# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>COVID-19 and Working Remotely — What you need to know now</td>
<td>4</td>
</tr>
<tr>
<td>Patch Management Solutions for Securing Your Remote Workforce</td>
<td>7</td>
</tr>
<tr>
<td>2020 Cyber Hygiene Report Uncovers a patching dilemma even before the move to remote work</td>
<td>10</td>
</tr>
<tr>
<td>Cybersecurity Checklist for a Secure Remote Workforce</td>
<td>13</td>
</tr>
<tr>
<td>SysAdmins — Tips to consider when most of your workforce is working from home...Including yourself</td>
<td>15</td>
</tr>
<tr>
<td>Effectively Managing Remote Teams While Keeping Your Company Secure</td>
<td>18</td>
</tr>
<tr>
<td>How The Cloud Improves Endpoint Security of Your Growing Remote Workforce</td>
<td>22</td>
</tr>
<tr>
<td>The True Cost Burden of On-Premises Patch Management Solutions</td>
<td>24</td>
</tr>
<tr>
<td>Automox — A modern approach to remote workforce use cases</td>
<td>26</td>
</tr>
</tbody>
</table>
Introduction

Over the last two decades, remote workforces have been starting to enter the mainstream; however, COVID-19 has forced companies to shift their entire workforce to 100% work-from-home practically overnight — whether they were ready for that transition or not. This sudden change has brought on a new set of security challenges that need to be addressed. Not only do more endpoints need to be secured remotely, but adversaries are exploiting vulnerabilities created by this change faster than ever. And yesterday’s virtual private networks (VPNs) were never designed to support the new needs of an entirely remote workforce.

Thing is, this new normal could exist beyond the COVID-19 outbreak. According to Gartner, Inc., nearly three in four CFOs plan to shift at least 5% of previously on-site employees to permanently remote positions post-COVID 19. Beyond the obvious goals of keeping employees healthy, there are other, undeniable benefits that suggest working from home could take hold as a permanent strategy.

Your new work-from-home policies could stick, so don’t rethink your telecommuting strategies too hastily in the face of the COVID-19 scare. Your decisions about remote work today may drive tomorrow’s results.

In this guide, we take a look at how to create new policies that effectively manage and secure your remote teams while greatly reducing cost and complexity. We also discuss how you can quickly and easily harden your endpoints in order to stay ahead of cyber threats and become a modern IT Operations (ITOps) team. And we share how Automox’s cloud-native endpoint hardening platform can reduce up to 80% of your vulnerabilities across Microsoft® Windows®, macOS®, and Linux® from a single console. No hardware needed. No VPNs required.
COVID-19 and Working Remotely — What you need to know now

LET’S TALK ABOUT WORKFORCE TRANSFORMATION

Here’s some big-picture thinking to help inform your decisions right now. According to Global Workplace Analytics, organizations save roughly $11,000 per year per part-time telecommuter. And data shows that working remotely leads to an increase in performance and higher job satisfaction, resulting in a 50% better attrition rate versus traditional office jobs. Additionally, companies with telework options have a distinct recruiting advantage, as modern job candidates expect the flexibility to work from home. They are even willing to sacrifice salary in exchange for reducing their daily commute. And as for those reduced commutes, if even half the Americans who could work from home actually did, greenhouse gases would be cut as if we removed the entire New York State workforce from the road.


BE PREPARED FOR A REMOTE WORKFORCE THAT LASTS

The short-term efficacy of using remote work policies to reduce COVID-19 exposure is certainly vital to business continuity in the face of this pandemic. Keeping your teams safe during this period is a no-brainer — as is making sure their remote laptops are safe, too.

However, once your teams get accustomed to working from home, more flexible policies might need to become the new normal. Distribute Consulting has found that revoking work-from-home capabilities is a dangerous overcorrection that only worsens the accessibility, efficiency, and sustainability of jobs. Consider that the United States government is projected to lose more than $800 million this year through retracting telework policies.

So, no matter if you’re making a short-term shift or a long-term transformation, one of your most important considerations is how to keep your remote endpoints secure from vulnerabilities.
Here’s what you should be asking yourself to make sure your IT has a seamless strategy for keeping remote laptops up to date and secure with the latest software, patches, and configurations.

**CAN YOU SECURE YOUR WORKERS’ ENDPOINTS WITHOUT A VPN?**

Make sure your VPN isn’t a critical point for securing your endpoints. Legacy patching platforms can only update systems and software on remote endpoints that are connected to the corporate network via VPN. Not only are companies concerned if their VPNs can even handle the upcoming spike in remote traffic, but also many users often avoid connecting altogether to circumvent the tedious, frustrating, and time-consuming process of making updates over slow VPN connections. **Cloud-native endpoint management solutions like Automox** seamlessly update and patch any corporate endpoint that’s connected to the internet, which means users are always current with patches and configurations.

**WILL YOU BE ABLE TO OUTMANEUVER ATTACKERS WHEN NEW VULNERABILITIES ARE ANNOUNCED?**

Today, attackers are weaponizing vulnerabilities faster and more frequently than ever. In fact, the moment new critical vulnerabilities are reported sets off a race to see if you can patch vulnerabilities faster than adversaries can exploit them. To be safe, you need to **remediate critical vulnerabilities within 72 hours of their announcement**. Traditional, VPN-based patching solutions — which users are reluctant to utilize — will likely not allow you to remediate in time. Automox customers, on the other hand, meet this speed threshold thanks to automated, cloud-native remediation.
ARE YOU ABLE TO PATCH AND UPDATE ACROSS OPERATING SYSTEMS AND THIRD-PARTY SOFTWARE?

Ponemon Institute recently found that 57% of data breaches are attributed to poor patch management. Additionally, third-party applications are responsible for more than 75% of all endpoint vulnerabilities. Yet managing and maintaining the latest software versions and configurations across multiple OSs and myriad remote laptops is a huge hurdle for legacy patch platforms. Automox keeps IT teams ahead of attackers across Windows, macOS, and Linux platforms, along with a growing library of third-party patching support — to secure remote laptops through a single cloud-native console.

DO YOU HAVE VISIBILITY AND CONTROL OF ALL YOUR REMOTE ENDPOINTS?

It’s difficult to automate policies for remote laptops you can’t see. As a cloud-native solution, Automox is uniquely able to provide a complete inventory of all hardware, software, patches, and configuration details for your remote endpoints. You’ll have a unified view of your remote laptops to identify misconfigured systems, discover missing patches, remediate patch vulnerabilities, deploy required software, and fix misconfigured systems across Windows, macOS, and Linux — without the need for multiple tools.

CAN YOU AUTOMATE YOUR ENDPOINT AND PATCH MANAGEMENT ON DEVICES NOT CONNECTED TO YOUR NETWORK?

Patching can be a thankless, time-consuming task that’s easy to fall behind on. What’s worse, IT administrators often can’t see which software titles on which systems are out of date and susceptible to attack. Unpatched and misconfigured laptops are a huge concern for maintaining cyber hygiene. And an increase in remote laptops not connected to the corporate network for extended periods will only compound this problem. Automox gives you visibility into the status of remote endpoints so you can customize and automate both operating system (OS) and third-party application updates or patches to eliminate this threat.

COVID-19 is already making significant disruptions to the global workforce. Only time will tell how long these disruptions last, but this outbreak could be providing a glimpse into the future of telework. Inexpensive video conferencing and communication tools are making it easier than ever to work from home and implementing new remote work policies now to account for COVID-19 concerns could be a sign of more flexible policies to come. Automox has solutions no matter which path you choose. Contact us now for a demo of how we can deliver fast, simple cyber hygiene solutions for your remote workforce.

Patch Management Solutions for Securing Your Remote Workforce

For many organizations, security can be a real concern when it comes to remote workers. If your IT staff is still relying on legacy patch management tools, securing remote endpoints can be a time-consuming, arduous process.

Between poor endpoint visibility and compatibility issues, it’s no wonder remote endpoints are often left vulnerable. And in this day and age, an unsecured endpoint is just an invitation for malicious activity.

**Patch Management for Remote Workers**

The digital landscape is rapidly evolving, and organizations of all sizes are dealing with a vast array of endpoints on their networks — and in many cases, IT staff must also contend with a bevy of different OSs and third-party applications. Patching all these things manually, or with archaic, one-trick pony solutions is simply no longer a viable option for organizations that want to make cybersecurity a priority. If you want to be secure in the modern digital age, you need a modern solution — one that will take care of every device on your network, no matter where it’s located or what OS and applications it’s running.

Patch management is an essential part of good cybersecurity practices. This is especially true when it comes to your remote workers, given that unpatched endpoints are an excellent route of entry for attackers. Time is of particular importance when it comes to patching: **Attackers can weaponize a vulnerability in just seven days.** Conversely, it can take an average of up to **102 days for organizations to patch for a vulnerability.** This discrepancy is a major problem — especially when it comes to endpoints.
WHY REMOTE TEAM SECURITY MATTERS

Generally speaking, every remote worker who’s on your company network is going to represent at least one endpoint. This means remote team security should be a priority for any organization looking to improve their overall cybersecurity and securing all of your endpoints is key to good cyber hygiene. Earlier in 2019, Forbes reported that an astonishing 70% of all breaches still originate on endpoints.

Experts agree that increasing endpoint visibility and having the ability to remediate vulnerabilities in real time are essential to good endpoint management. When it comes to securing your remote workforce, endpoint protection and visibility should be at the top of your list.

It’s common to underplay the need for security when it comes to remote workers, but while they may not work in the office, remote workers are still often a significant part of your team. And in many cases, in-house employees may also have the option to work from home. These workers often have administrative privileges or access to sensitive information on your network — and if their devices aren’t secured properly, they can pose a risk to your organization’s security.

THE CHALLENGE OF SECURING REMOTE ENDPOINTS

Securing remote devices can be a monumental task if you don’t have the right tools. Dark endpoints are notoriously difficult to reckon with. “Have they been patched? Did the last security update fail? No one knows. The endpoints may exist, they may not.”

Poor endpoint visibility is a real problem that plagues organizations of all sizes. And the more remote workers you have, the more challenging it can be for your IT staff to keep track of all the remote endpoints on your network.

Endpoints are a continual target for malicious actors, and with some 60% of all data breaches linked to an unpatched vulnerability, it’s clear that patching your endpoints should be a major concern. Unpatched endpoints are routinely billed as one of the leading threats to endpoint security — yet endpoint visibility remains a significant problem for many organizations. Recent statistics show that 80% of CISOs and CIOs wrongly believed a patch was deployed successfully, when it had actually failed to reach across their entire network.

Older patch management options are often lacking when it comes to endpoint visibility, but modern, cloud-native solutions, like Automox, offer full endpoint visibility — including the ability to see patch status and take action to remediate vulnerabilities in real time.
CROSS-PLATFORM PATCH MANAGEMENT FOR YOUR REMOTE TEAM

The issue of patching remote endpoints that you can’t see or track can be further compounded by overly complex patch management strategies. Legacy patch management platforms like Windows Server Update Services (WSUS) are severely limited when it comes to handling multiple OS or third-party applications — and these older options also tend to be expensive, hard to configure, and endpoint visibility is typically poor.

While your in-house team may use Microsoft Windows, your remote workers may be using macOS or Linux. Maybe your remote workers use one of the many Adobe® applications, too. Using a different patching platform for every OS and third-party application on your network is as inefficient as it is frustrating.

The limitations of legacy options can put a real crimp in your cybersecurity efficiency, especially when it comes to managing remote team security. Remote endpoints are just as likely to be attacked as any other part of your network — if not more so — and ensuring patches are deployed across your entire network can be next to impossible if you’ve got poor endpoint visibility and you’re trying to keep track of everything you need to patch with multiple tools.

With a strong cross-platform patch management solution, your IT staff can secure every device on your network from one, singular location — no matter where the devices are located or what OS they’re running. This greatly simplifies the task of patching for an array of devices running different OS and third-party applications — and it increases the efficiency and effectiveness of your remote team cybersecurity management.

MANAGING REMOTE TEAMS WITH EASE

Cloud-native, cross-platform solutions like Automox offer organizations of every size an affordable, easy-to-use option for patch management. With Automox, users have full visibility over every endpoint — as well as the ability to assess patch status and remediate vulnerabilities in real time. The same interface can patch across multiple OSs, as well as third-party applications. Custom automated patching protocols and policies can be tailored to fit the needs of your organization — including your remote workers — and, as a cloud-native solution, configuration is simple.

Patch management for remote devices has long been a thorn in the side of every IT staffer, but modern solutions like Automox can help solve many of the issues that organizations face when it comes to endpoint security and managing remote teams.
Research released from Automox in partnership with AimPoint Group has uncovered some alarming gaps in how effectively organizations were patching even BEFORE most of their employees were working remotely. The data shows that prior to COVID-19, less than 50% of organizations could patch vulnerable systems swiftly enough to protect against critical threats and zero-day attacks, and 81% have suffered at least one data breach in the last two years. And that was when most employees were on the same network as on-premises patching tools.

These findings suggest organizations need a better way to patch more efficiently and effectively to secure their remote teams faster and more easily. There will likely be worrisome consequences for organizations that do not update their patching policies to reflect our new work-from-home realities.

The research, titled The 2020 Cyber Hygiene Report: What You Need to Know Now, surveyed 501 IT Operations (ITOps) and security professionals at enterprises with between 500 and 25,000 employees, across more than 15 industries and government agencies to benchmark the state of endpoint patching and hardening. While most enterprises want to prioritize patching and endpoint hardening, they are inhibited by the pace of digital transformation and modern workforce evolution, citing difficulty in patching systems belonging to mobile employees and remote offices, inefficient patch testing, lack of visibility into endpoints, and insufficient staffing in SecOps and ITOps to successfully do so.
MISSING PATCHES AND CONFIGURATIONS ARE AT THE CENTER OF DATA BREACHES

The 2020 Cyber Hygiene Report confirmed that four out of five organizations have suffered at least one data breach in the last two years.

When asked about the root causes, respondents placed phishing attacks (36%) at the top of the list, followed by:

- Missing operating systems patches – 30%
- Missing application patches – 28%
- Operating system misconfigurations – 27%

With missing patches and configurations cited more frequently than such high-profile issues as insider threats (26%), credential theft (22%), and brute force attacks (17%), three of the four most common issues can be addressed simply with better cyber hygiene.

ENTERPRISES ARE NOT PATCHING FAST ENOUGH, ESPECIALLY WHEN IT COMES TO ZERO-DAYS

When critical vulnerabilities are discovered, cybercriminals can typically weaponize them within seven days. To ensure protection from the attacks that inevitably follow, security experts recommend that enterprises patch and harden all vulnerable systems within 72 hours. Zero-day attacks, which emerge with no warning, pose an even greater challenge, and enterprises should aim to patch and harden vulnerable systems within 24 hours.

With cyber hygiene, endpoints need to be scanned and assessed on a regular basis, and if problems are found, promptly patched or reconfigured. Automation dramatically speeds up cyber hygiene processes by enabling ITOps and SecOps staff to patch and harden more systems with less effort, while reducing the amount of system and application downtime needed. Organizations that have fully automated endpoint patching and hardening are outperforming others in basic cyber hygiene tasks.

Currently:

- Less than 50% of enterprises can meet the 72-hour standard and only about 20% can match the 24-hour threshold for zero-days.
- 59% agree that zero-day threats are a major issue for their organization because their processes and tools do not enable them to respond quickly enough.
- Only 39% strongly agree that their organizations can respond fast enough to critical and high-severity vulnerabilities to remediate successfully.
- 15% of systems remained unpatched after 30 days.
- Almost 60% harden desktops, laptops, and servers only monthly or annually, which is an invitation to adversaries.
THE MODERN WORKFORCE PRESENTS A CYBER HYGIENE DILEMMA

Survey respondents are more confident in their ability to maintain cyber hygiene for on-premises computers and servers compared with remote and mobile systems such as servers on Infrastructure as a Service (IaaS) cloud platforms, mobile devices (smartphones and tablets), and computers at remote locations.

In fact, they rated their ability to maintain cyber hygiene for Bring Your Own Device (BYOD) lowest among all other IT components.

These patterns can be explained by the fact that most existing patch management tools don’t work well with cloud-based endpoints, and that virtual systems are very dynamic and therefore harder to monitor and protect than physical ones.

“We are unquestionably in the midst of a major patching dilemma which is getting increasingly worse by the day as the number of enterprise endpoints — and the typical enterprise attack surface — is growing at unprecedented rates and making it nearly impossible for organizations to keep up,” said Automox CEO Jay Prassl. “Our 2020 Cyber Hygiene Report shows a very strong correlation between automation and the ability to patch endpoints faster and proactively harden them more frequently than typical legacy systems allow. Organizations that prioritize cyber hygiene through these methods reduce risk across the enterprise, lower IT costs, and accelerate their business transformation.”

To download a copy of “The 2020 Cyber Hygiene Report: What You Need to Know Now,” please visit:

automox.com/lp/2020-cyber-hygiene
Cybersecurity Checklist for a Secure Remote Workforce

2020 and 2021 will go down as the years many organizations rapidly expanded their remote workforce. While remote work has its perks, it is not always ideal from a cybersecurity standpoint. Organizations that succeeded in this sudden, unexpected transition from on-premises to at-home work will have solved for gaping holes in their cybersecurity strategy and implemented new security policies that outsmarted attackers.

As endpoints move from in-house to an unplanned, remote environment, there can be several challenges. Legacy options for managing remote workforce security are cumbersome and are typically limited in their capabilities. Slow connections, poor visibility, and overly complicated configurations can impact cybersecurity for remote teams. And most notably, users may have an aversion to slow VPN connections — which can ultimately prevent them from receiving critical security updates.

Modern patch management solutions, however, make it possible for organizations to manage the security of their endpoints without the hassle of legacy solutions. By using today’s cloud-native approaches to endpoint management, maintaining your cybersecurity posture across your remote workforce is achievable. Here’s what you need to know to succeed.

**CYBERSECURITY CHECKLIST FOR REMOTE WORKERS**

Securing the remote workforce requires a special emphasis on following cyber hygiene basics and patch management best practices. Remote devices are often some of the most vulnerable, especially during a time when so many organizations have had to rapidly change how they do business. Utilizing the core competencies of cyber hygiene and patch management can help ensure your organization is protected, even when everyone is working from home.
INVENTORY OF ALL SYSTEMS
Inventoring all devices and software is a critical element of cyber hygiene and patch management best practices, and it is even more important for remote workers. Having a living record of all devices and software being used remotely is essential to ensuring endpoints are secured properly.

EMPLOYEE EDUCATION
Ensure remote employees can identify phishing emails and understand the basic elements of cybersecurity, such as password protection.

PASSWORD POLICIES
Remote employees should follow the same password protocols as in-house staff: creating secure passwords and changing them on a regular basis.

ENDPOINT VISIBILITY
Having full visibility over the patch status of remote endpoints strengthens overall cybersecurity efforts. Modern tools make it possible for organizations to know which devices have received critical security updates and see what still needs remediation. This enables IT staff to resolve vulnerabilities faster and more efficiently.

TRACK SOFTWARE INSTALLS
All new installs should be done correctly and inventoried appropriately. Remote workers may have additional third-party software on their devices that needs to be accounted for and updated regularly.

REGULAR PATCHING
All endpoints need to be patched regularly in order to mitigate cyber vulnerabilities and reduce the risk of attack. Patching security vulnerabilities minimizes the attack surface and reduces the likelihood of an endpoint being compromised by a malicious actor.

AUTOMATION
Cloud-based, automated tools can help organizations streamline the process of patching remote devices. Cloud-native Modern IT Operations platforms like Automox can be installed on virtually any device and simplify the process of deploying security updates to remote endpoints. Automating the patching process helps ensure overall cybersecurity efficiency, giving users the option to set a patching schedule tailored to fit their needs. With automated patching, organizations can ensure that security updates are getting deployed in a timely manner and without the hassle that comes with manual patching.

Don’t let attackers get ahead of you. By following this checklist and staying up to date with modern patching tools, organizations can stay ahead of threats, even during the most inconvenient of disruptions.
SysAdmins

Tips to consider when most of your workforce is working from home... Including yourself

With the spread of COVID-19, many organizations have quickly shifted to remote work plans to accommodate their employees and reduce the spread of the virus. While you hear a lot about the shift from working effectively in the office to working effectively at home, you don’t hear a lot about how best to manage and support remote workforces when you, too, are remote.

As a system administrator, if you are currently working remotely, here are some tips to consider on how to be effective while you (and most of your office) are working from home:

**Make sure you have enough VPN licenses**

You probably provisioned those initial licenses expecting only a fraction of your workforce to be on the VPN at any given time. Make sure you get a new count of those needing VPN access to internal resources and purchase licenses accordingly.

**Ensure that all of your monitoring systems and dashboards are easily available from home**

You might be used to having everything on a big TV or monitor at work, and now your screen real estate is more limited. This is the perfect excuse to get that third or fourth home monitor. If you rely on VPN connectivity to view the status of your remote endpoints, make sure you have a well-thought plan to keep your employees connecting to the network to ensure compliance with corporate patching protocols and configuration updates. Or, maybe it’s time to consider a cloud-based solution that removes the barrier of having to connect to a VPN to receive patch updates.
Enable remote server and desktop management tools, such as iLO and iDRAC, on your servers and endpoints

You may have some servers in your office that you haven’t bothered to do this for because it’s easier to go to the server room. Now that you’re remote, you don’t have that option. If you have to reboot a server or an endpoint after a patch, what if it doesn’t boot back up again?

Maintain access to your on-premises patching server

Speaking of VPNs...recall that shiny, new on-premises patching server you just bought? If you didn’t address the first bullet, then the majority of your organization won’t be able to access it. You’ve now gone from a handful of remote employees who are laggard with their patching, to almost all employees. Your exploitable attack surface for known vulnerabilities has gone from a manageable percentage of remote employees to the entire inventory of company laptops.

Set your remote employees up for success

For some employees, working remotely is a dream come true, for others, not so much. Educate your remote users on how best to work from home, how to connect to the VPN, and how to reach you if they need help. If you don’t already have a help desk system, now’s a good time to get one. Additionally, consider investing in good headsets and microphones. There’s nothing that makes virtual meetings as annoying as bad sound quality.
Set YOURSELF up for success
As an IT admin, having redundancies and contingency plans is the key to keeping businesses online and operational. It’s no different at home. Have a backup plan if your internet goes down. The easiest way to do this is to make sure your phone data plan has a tethering option. Also, have a backup router in case any of your home hardware fails.

Get yourself a rock-solid software deployment solution
Now that everyone is working remotely, it’s going to be harder to troubleshoot and tinker with any issues in deploying software. Look for opportunities to leverage free use of your workplace software. Also, companies like Zoom, Microsoft, Google, Slack, and many more have free or lost cost offerings. There are many online “best of” listings to help you evaluate video conferencing software to help you support remote users.

Make sure you’re ready for a zombie apocalypse
And, while you’re doing all of the above, you may as well be prepared for an invasion of the walking dead. Okay, maybe that was a bit of a stretch. But you can take some basic precautions such as having sufficient battery backups (uninterruptible power supplies) for every computer and your home network gear to keep you working during a power failure.

With some thought and preparation, you can keep your employees and your equipment protected from known exploits and viruses when working remotely from home. But, consider this: Once you’ve established your remote-work response, this short-term solution could be a viable long-term plan.

Take this opportunity to research and invest in modern, innovative technologies that can effectively set your organization up for success and keep your endpoints secure for the long haul — in crisis or not. It’s a no-brainer.
Effectively Managing Remote Teams While Keeping Your Company Secure

There are many steps managers can take to ensure their remote workforce is operating at its best — and its most secure. Taking the time to treat your remote workers like in-house employees is crucial to managing remote teams effectively. Which means keeping your remote team functioning the same way you manage your in-house team is key to keeping your organization secure at every endpoint.

HIRING REMOTE WORKERS DOESN’T HAVE TO BE A SECURITY NIGHTMARE

It’s one thing when a long-time, trusted employee asks to work from home a few days a week. But hiring remote workers from scratch can be a daunting task for management — and your IT team. Every remote worker is another endpoint to keep track of, and if your remote workers have access to your organization’s network, securing those endpoints is essential.

For organizations looking to secure their remote endpoints, cloud-native management tools are a unique solution to a growing problem. These tools reduce your corporate reliance on a VPN as a means to provide security or system updates to your distributed corporate endpoints. Remote workers simply connect to the internet, and your IT management tools can push any necessary updates to ensure these devices are adequately secured in a timely, efficient manner.
MANAGING REMOTE WORKFORCE CYBERSECURITY REQUIRES GOOD COMMUNICATION

Good communication is necessary for managing all your employees, regardless of where they work. It’s easy to keep the lines of communication open with in-house employees, but remote workers miss out on in-office interactions that help build rapport and give them the opportunity to spontaneously discuss issues.

Experts suggest taking one hour a week to have one-on-one conversations with your remote team members over video conference to give both parties visual cues that can’t be shared over the phone or in an email. Communicating with your remote team members regularly will help them function better as a whole — and it will give them a sense of inclusion.

Employees who regularly work from home can miss out on critical security updates. Whether your company is issuing directives on dealing with phishing emails or deploying new patches, it’s essential that you keep your remote team in the loop. More importantly, if a remote worker has a security concern, such as a patch that failed on their end, they need to be able to communicate that information to your IT team as soon as possible.

Cloud-native patching tools, like Automox, offer full visibility across all endpoints, no matter where they are located — as well as the ability to remediate vulnerabilities, even on remote devices. For your tech team, this simplifies the task of resolving vulnerabilities on remote devices and increases their efficiency.
**TIME ZONES AND REMOTE TEAM MANAGEMENT FOR CYBERSECURITY**

Living in different time zones can make remote team management especially difficult. This is especially true when it comes to patch deployment. While a one-hour time difference may not be a huge deal, more drastic differences can really become a hindrance to your security efforts, depending on how your system is set up.

If your IT team needs to deploy a systemwide update, your remote workers should know about it. Depending on how your network is configured, they may need to ensure their devices are turned on. And at the very least, it’s nice to give your remote employees a heads-up if there’s going to be a major update the next time their device turns on. With Automox’s single console, you can take some of the pressure off your team because you can remediate vulnerabilities from one central location, without needing multiple other programs.

**REMOTE TEAM PROJECT MANAGEMENT**

Good communication at the right time is important for keeping your remote workers happy, but it’s also essential for good management. Be open with your remote workers about what your expectations are in terms of turnaround time, quality, and quantity. Making sure everyone is on the same page is key to ensuring projects are completed on time.

Organizations with remote teams can also employ project management tools to help keep the team up to date and ensure that tasks are being completed as requested. While it can be tempting to rely on email, project management for remote workers can get out of hand pretty quickly if documents and conversations aren’t organized. Project management tools can help your team make the information they need and share readily accessible.

Effective collaboration is essential when it comes to project management for remote teams. In-house employees have the benefit of communicating in person, getting to “whiteboard” ideas, and speaking more casually about work. Remote teams miss out on this, but with a solid project management system in place, you can keep your remote team members “in the loop” more easily.
One of the most important tenets of remote team management is cyber hygiene. Patch management and endpoint security are particularly concerning when it comes to remote workers. If your remote team is using devices (or endpoints) that are part of your company’s network, you need to know if those devices are being patched and updated regularly.

Unsecured endpoints are a major risk to every organization’s security, regardless of size. Managing cybersecurity needs across a remote workforce can be a difficult task — especially if you have workers who are using different OSs. Many on-premises patching solutions are limited in terms of endpoint visibility and ability to transcend OS. Limitations in endpoint visibility are already problem enough; most CIOs and CISOs say that patches they thought were successful actually failed to deploy across all their endpoints.

If you have a remote team, it’s essential to make sure those endpoints are secure, regardless of whether they are BYOD, company-owned devices, devices that are part of a domain, or devices that aren’t. Modern, cloud-native solutions, like Automox, give you full endpoint visibility — including remote endpoints. With Automox, users can see in real time which patches were successful and which vulnerabilities need to be resolved, as well as take action to remediate those vulnerabilities. There are many things to consider when it comes to successful remote team management but securing your remote team should be your top priority.
How the Cloud Improves Endpoint Security of Your Growing Remote Workforce

CHALLENGES IN SECURING THE REMOTE WORKFORCE

The remote workforce can pose a significant problem for many organizations — it introduces unique challenges for IT security. According to a 2018 OpenVPN survey, 90% of IT professionals who responded reported that they believe their remote workforce poses a security risk. And 36% reported that a remote employee was the cause of a security incident. Apricorn reported that 57% of IT decision-makers in the United Kingdom believe that remote workers will expose their organization to the risk of a data breach. Like any other disruptive transformation, the speed to adopt a flex-work model has often outpaced the ability to effectively manage new risks.

Organizations have to ask themselves how they are managing their remote endpoints. Specifically, do they have continuous visibility into something that isn’t in their corporate network? If the answer is that they don’t have continuous visibility — and most likely, they don’t — that’s a serious issue.

With traditional security and IT tools that were architected to be in a data center, when an endpoint leaves the corporate network it basically disappears or goes “offline.” The prolonged absence from regular cyber maintenance intervals results in a significant number of missing patches and configuration drift as those traveling endpoints fall further and further out of compliance. Without continuous ongoing cyber hygiene, the exploitable attack surface on these endpoint fleets may expand to the point that they are easily compromised. This is an unacceptable price to pay, just because endpoints aren’t connected to the corporate network. In order to get around this, some organizations require their endpoints to connect back into the corporate environment via a VPN for certain tasks, such as patch management. But for the end user, that can be an awful experience.
IMAGINE THIS SCENARIO:

You’ve been working from various coffee shops and other locations because you’re traveling to various meetings throughout the week. But when you get back to your home office and have to connect back to the VPN to access the corporate network to do something, instead of getting access to the internet and all of the information, services, and tools you need to get your job done, you get inundated with a myriad of patch management tasks because you haven’t shown up on the corporate network in a while. These tasks are all queued up, and you have to reboot five times before you can even begin working again. This scenario just further enforces behavior of remote employees never connecting to the corporate VPN if they aren’t required to do so.

Consequently, many organizations are dealing with the fact that they have to either accept degraded protection and compliance levels as a result of lacking visibility or come to terms with the reality that they’ll be frustrating their end users by jamming patches and policy updates down their throats every time they connect to the corporate VPN. Organizations can reverse publish on-premises services in their network demilitarized zone (DMZ) as a workaround for these legacy technology implementations, but this approach doesn’t scale to the reality of the remote workforce.

If remote endpoints are the new norm and trying to shoehorn them back into a corporate network to manage and secure them isn’t working — then what’s the answer? It’s simple — a globally available cloud-native cyber hygiene service. Like any other critical Software as a Service (SaaS) function, the ongoing maintenance and security for remote work fleets is best serviced through highly scalable and always connected cloud services. After all, remote workers are always connected to the internet — just not necessarily to the corporate network. By making a secure, globally scaled SaaS always available to them, organizations can maintain continuous visibility and control.
The True Cost Burden of On-Premises Patch Management Solutions

Many organizations are caught unaware of the actual cost of their software and solutions. Oftentimes, the sticker price of the software is the assumed cost, but there are many hidden setup and maintenance costs necessary to run your on-premises patch management tool.

THE HIDDEN COSTS OF ON-PREM

There are three main areas in which hidden costs arise with on-premises patch management: hardware costs, software costs, and operational costs. Automox can reduce your total cost of ownership by up to 80% with our cloud-native, easy-to-use patch management and endpoint hardening platform. Find out exactly how much time and money you could be saving with this TCO Calculator.
HARDWARE COSTS
Hardware costs can include servers, storage space, network infrastructure, data backup and replication, and hardware redundancy. Naturally, if you are using an on-premises solution, you will bear the burden of deploying and maintaining the physical servers on which it will run. You can’t run a legacy software solution without good old iron to run it on, of course. A typical deployment will require at least one central management server as well as a server at each physical site to distribute patches.

SOFTWARE COSTS
The second major area is software costs. Once you rack your pile of gear, it’s time to get your OSs, databases, management, performance, reliability, and security software deployed. Each of those components carries its own extra costs. Costs can quickly top $200 per endpoint over three years, even with ideal conditions.

OPERATIONAL COSTS
Finally, once you get your hardware and software squared away, it’s time to get busy actually putting it all together and running it. This comes with a host of new costs. Operational costs can quickly become the single largest line item in the TCO for an on-premises solution. You will need to consider the cost to design the system, deployment, testing, hardware maintenance, software maintenance, rack space, and heating and cooling costs just to maintain the infrastructure needed for your deployment.
The Automox platform is designed to treat endpoints as equals, providing organizations equal visibility control whether dealing with remote endpoints or on-premises machines. Automox is a cloud-native solution, which means that any endpoint connected to the internet is essentially in continuous contact with us.

Automox
A modern approach to remote workforce use cases
There’s no routing through a corporate network or VPN, linking back so that a command or control server can see that remote endpoint and manage it. As long as you’ve got an Automox agent or sensor installed on an endpoint, the Automox platform can manage corporate-owned devices, BYODs, and devices that are part of a domain or devices that aren’t — it doesn’t matter.

Not only does this cloud-native approach work to solve the remote workforce issue, it’s doing so in a way that allows organizations to avoid incurring any physical or on-premises infrastructure costs. With Automox, you don’t have to install and set up a management server or install distribution points in your corporate environment, you’re not forced to maintain costly VPN clients on remote endpoints, set up regional patch repositories, or even externally publish your patching service in the DMZ or perimeter network. With Automox’s cloud-native solution, organizations have continuous global visibility of their remote endpoints and can effectively automate patch management and other cyber hygiene actions on a consistent cadence that impacts employees far less.

Alongside digital transformation comes pressure on IT teams to keep pace with the rapid speed of business, but legacy patch management tools are particularly prone to shortcomings when it comes to the remote workforce, whether it’s a poor experience for end users or something even worse: the acceptance of having a vulnerable attack surface. Fortunately, cloud-native solutions like Automox solve the problem of continuous connectivity and visibility into these remote systems because there’s no reliance on internal or on-premises infrastructure, and no matter where an endpoint is, the Automox platform is always in communication.

**ABOUT AUTOMOX AUTOMATED PATCH MANAGEMENT**

Facing growing threats and a rapidly expanding attack surface, understaffed and alert-fatigued organizations need more efficient ways to eliminate their exposure to vulnerabilities. Automox is a modern cyber hygiene platform that closes the aperture of attack by more than 80% with just half the effort of traditional solutions.

Cloud-native and globally available, Automox enforces OS and third-party patch management, security configurations, and custom scripting across Windows, macOS, and Linux from a single intuitive console. IT and SecOps can quickly gain control and share visibility of on-premises, remote, and virtual endpoints without the need to deploy costly infrastructure.

Experience modern, cloud-native patch management today with a 15-day free trial of Automox and start recapturing more than half the time you’re currently spending on managing your attack surface. Automox dramatically reduces corporate risk while raising operational efficiency to deliver best-in-class security outcomes, faster and with fewer resources.