Action1 Corporation
November 2021

2021 Remote IT Management Challenges Report

Action1

Contents

3 PART I. Introduction

- **3** About this Report
- **4** Executive Summary

5 PART II. Key Findings

- **5** Will Organizations Keep Remote Work in 2022?
- **6** Do Organizations Have Reliable, Automated Patching?
- **7** Can Organizations Deploy Critical Updates Without Undue Delay?
- **8** How Serious Is the Risk from Slow Patching of Remote Endpoints?
- **10** What Are the Chief Barriers to Effective Patching of Remote Endpoints?
- **11** Do IT Teams Have Sufficient Visibility Into and Control Over Remote Endpoints?
- **12** Can IT Teams Provide Efficient and Responsive Support to Remote Employees?

13 PART III. Key Recommendations

14 PART IV. Appendixes

- **15** Appendix A. Methodology & Demographics
- **16** Appendix B. Responses to Open-Ended Questions

Action1

About this Report

Many organizations have embraced a remote or hybrid work model permanently. In fact, most of them have learned how to reap the benefits from remote work, such as reduced costs, broader hiring opportunities, and increased employee satisfaction.

While many IT teams were able to rapidly revise existing processes and implement new, more agile technologies to enable the business to operate efficiently when a significant part of the workforce was remote, some routine and essential IT tasks became far more challenging — especially patching and managing all the newly remote endpoints and providing IT support to remote workers.

Multiple factors played a role. The number of critical patches issued increased, and applying them became more urgent as adversaries became faster at exploiting publicly known vulnerabilities. There were also far more applications to keep patched, as the digital transformation increased the number of third-party software products organizations relied upon. Trying to use the IT management solutions that had worked pretty well for in-office endpoints turned out to be ill-suited for the remote workforce. For example, patching of remote endpoints can be done manually via VPN, but this method is time-consuming, insecure, and error-prone. As a result, it increases the risks of missing critical updates, which puts the organization at increased risk from cyberattacks. At the same time, remote workers are susceptible to risky behaviors like using their corporate machines for personal purposes and installing unapproved applications on them, which creates additional security risks that on-premises IT management tools are not designed to mitigate.

In short, large-scale remote work diminishes an IT team's visibility into corporate endpoints and hampers their ability to detect and resolve issues, which threatens security, productivity and business continuity. No organization can afford such risks, especially if it plans to keep at least some remote work in the long term.

Therefore, as we head towards 2022, it is vital to understand the shape of the workforce to expect in the next year, and whether current approaches to remote IT management will meet the associated needs. To find out, we surveyed 491 IT professionals from the USA, Canada, Europe, and other regions. The key findings are presented in this report.

Executive Summary

62% of incidents this year involved exploitation of a vulnerability for which a patch was available but had not yet been deployed.

Most organizations plan to keep at least some remote work in 2022. Some organizations will even increase the share of remote devices in their network.

Unsurprisingly, Windows is the most commonly used operating system (OS); Mac is used by only about half as many organizations as Windows.

Although reliable software updates are critical to both IT operations and cybersecurity, most organizations (59%) automate patching for OS updates only; they manage patches for other software products manually. About one in six (14%) still manage all patches manually.

Even critical updates are not always applied in a timely manner: 78% of respondents experienced delays in patching critical vulnerabilities at least a few times during the last 12 months. It takes more than twice as long to patch a critical vulnerability when endpoints are remote.

Lack of efficient patch management is costly. 77% of organizations suffered at least one security incident in the past year, and 62% of them said the incident involved a known vulnerability that had not been mitigated even though a patch was available. The most common type of incident was a ransomware and other malware attack. Respondents say they do not have enough bandwidth to keep up with patches because they cannot get all the information about updates in one place and they have to juggle multiple non-integrated tools.

More than a third (35%) of respondents are unable to spot unwanted software installed on their endpoints, and 43% are concerned about employees letting family members use their corporate devices when they work from home.

Finally, the survey found that responding to IT support requests takes twice as long when employees are remote, which might be due to the IT team's lack of visibility into and control over remote endpoints.

Will Organizations Keep Remote Work in 2022?

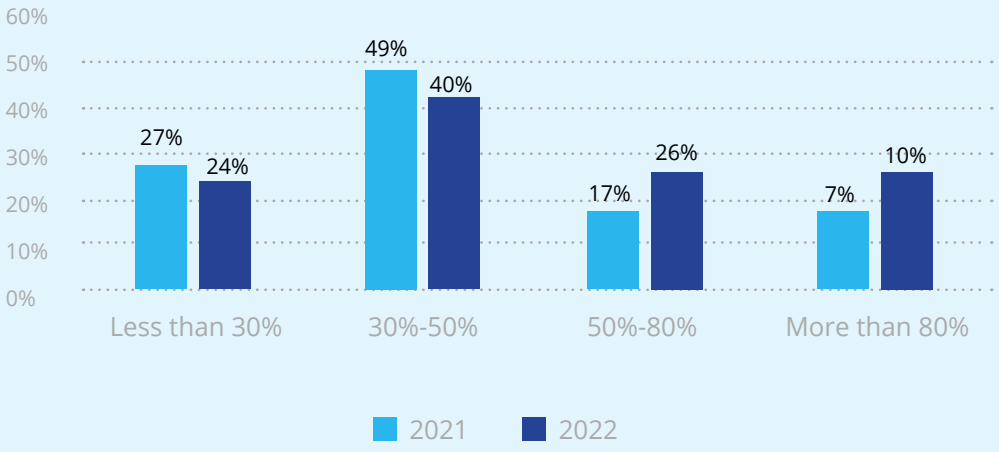
Despite the warnings in late 2021 about various issues with remote work, our survey data shows that the majority of organizations plan to keep some remote work:

- Only about a quarter (27%) of organizations say that less than 30% of their endpoints are remote; that number is projected to drop slightly in 2022.
- The share of organizations that are at least half remote is expected to grow from one fourth (24%) in 2021 to more than a third (36%) in 2022.

Perhaps organizations plan to require some workers to be remote, because the pandemic has demonstrated to business leaders that employees can remain productive when working from home. Indeed, remote work offers significant benefits to organizations, including better employee satisfaction and more flexible hiring opportunities. Many organizations are considering adopting a hybrid model in which employees work from home part of the time but come into the office to facilitate collaboration, enable face-to-face meetings and reignite the culture they miss when remote.

> *By the end of 2023, more than 90% of infrastructure and operations (I&O) organizations will have the majority of their staff working remotely. COVID-19 may have accelerated this trend, but it is also the result of the changing nature of infrastructure led by the shift to cloud and edge.*
>
> *— Smarter with Gartner*

Figure 1
Percentage of endpoints organizations expect to be remote in 2022 as compared to 2021



Do Organizations Have Reliable, Automated Patching?

Updates issued to patch critical vulnerabilities need to be deployed as fast as possible because attackers might already be exploiting the vulnerability or will start doing so upon its public disclosure.

However, the survey data shows that the vast majority (73%) of respondents take a manual approach to patching for at least some types of systems. 59% automate OS patching only and manage updates for other applications manually, while 14% manage all patches manually. While the OS patching is certainly the top priority for patch management, third-party software often has important vulnerabilities that also need to be patched. With the average enterprise today having 464 applications deployed, taking a manual approach means incurs a huge risk of missing important updates.

The good news is that one fourth of respondents (24%) use cloud-based remote monitoring and management (RMM) tools. By automating all types of patching across their organization from a single pane of glass, these tools help organizations adhere to security best practices and improve their security posture.

Unsurprisingly, Windows is the most common OS, used by 75% of respondents. Mac is second with 35%.

59% of organizations automate patching only for OS updates; they manage the patches for their many other software products manually.

Figure 2
How do you manage patches?

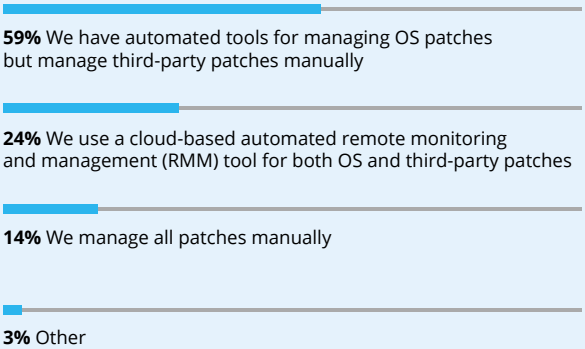
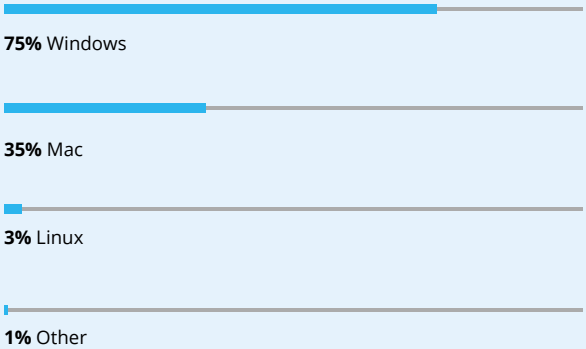


Figure 3
Which types of endpoints are the main focus of your IT management efforts? (Choose all that apply.)



Can Organizations Deploy Critical Updates Without Undue Delay?

Updates issued to patch critical vulnerabilities need to be deployed as fast as possible because attackers might already be exploiting the vulnerability or will start doing so upon its public disclosure.

The survey reveals some concerning statistics. More than a quarter (29%) of organizations don't know how many of their endpoints are missing critical patches, and a solid majority (78%) admit they've experienced delays in patching critical vulnerabilities at least a few times during the last 12 months.

78% of organizations admit they failed to patch several critical vulnerabilities in a timely manner during the past year.

Figure 4
Do you know how many of your endpoints have critical patches missing?

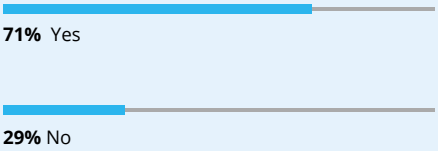
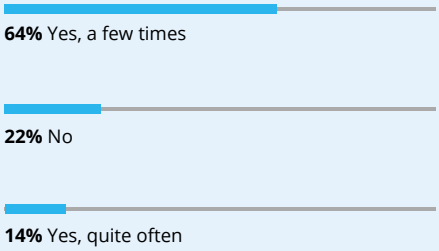


Figure 5
Has your organization experienced delays in patching critical vulnerabilities on its endpoints in the last 12 months?



It takes more than twice as long to patch a critical vulnerability when endpoints are remote

In addition, respondents confirm that deploying critical patches is more time-consuming when endpoints are remote. On average, it takes almost two weeks to get all remote devices patched, and some organizations need three months (90 days)!

Table 1*
The average time to patch a critical vulnerability on remote/office-based endpoints.

Respondent	Remote endpoints	Office-based endpoints
Average value	10 days	4 days
Maximum value	90 days	30 days
Minimum value	8 hours	1 hour

*We asked respondents to share their experience about patching remote and office-based endpoints using open-ended questions; this table summarizes their responses. The detailed responses are provided in Appendix B.

How Serious Is the Risk from Slow Patching of Remote Endpoints?

In 2021, there were many publicly known cases in which hackers exploited recently disclosed vulnerabilities to compromise unpatched systems. Our survey found that this type of incident is alarmingly common.

77% of respondents reported that their organization suffered at least one security incident during the past year — and 62% of them indicated that the incident involved a vulnerability for which a patch had been issued but had not been applied.

The three most common types of incidents were:

- Malware attack (such as ransomware) – 41%
- Phishing attack – 31%
- Man-in-the-middle attack (MitM) – 21%

Although the survey did not investigate which vulnerabilities were exploited in these attacks or how the attacks worked, there are other relevant data points that shed light on the survey results. In particular, phishing is one of the top vectors for malware attacks, and malware typically exploits older known vulnerabilities.

> *Adversaries' use of known vulnerabilities complicates attribution, reduces costs, and minimizes risk because they are not investing in developing a zero-day exploit for their exclusive use, which they risk losing if it becomes known.*
>
> *— The US Cybersecurity & Infrastructure Security Agency*

Figure 6
Did your organization have one or more security incidents in the last 12 months?

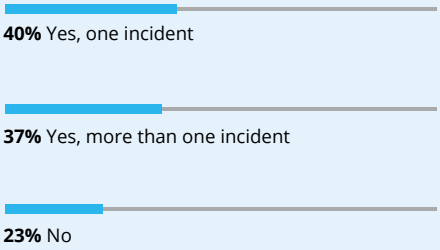
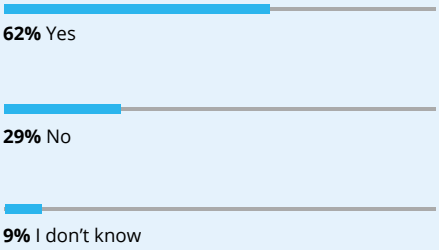


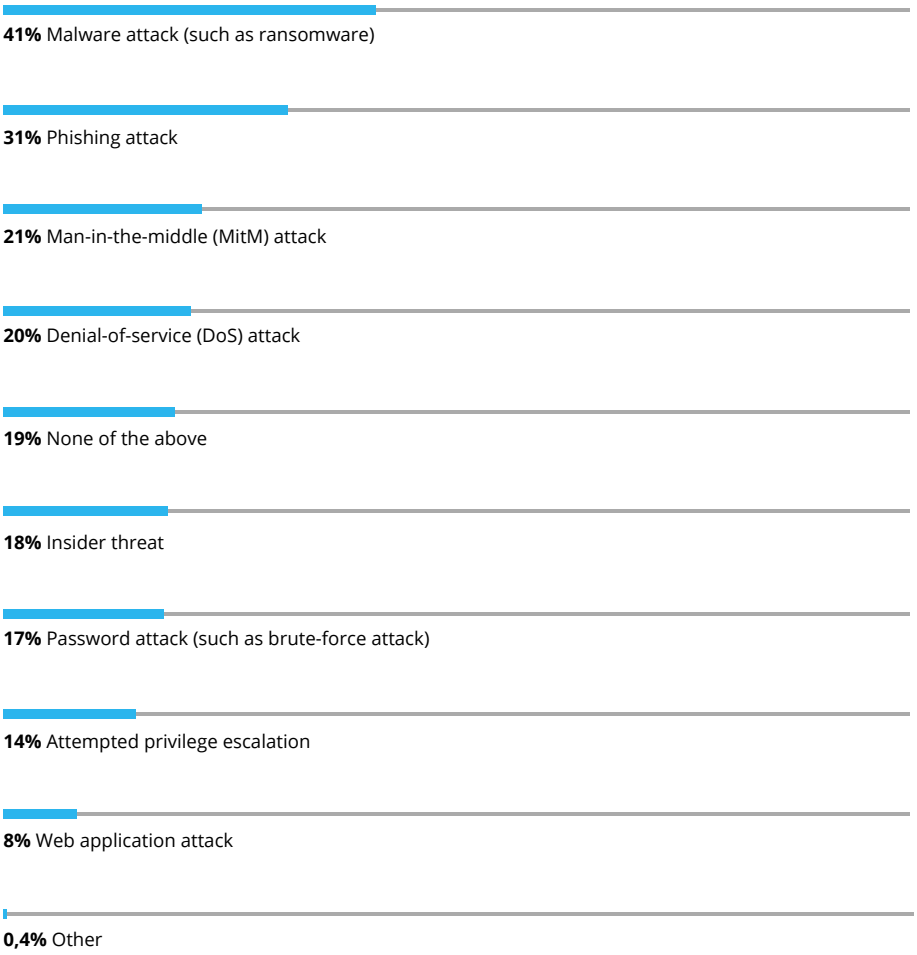
Figure 7
Did any of those incidents involve a vulnerability for which a patch had been issued but was not yet deployed?



62% of security incidents during the past 12 months involved an unpatched vulnerability

Remote work makes organizations more susceptible to man-in-the-middle attacks. Such attacks involve hackers inserting themselves into the communications between a user and an application, usually in order to steal personal information like login credentials, account details and credit card numbers. One technique is for an attacker to make a malicious Wi-Fi hotspot available for free to the public in cafes, coworking, and other public places.

Figure 8
What types of security incidents did your organization have in the last 12 months? (Choose all that apply.)



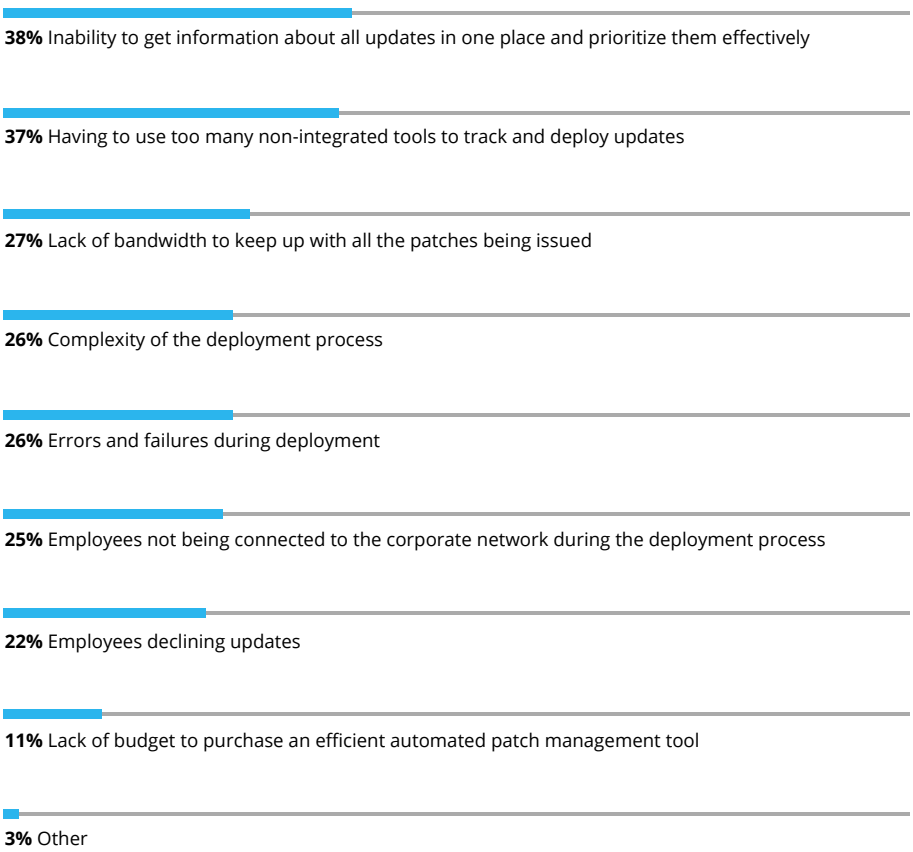
What Are the Chief Barriers to Effective Patching of Remote Endpoints?

Organizations realize they need to keep all their endpoints up to date, so why exactly is it so hard to patch remote endpoints?

The top reason, reported by 38% of our survey respondents, is that they cannot get information about all updates in one place and prioritize them effectively. Nearly as many (37%) say they have to use too many non-integrated tools to track and deploy updates.

Multiple other issues were called out by about a quarter of respondents: lack of bandwidth to keep up with all the patches being issued, the complexity of the process, errors during deployment, endpoints not being connected to the network, and employees declining the updates.

Figure 9
Which of the following are the most critical barriers to efficiently patching your remote endpoints? (Choose all that apply.)



Do IT Teams Have Sufficient Visibility Into and Control Over Remote Endpoints?

IT teams need visibility into the software and hardware of remote endpoints, as well as the ability to manage applications remotely and flag any misuse that is taking place. These capabilities are essential to high IT productivity, strong security, and system availability.

More than a third of respondents are unable to spot unwanted software on remote endpoints.

The survey found that organizations perform fairly well on some endpoint management tasks but lag on others.

In particular, 74% of respondents have automated remote software deployment, which means they can provide remote employees with the tools they need to do their jobs, just as they do for office-based users.

However, more than a third (35%) of respondents are unable to spot unwanted software on remote endpoints. That's a big security gap, since 43% of respondents worry that remote employees are likely to allow family members to use their corporate devices for personal matters — which often includes installing unapproved applications.

Figure 10
Do you have a bird's eye view of the unwanted software installed on your remote endpoints?

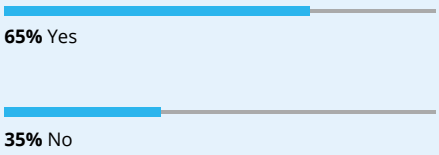


Figure 11
Are you able to automatically deploy software to a large number of remote endpoints at once?

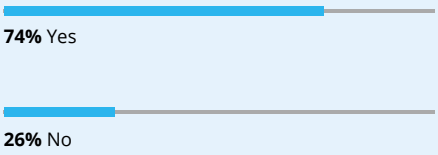
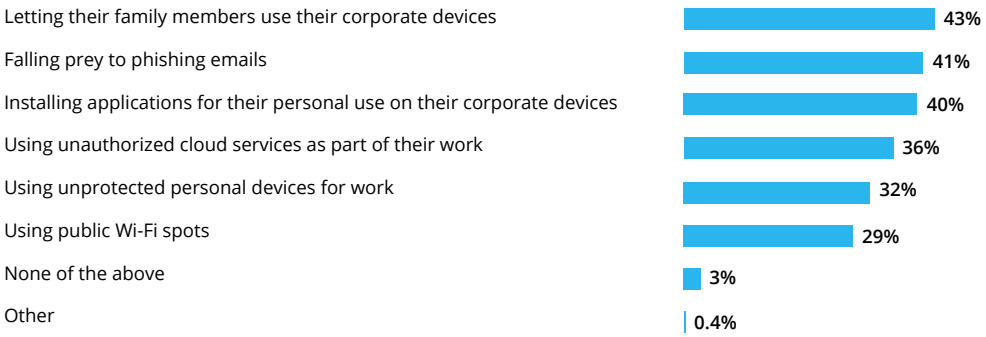


Figure 12
Which of the following risky behaviors do you suspect your employees are more susceptible to when they're working from home? (Choose all that apply.)



Can IT Teams Provide Efficient and Responsive Support to Remote Employees?

To ensure that productivity does not suffer when employees are remote, IT teams must be able to provide all employees with high-quality IT support.

Unfortunately, the survey data shows that resolving IT support requests takes twice as long when employees are remote.

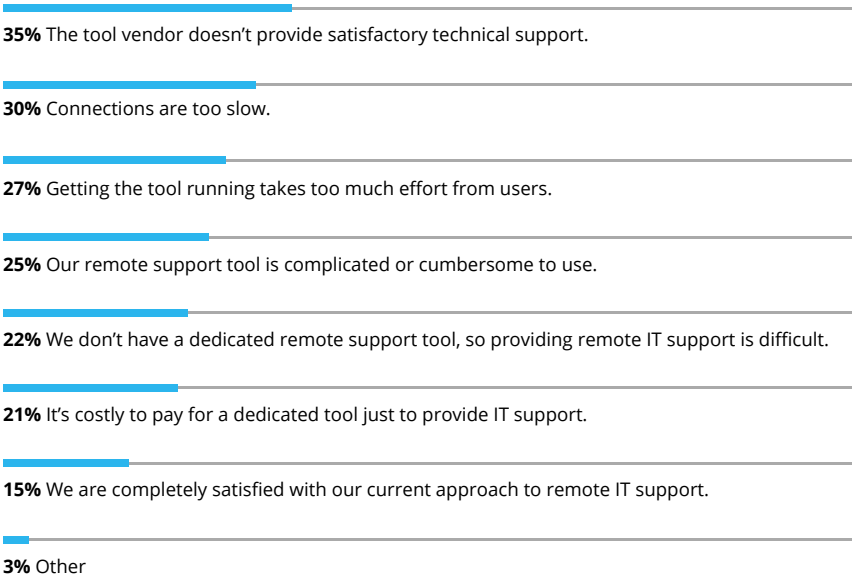
Table 2**
The average time to resolve an IT support request for a remote/office-based employee.

Respondent	Remote employee	Office-based employee
Average time	60 min	32 min
Maximum time	40 hours	4 hours
Minimum time	10 min	5 min

**We asked respondents to share their experience about providing IT support to remote and office-based employees using open-ended questions; this table summarizes their responses. The detailed responses are provided in Appendix B.

The top barriers preventing organizations from providing their remote employees with efficient IT support are of technical nature: 35% of respondents say they can't get satisfactory technical support from the remote support tool vendor, and 30% say connections are too slow.

Figure 13



PART III. Key Recommendations

Since most organizations plan to continue using a hybrid model through 2022, it's essential for them to adopt tools and processes that support remote work for the long term. Here are our top recommendations:

Improve and automate critical aspects of remote IT management, especially software patching. The findings show that too many organizations have experienced security incidents that involved delays in deploying critical patches. Since most IT teams are understaffed, it is no surprise that they cannot stay on top of all the patches being issued, especially as organizations are deploying ever more third-party solutions to maintain business continuity with a remote workforce. Our recommendations include automating patches not just for operating systems but all software. In addition, organizations need to enable IT teams to prioritize updates based on risk, and to help them streamline all their patch management efforts in one place without having to juggle multiple tools.

Empower IT teams with deep visibility into and control over remote endpoints. With these capabilities, IT teams can maintain endpoints more effectively, including spotting and removing unwanted or outdated applications, which enhances security and compliance. They can even resolve IT support requests from remote employees as quickly as those from in-office staff, helping ensure high productivity.

Invest in cybersecurity awareness education for all employees. With a remote or hybrid workforce, it is especially important that everyone is closely following security policies. Specific recommendations include making sure all users are adept at identifying phishing attacks and know to avoid risky behaviors like letting family member use their corporate devices or using public Wi-Fi networks. More broadly, foster a culture of cybersecurity in which everyone encourages their peers to do the right things and acts as a cybersecurity ambassador in the organization.

Implement an actionable incident response plan. Though every organization wants avoid being compromised, the risk is always there. Therefore, it is essential to have an actionable incident response plan that is regularly tested and rehearsed.

Appendix A. Methodology & Demographics

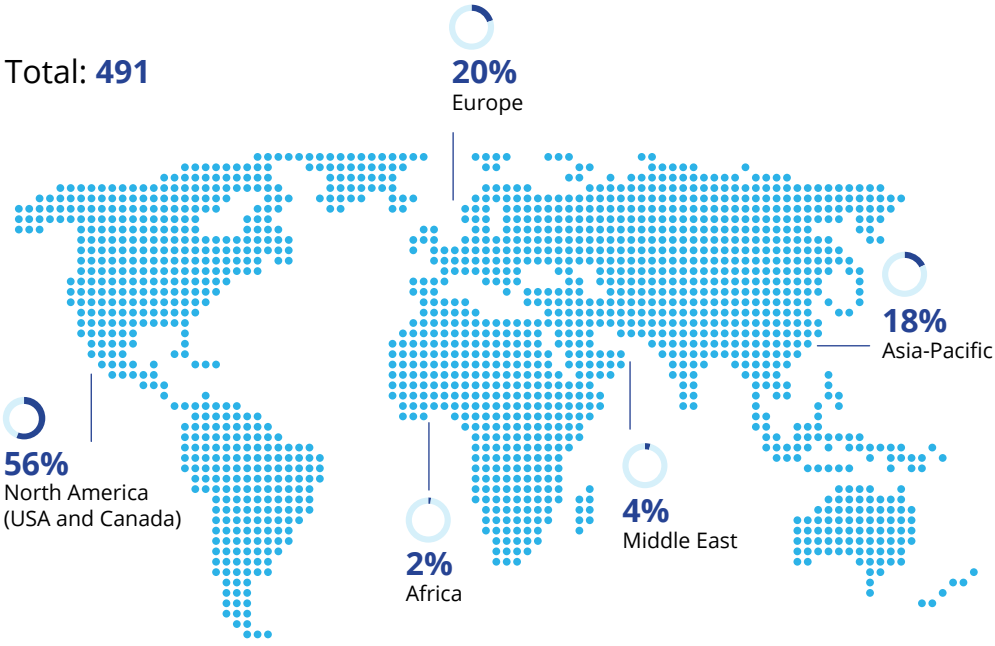
To compile this report, we collected feedback from 491 IT professionals. Respondents were invited to participate in a giveaway to get a chance to win a small monetary reward. Responses were collected in September 2021.

The survey comprised 21 questions. Our analyses of the results are provided in the "Key findings" part of the report, and all responses to the 2 open-ended questions from the survey are provided in Appendix B.

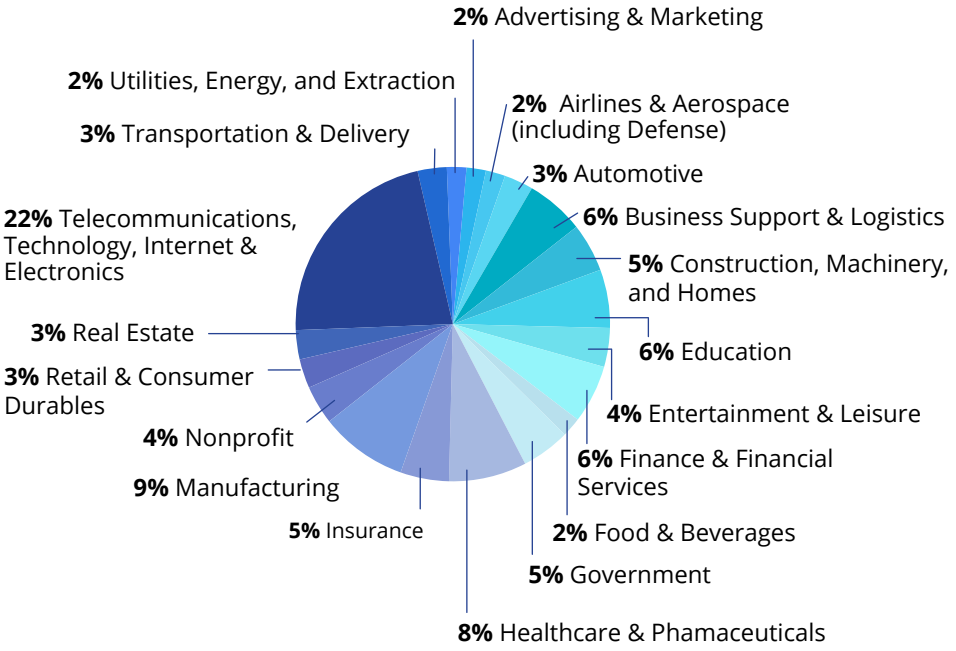
The charts below illustrate key demographics for the respondents.

Chart 1. Location

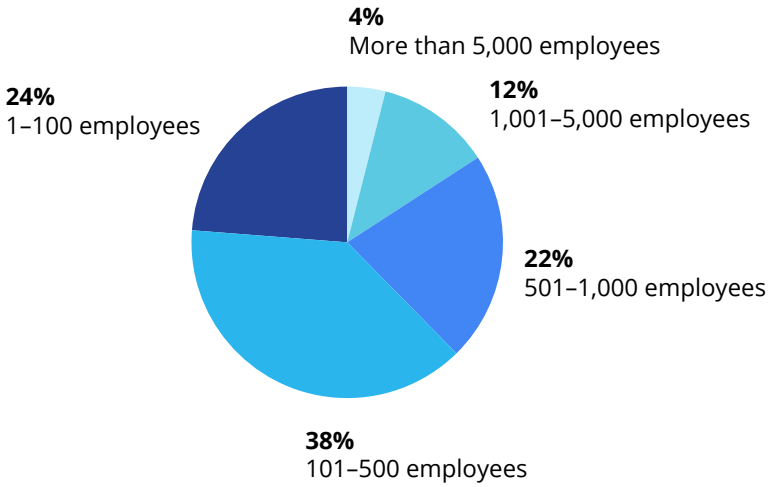
Total: **491**



Pie Chart 2.
Industry



Pie Chart 3.
Headcount



Appendix B. Responses to Open-Ended Questions

Open-ended responses summarized in Table 1

To explore how well organizations can deploy critical patches on remote and office-based endpoints, we asked the respondents the following open-ended questions:

- On average, how long does it take you to patch a critical vulnerability on your remote endpoints after the patch is released? Please put the value in days.

- On average, how long does it take you to patch a critical vulnerability on your office-based endpoints after the patch is released? Please put the value in days.

473 respondents answered these two questions. We normalized the responses by changing number words to numerals and converting fractions to decimal values. 8 responses were excluded for failing to provide numeric values; the remaining 467 responses were used to calculate the data reported in Table 1.

The unedited responses are shown below.

On average, how long does it take you to patch a critical vulnerability on your... after the patch is released? Please put the value in days.

Respondent	Remote endpoints	Office-based endpoints
1	10	2
2	16	7
3	14	7
4	30	14
5	14	7
6	na	?
7	7 days	1/2 day
8	30	14
9	4	2
10	2	1/4
11	4	2
12	1/3	1
13	4	2
14	10	2
15	2	1
16	14	2
17	35	14

18	half of the day	half of the day
19	half of the day	1 day
20	2	one third
21	6	half a day.
22	20	7
23	14	7
24	14	7
25	2	2
26	a day	1/2
27	14	7 days
28	2	1
29	2	1/2
30	1	2
31	7	1
32	2	1/2
33	7	3
34	20	7
35	1/2	1/2
36	2	1/2
37	2	1
38	7	3
39	21	7
40	2	1
41	2	1
42	1	1
43	2	1/2
44	1/2	1
45	2	1
46	7 days	1
47	20	7
48	2	1/2
49	4	1
50	2	2
51	6	1
52	60	14
53	2	1
54	2	2
55	6	1
56	1/2	1
57	1 day	1/2
58	6	Half a day
59	4 weeks	14
60	6	1 day

61	28	14
62	30	14
63	Up to 2 months	21
64	14	4 business days
65	4	1/2
66	24	14
67	30	7
68	1/2 day	1/2 day
69	7	3
70	16	7
71	4	1
72	7	1/8
73	4	1/2
74	7	3
75	1	1
76	1 day	1 hour
77	14	3
78	14	7
79	28	14
80	7	1
81	n/a	n/a
82	7	2
83	2	0.5
84	One day	One day
85	30	7
86	60	14
87	1/2	1
88	4	1
89	Half of the day 1/2	Half of the day
90	60	15
91	14	7
92	14	7
93	We have no remote endpoints	1/2 or less
94	21	7
95	14 days	7 days
96	14	5
97	3 days	1 day
98	One day	1/2
99	4	1
100	30	14
101	2	0.5
102	7	0.5
103	2	1

104	A day at most	Half a day
105	Half a day to use	A day at most
106	Half a day to use	0.5
107	As the case may be; Sometimes half a day; Sometimes two days	Half a day
108	2	1/2
109	10	3
110	30	7
111	14	3
112	Depends on the day really, with the software we use sometime it'll deploy the patches within minutes, other times it can take up to 24 hours before they deploy	Same as the previous question, although it would generally take no more than 12h
113	4	1
114	2	2
115	14	7
116	4	2
117	1	1
118	2	1
119	1/2	1
120	2	1
121	2	1/4
122	20	7
123	2	1
124	1/2	1/4
125	2	1/2
126	2	2
127	60	30
128	2	1
129	20	7
130	4	1/2
131	1	1
132	2	1/2
133	2	1
134	15	7
135	2	1
136	7	1/2
137	21	7
138	60	14
139	14	7
140	2	1/2
141	6	1
142	2	1
143	1/2	1
144	2	1

145	7	3
146	21	14
147	1/2	1/2
148	2	2
149	1	1
150	7	2
151	2	1
152	7	1
153	1/2	1/2
154	7	1
155	28	14
156	2	1
157	4	1
158	4	1
159	5 days	1
160	7	1
161	60	21
162	4	1
163	14	1
164	14	3
165	4	1/2
166	1/3	1
167	2	1
168	4	1/2
169	21	7
170	2	1
171	4	1
172	7	1
173	2	2
174	7 days	2
175	10	1
176	14	7
177	7	1
178	21	14
179	1/3	1
180	2	1/2
181	2	1
182	20	7
183	1/2	1/2
184	1/2	1
185	2	2
186	2	1
187	21	5

188	28	14
189	7	2
190	4	1
191	2	1
192	2 weeks	4
193	4	1
194	2	1
195	4	2
196	4	1/2
197	14	7
198	1/2	1
199	2	1
200	7	2
201	2	2
202	30	7
203	1/2	1/2
204	7	1
205	35	7
206	7	1
207	2	1
208	1/2	1
209	30	14
210	2	1
211	4	2
212	1/2	1
213	2	1
214	21	4
215	4	1
216	30	14
217	7	1
218	14	3
219	7	1
220	1/2	1/3
221	2	2
222	2	2
223	7	2
224	2	1/2
225	2	1
226	2	1
227	30	14
228	4	1
229	14	7
230	14	3

231	2	1
232	30	14
233	7	2
234	5	1
235	2	1
236	3	2
237	7	3
238	28	7
239	3	2
240	2	1/2
241	2	2
242	14	1/2
243	3	1
244	1/2	1/2
245	5	2
246	14	4
247	14	3
248	2	1/2
249	1 week	3
250	3	3
251	2	2
252	4	1/2
253	7	1
254	21	14
255	30	16
256	2 weeks	2
257	30	15
258	30	4
259	1/2	1/3
260	21	5
261	1/2	1/2
262	7	2
263	14	3
264	2	1/2
265	35	7
266	4	3
267	15	4
268	3	2
269	2	2
270	1	1
271	3	1
272	21	12
273	1/2	1

274	5	2
275	8	1/2
276	1/3	1/3
277	14	5
278	5	1/3
279	8	5
280	14	7
281	5	3
282	1/3	1/3
283	3	1/3
284	1/3	1/3
285	21	7
286	3	2
287	1	2
288	7	7
289	30	14
290	1	1
291	3	2/1
292	2	2
293	1/2	1/2
294	5	4
295	6	5
296	3	4
297	7	3
298	5	4
299	3	2
300	14	7
301	7	2
302	3	3
303	1/2	2
304	1	1/2
305	5	2 1/2
306	10 days	7
307	1/2	1/2
308	3	1/2
309	4	a half of the day
310	30	15
311	14	5
312	2	2
313	a half of the day	a half of the day
314	a half of the day	a half of the day
315	2	4
316	7	3

317	5	2
318	1	2
319	1 Day	4
320	2	1 hour
321	4	3
322	4	2
323	7	2
324	14	9
325	7	6
326	2	2
327	6	1
328	2	4
329	2	1
330	1 day	1 day
331	3	3
332	half of the day	half of the day
333	5	3
334	2	1
335	60	1
336	7	1
337	3	1
338	4	1
339	3	1
340	10	3
341	2	2
342	2	1
343	7	1
344	14	5
345	2	1
346	60	21
347	3	5
348	3	1/4
349	4	2
350	60	21
351	half of the day	half of the day
352	half of the day	half of the day
353	5	5
354	2	1
355	14	5
356	1	2
357	14	2
358	2	1
359	14	2

360	2	2
361	10	2
362	28	7
363	14	5
364	1	2
365	2	2
366	1	1
367	7	1
368	2	1
369	2	1
370	2	2
371	8	2
372	1	1
373	3	3
374	20	7
375	5	3
376	2	2
377	1	1
378	14	5
379	2/3	1/2
380	30	15
381	28	14
382	9	1 day
383	7	2
384	30	14
385	2 days	1 days
386	1- 3 days	Half a day to 3/2
387	1	1/2
388	3	3
389	1/3 day	1/3 day
390	up to 7	1 to 2
391	35	10
392	3	1
393	2	1
394	1/2	1/5
395	25	0.25
396	2	0.5
397	2	1
398	60	30
399	10	5
400	1 day	1 day
401	3-5 days	2-3 days
402	3	2

403	2	1/2
404	3	1
405	Unknown.	2
406	2	1/4
407	30	2
408	7	1/4
409	44	30
410	na	na
411	2	1
412	5	2
413	2	1
414	3	3
415	21	7
416	2	2
417	14	4
418	21	5
419	14	5
420	30	14
421	1 day	1/2 day
422	14	7
423	2	1/2
424	7	3
425	14	7
426	1 and 1/2 day	1/2 a day
427	1/2	1/2
428	7 days	1 day
429	2	2
430	30	14
431	4	2
432	Na	5
433	10	5
434	20	10
435	1/2	1/2
436	2	1/2
437	7	3
438	90	30
439	21	14
440	30	1/2
441	5	3
442	7	7
443	5	1
444	7	0
445	21	2

446	1/2 half of a day	1/2 half of a day
447	4	2
448	I don´t know, sometimes I do, when I have time...	I don´t know, sometimes I do, when I have time...
449	1 Day	1 hour
450	4 Days	less than 1 hour
451	90	30
452	30	14
453	2 weeks	7
454	5	5
455	14	7
456	5	5
457	2	1
458	21	7
459	30	14
460	7 days	3
461	14	7
462	7 Days	2 days
463	7	2
464	3 weeks	14
465	15	4
466	30	7 days
467	4	1/2
468	30	14
469	90	30
470	12	1
471	15	5
472	21	7
473	60	30

Open-ended responses summarized in Table 2

To explore how well organizations can provide remote and office-based employees with efficient IT support, we asked the respondents the following open-ended questions:

- On average, how much time do you need to resolve an IT support request from a remote employee? Please put the value in minutes.
- On average, how much time do you need to resolve an IT support request from an office-based employee? Please put the value in minutes.

We recieved 469 responses. We normalized the responses by changing number words to numerals and converting fractions to decimal values. 4 responses were removed for failing to provide numeric values; the remaining 465 responses were used to calculate the data reported in Table 2.

The unedited responses are shown below.

On average, how much time do you need to resolve an IT support request from... Please put the value in minutes.

Respondent	A remote employee	An office-based employee
1	90	15
2	120	20
3	60	15
4	100	20
5	30	20
6	?	?
7	90	60
8	60	20
9	120	50
10	120	5
11	35 minutes	25 minutes
12	55	20
13	40	10
14	30	15
15	30	20
16	25	24
17	100	60
18	60	30
19	Fifty minutes	30 minutes
20	45	20
21	20	15
22	40	15
23	60	15
24	60	20
25	35 minutes	25 minutes
26	15 minutes	Ten minutes
27	120	100
28	25	30
29	90	60
30	60	25
31	20	15
32	20	10
33	20	15
34	60	15
35	40	30
36	120	10
37	23	35
38	60	25

39	60	25
40	25	30
41	60	15
42	60	35
43	35	20
44	30	20
45	60	30
46	90	20
47	60	25
48	35	30
49	30	10
50	60	25
51	120	90
52	30	10
53	14	10
54	50	20
55	5	10
56	30	20
57	120	30
58	Twenty minutes	30 minutes
59	30	20
60	60	60
61	40	40
62	46 minutes	65 minutes
63	120	60
64	210	90
65	60	30
66	60	25
67	30	30
68	0	5
69	30	15
70	30	30
71	480	240
72	120	60
73	0	10
74	60	30
75	15	15
76	60	60
77	10	10
78	20	30
79	1440	60
80	15	10
81	15	15
82	10	5

83	30	5
84	25	10
85	15	10
86	30 minutes	30 minutes
87	30	15
88	30	15
89	40	5
90	30	30
91	20	20
92	30	10
93	90	30
94	20	5
95	30	30
96	30	10
97	60	30
98	45 minutes	25 minutes
99	40 minutes	25 minutes
100	Twenty minutes	Ten minutes
101	30	20
102	30	26
103	26	20
104	Ten minutes	5 minutes
105	23	19
106	18	15
107	26	14
108	20	15
109	10	10
110	30	20
111	30	30
112	Generally between 45 mins to an hour, although if the issue requires me to go on-site it could take up to 8 hours	Generally no more than 2 hours, average around 20 minutes
113	20	20
114	30	10
115	60	60
116	50	30
117	40	50
118	30	10
119	45	35
120	60	30
121	30	40
122	20	10
123	20	30
124	60	30

125	60	30
126	100	60
127	45	30
128	45	30
129	35	20
130	30	20
131	35	25
132	25	30
133	20	10
134	15	10
135	60	60
136	35	40
137	35	30
138	30	30
139	40	40
140	35	30
141	35	30
142	33	21
143	80	80
144	10	5
145	60	60
146	30	30
147	90	90
148	50	25
149	30	20
150	10	20
151	90	80
152	45	32
153	26	22
154	20	30
155	50	60
156	50	30
157	35	25
158	30	35
159	30	25
160	30	25
161	30	25
162	30	25
163	20	20
164	15	20
165	45	30
166	60	60
167	180	15
168	90	60

169	40	30
170	100	30
171	40	35
172	30	30
173	25	20
174	20	15
175	20	15
176	10	10
177	80	80
178	60	5
179	160	120
180	90	60
181	90	35
182	120	60
183	100	36
184	60	30
185	90	15
186	60	60
187	20	10
188	60	60
189	30	30
190	25	25
191	35	23
192	34 minutes	60 minutes
193	55 minutes	25 minutes
194	50 minutes	25 minutes
195	Twenty minutes	Twenty minutes
196	45 minutes	Twenty minutes
197	140 minutes	60 minutes
198	45 minutes	Twenty minutes
199	46 minutes	40 minutes
200	46 minutes	10
201	45	40
202	44	33 minutes
203	30	24
204	66	24
205	25	23
206	15	10
207	20	10
208	70	60
209	50	6
210	60	40
211	100	80
212	120	60

213	50	60
214	80	70
215	240	180
216	60	60
217	90	60
218	90	60
219	50	30
220	60	25
221	30	30
222	20	20
223	120 minutes	70 minutes
224	90 minutes	64 minutes
225	36 minutes	45 minutes
226	34 minutes	33 minutes
227	23 minutes	22 minutes
228	180	100
229	30	15
230	20	10
231	100	50
232	90	80
233	50	50
234	60	45
235	180 minutes	56 minutes
236	30 minutes	44 minutes
237	80	60
238	60	60
239	30	30
240	60	30
241	22	11
242	80	50
243	20	30
244	150	15
245	120 minutes	60
246	1 hour	40 minutes
247	Twenty minutes	Twenty minutes
248	45	30
249	55	25 minutes
250	180minutes	100
251	60	60
252	45 minutes	25 minutes
253	45 minutes	25 minutes
254	35 minutes	25 minutes
255	70	70
256	20	10

257	50	80
258	45	63 minutes
259	90 minutes	60
260	45 minutes	33 minutes
261	10	22
262	58	63
263	56	65
264	32 minutes	30 minutes
265	55	70
266	40	66
267	55 minutes	42 minutes
268	30 minutes	22 minutes
269	30 minutes	34 minutes
270	30	20
271	20	32
272	20	22
273	60	15
274	50	30
275	35 minutes	25 minutes
276	35 minutes	25 minutes
277	35 minutes	25 minutes
278	35 minutes	30minutes
279	35 minutes	15
280	35 minutes	25 minutes
281	35 minutes	25 minutes
282	40	15
283	35 minutes	25 minutes
284	20	10
285	45	60
286	40	70
287	34 minutes	27 minutes
288	43 minutes	9
289	20	30 minutes
290	11	10
291	45	60
292	180 minutes	60
293	120	17 minutes
294	45 minutes	33 minutes
295	34 minutes	27 minutes
296	32 minutes	48 minutes
297	43 minutes	20 minutes
298	40	70
299	22 minutes	40 minutes
300	30 minutes	56 minutes

301	30 minutes	30 minutes
302	45	60
303	65	65
304	45	35 minutes
305	35 minutes	15 minutes
306	35 minutes	15 minutes
307	35 minutes	35 minutes
308	35 minutes	10
309	20	10
310	25 minutes	25 minutes
311	120	230
312	25 minutes	25 minutes
313	25 minutes	25 minutes
314	45	30
315	250	15
316	40	70
317	20	10
318	45	60
319	14	12
320	58 minutes	47 minutes
321	90 minutes	47 minutes
322	33 minutes	33 minutes
323	30 minutes	20 minutes
324	30 minutes	20 minutes
325	30 minutes	56 minutes
326	60	70
327	60	70
328	40	60
329	20	10
330	15	8
331	11	15
332	80 minutes	10 minutes
333	30 minutes	25 minutes
334	30 minutes	25 minutes
335	30 minutes	25 minutes
336	30 minutes	25 minutes
337	Ten minutes	Ten minutes
338	30 minutes	25 minutes
339	30 minutes	25 minutes
340	30 minutes	25 minutes
341	30 minutes	25 minutes
342	60	70
343	30	10
344	60	60

345	180minutes	30minutes
346	15	10
347	40	70
348	90	50
349	30 minutes	30 minutes
350	22	17
351	30	20
352	15 minutes	5 minutes
353	Ten minutes	Ten minutes
354	180	70
355	45	15
356	30	30
357	90	30
358	70	20
359	15	15
360	15	15
361	10	10
362	10	10
363	50	25
364	50	50
365	60	50
366	70	30
367	70	25
368	80	30
369	30	15
370	20	10
371	20	10
372	20	10
373	40	20
374	70	70
375	15	13
376	60	45
377	30	30
378	40	30
379	45	25
380	120	20
381	40 minutes	5 minutes
382	30	30
383	20	10
384	240	120
385	50 minutes	30 minutes
386	About 100 minutes	About 140 minutes
387	10	10
388	60	10

389	20	45
390	15 to 30	5
391	45	10
392	30	5
393	15	15
394	50	25
395	15	15
396	10	10
397	10	3
398	60	120
399	15	15
400	30	30
401	30 mins	20 mins
402	30	10
403	240	60
404	10	10
405	30	10
406	30	30
407	90	30
408	60	30
409	n/a	n/a
410	15	15
411	60	30
412	120	90
413	180	120
414	20	20
415	30	15
416	20	20
417	10 to 30 minutes	5 to 15 minutes
418	120	60
419	60	20
420	480 mins	240 mins
421	45	30
422	30-90	30-60
423	320	30
424	120	60
425	10	10
426	30	15
427	20	20
428	90	90
429	10	10
430	60	10
431	60	15
432	90	10

433	120	5
434	30	30
435	30	5
436	30	10
437	60	45
438	30	20
439	20	20
440	30	10
441	15	15
442	60 minutes	30 minutes
443	35	25
444	20	10
445	30	30
446	15	15
447	30	15
448	15	10
449	100	5
450	?	?
451	30	30
452	30	30
453	60	30
454	100	30
455	2400	20
456	90	30
457	120	5
458	30 minutes	15 minutes
459	60	30
460	?	?
461	30	15
462	30	15
463	n/a	25
464	60	10
465	40	30
466	30	15
467	15	10
468	15	5
469	20	10

About Action1 Research

The report is brought to you by Action1 Research, which conducts industry surveys among IT pros worldwide to discover trends in cybersecurity, IT operations, and the MSP industry.
For more information, please visit:

www.action1.com/research/

About Action1 Corporation

Action1 provides a cloud-based solution for remote monitoring and management (RMM) that includes automated patch management, remote desktop access, software deployment and distribution, IT asset inventory, network monitoring, reporting, and more. The company was founded by Netwrix cybersecurity veterans Alex Vovk and Mike Walters in 2018 to give companies and MSPs worldwide a modern alternative to traditional on-premises solutions that do not function in remote workforce scenarios.

Corporate Headquarters:
12333 Sowden Rd., Suite B 36066
Houston, TX 77080

Copyright © Action1 Corporation. All rights reserved. Action1 is trademark of Action1 Corporation and/or one or more of its subsidiaries and may be registered in the U.S. Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are the property of their respective owners.