. At the other end of the spectrum, only five percent of respondents in APAC consider DNS to be of low importance or not important at all versus 12 percent in North America and 16 percent in EMEA.

Seventy-four percent consider DNS to be important to their overall cybersecurity efforts.

HOW IS DNS USED FOR DETECTION OR PROTECTION?

DNS is used for a wide variety of detection and protection purposes, most notably blocking DNS specific attacks like FastFlux and DNSMessenger, as well as blocking ransomware and other types of malware, and blocking phishing attempts. However, 26 percent of respondents indicated that they are not using DNS for any threat detection or protection purpose today. But this may be related to why 26 percent of respondents indicated in Q13-15 that they plan to acquire/deploy or expand their DNS security in the future.

Figure Q19
Threat Types That Organizations are Detecting or Protecting Against With the Use of DNS



Source: Osterman Research, Inc.

DNS is used for a wide variety of detection and protection purposes.

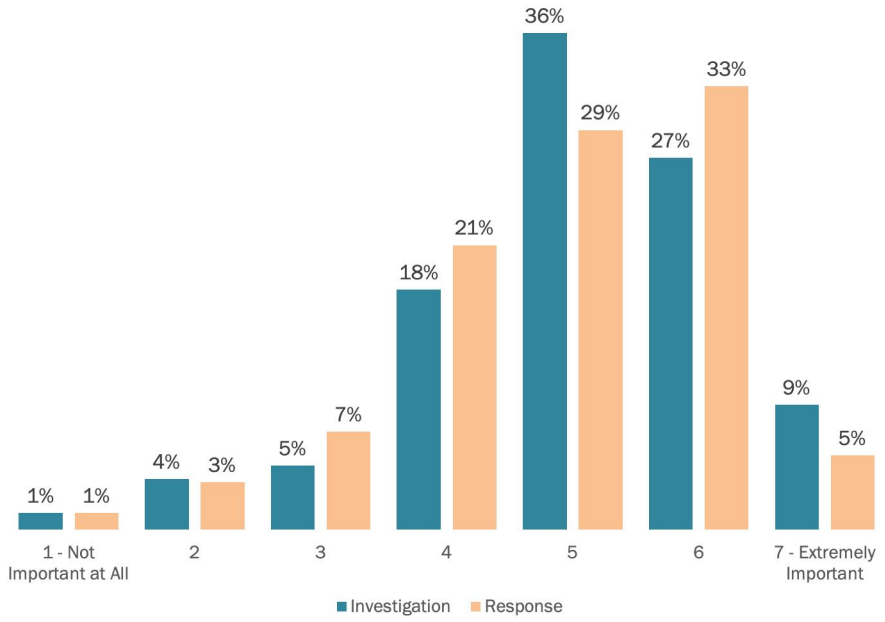
We found some regional differences in the use of DNS. For example:

- In North America only 23 percent of organizations are not using DNS for detection or protection, whereas this figure is 25 percent in APAC and 34 percent in EMEA.
- In North America, 55 percent of organizations are using DNS to block DNS-specific attacks, but this drops to 49 percent in EMEA and 45 percent in APAC.

DNS ACTIVITY VISIBILITY IS IMPORTANT FOR INCIDENT RESPONSE

As shown in Figure Q20, most organizations consider DNS activity visibility to be relatively important in the context of their investigation and response capabilities. Thirty-six percent of organizations consider DNS activity visibility to be important or extremely important to their investigative capabilities, while 38 percent consider DNS activity visibility to be this important for their response activities.

Figure Q20
Importance of DNS Activity Visibility in the Context of Investigation and Response



Source: Osterman Research, Inc.

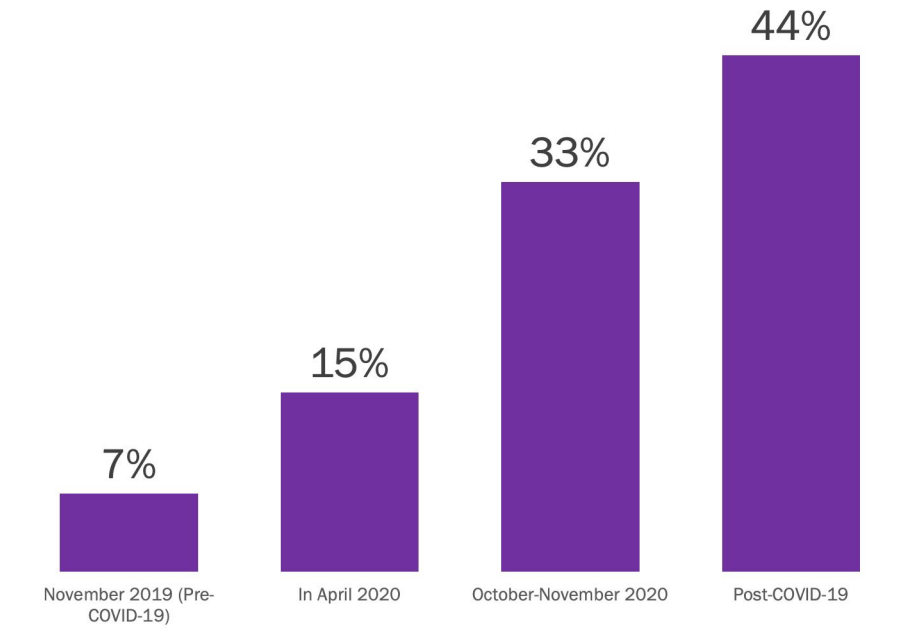
We did not find large differences between North America, EMEA and APAC in the context of the importance of DNS activity visibility for investigation and response activities. In fact, the range of responses for those who consider DNS activity visibility to be important or extremely important was 31-40 percent for investigation, and 36-41 percent for response.

Thirty-six percent of organizations consider DNS activity visibility to be important or extremely important to their investigative capabilities over time.

VISIBILITY IS INCREASING

When decision makers were asked about the level of visibility they had, currently have, and expect to have for remote workers, we found that visibility has been increasing steadily over time. As shown in Figure Q21, only seven percent of respondents considered that they had either very good or excellent visibility into the activities of remote workers just prior to the pandemic. However, the proportion that considered their visibility this good more than doubled by early in the pandemic and more than doubled again six months later. After the pandemic is over, decision makers anticipate even more gains for visibility into their remote workers' activities.

Figure Q21
Level of Visibility into Remote Worker Activity Before, During and After the COVID-19 Pandemic
Percentage responding "very good" or "excellent visibility"



Source: Osterman Research, Inc.

While remote worker visibility is increasing, it's still not nearly as good as it should be.

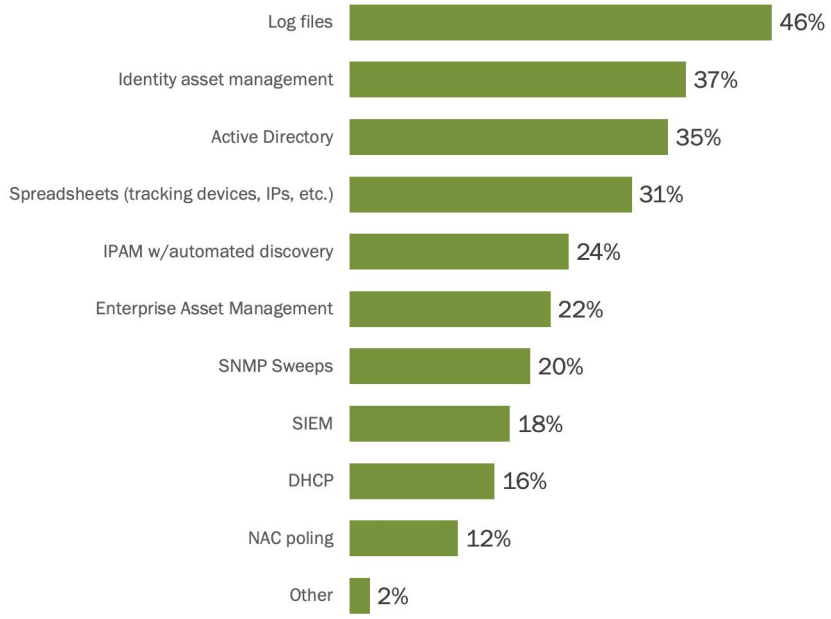
It's important to note that while remote worker visibility is increasing, it's still not nearly as good as it should be. For example, prior to the pandemic, 17 percent reported that their visibility into the activities of remote workers was poor or they had no visibility at all, and this had fallen to 11 percent early in the pandemic. Even after the pandemic is over, 56 percent of organizations anticipate that they will not have very good or excellent visibility.

We found some regional differences on this question. For example, prior to the pandemic 11 percent of North American organizations felt they had very good or excellent visibility into the activities of their remote workers, while these figures were just three percent for APAC and two percent for EMEA. Post-pandemic, however, the proportion that anticipate very good or excellent visibility across all three regions is expected to be robust – in the range of 40-47 percent.

MANY TOOLS ARE USED FOR DEVICE AND USER VISIBILITY

As shown in Figure Q22, log files are the most often-used tool in an attempt to enable visibility for endpoint users and devices – nearly one-half of organizations are using log files for this purpose. However, identity asset management and Active Directory are also used in an attempt to gain visibility.

Figure Q22
Tools Used for Device and User Visibility for Endpoints



Source: Osterman Research, Inc.

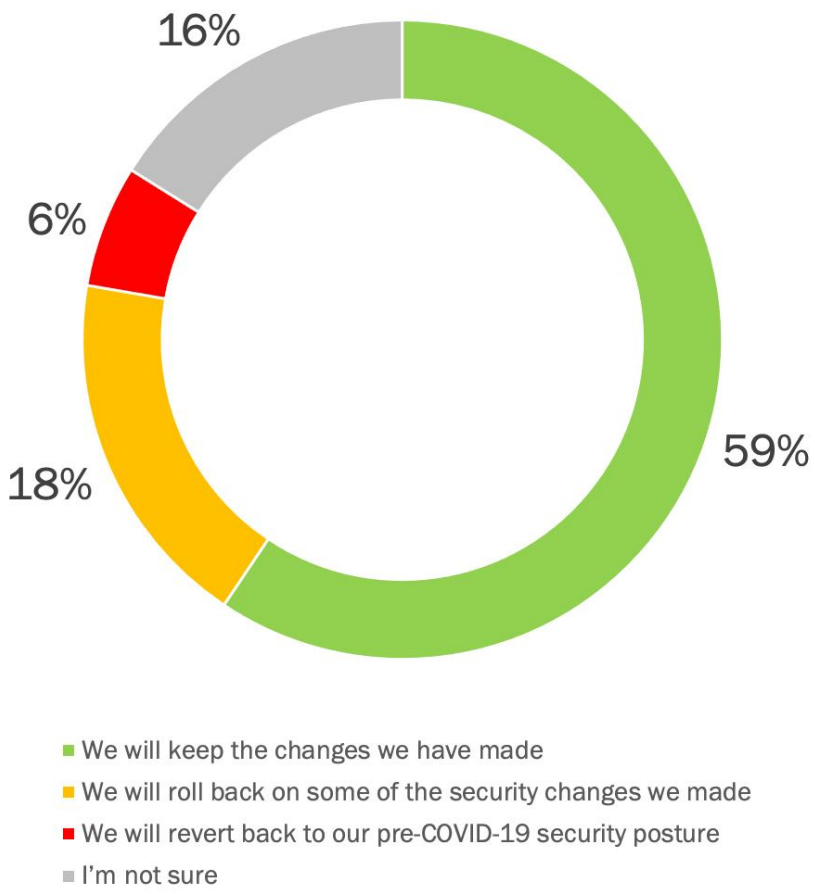
Our research found that log files are commonly used across all three regions, from 50 percent of organizations in North America to 43 percent and 42 percent in APAC and EMEA, respectively. However, while Active Directory is used to enable visibility for endpoint users and devices by 42 percent of organizations in North America, it is used far less in APAC and EMEA: by 29 percent and 26 percent of organizations, respectively.

Our research found that log files are commonly used across all three regions.

MOST WILL KEEP THE CHANGES THEY MADE

As shown in Figure Q24, about three in five organizations anticipate that they will retain the security changes they made as a response to the pandemic. A smaller proportion – 18 percent – will roll back some of the changes, while six percent will actually revert back to the security posture they maintained prior to the pandemic.

Figure Q24
Anticipated Changes to Security Posture Post-COVID-19 Pandemic



Source: Osterman Research, Inc.

The likelihood of keeping the security changes that have been made is dependent to some extent on the size of the organization.

The likelihood of keeping the security changes that have been made is dependent to some extent on the size of the organization, the proportion of employees that are anticipated will be working from home post-pandemic, and the region:

- The mean size of the organizations that will retain the security changes they made is 13,477 employees versus 4,106 employees at the organizations that will roll back some of the changes, and 3,509 employees at the organizations that will revert back to their pre-pandemic security posture.
- For organizations that will have fewer than 25 percent of employees working from home post-pandemic, 55 percent will retain the security changes they made; however, if organizations anticipate having 25 percent or more of their employees working from home after the pandemic, 67 percent will retain their security changes.

- Organizations in North America are much more likely to retain the changes they made: 70 percent versus 51 percent in EMEA and 47 percent in APAC.

Summary

The survey findings help tell a story about how decision makers' responses to the global COVID-19 outbreak are helping to shape the future of endpoint security. The pandemic put a spotlight on the inadequacies of pre-pandemic mobile worker security and served as a catalyst for executives and others to support the necessary investments to enable a productive work-from-anywhere environment while minimizing security risks.

While incidents spiked early on, IT and security leaders responded quickly in a way that has given them greater confidence in their off-network visibility and defensive capabilities. However, security measures intended for a relatively small number of mobile workers at any given moment are proving either inefficient or a struggle to maintain when asked to support a large remote workforce. Solutions like VPN have introduced connectivity, productivity and management issues that must be addressed over the long term.

So, while current measures are helping survey respondent organizations to address current needs, most are looking at transitioning to more long-term solutions such as next-gen endpoint anti-virus, cloud-native DNS Security, and CASB.

About Infoblox

Over the past 20 years, we've been recognized as the leader in core network services, which includes Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and IP address management (IPAM), collectively known as DDI. Building upon this proven foundation, we're bringing DDI and core network services to the next level with our Secure Cloud-Managed Network Services. This enables all customers to go to the next level that's right for them—whether their networks are completely on-premises, full cloud or hybrid cloud.

www.infoblox.com
@Infoblox
info@infoblox.com
+1 888 463 6259