ManageEngine

Manage and **secure** your remote workforce

Remote workers use a range of internet-connected endpoints to get their work done, which poses a threat to your organization's overall security posture. Christopher Sherman, a senior analyst at Forrester Research, says, "With much of the global workforce moving to work remotely, endpoint security has never been more critical." If endpoints and remote workers aren't managed pertinently, your organization will be at risk.

Endpoint management and security will shape the future of work, and ispoised to be a long-term solution for remote work. That said, now is the right time to double-check your remote work capabilities and implement some best practices to enforce proper remote work.

Best practices

to secure your

remote endpoints

Not every vulnerability needs immediate patching. Assess them!

You might be inundated with vulnerabilities, but not every vulnerability requires immediate patching. Automate the assessment of each vulnerability, configure thehealth of your systems, and deploy patches when the need is dire.

Test every patch before you deploy it

It is vital to test each patch before rolling it out to machines, especially if it's a server-installed machine.

Curate a list of malicious executables, and block them completely

Despite a foolproof security system, malicious executables still sometimes find their way into networks. Curate a list of malicious executables, and block them completely by providing the hash value of the executable.

Schedule and automate OS updates

More often than not, users tend to skip OS updates. Cybercriminals often exploit known vulnerabilities in outdated OSs to attack the endpoint and use it as a conduit to attack the entire network. Always automate OS updates and schedule the update for specific groups of users to prevent bandwidth bottleneck issues.

Audit high-risk software and system misconfigurations

Look out for the presence of high-risk software such as end-of-life, peer-to-peer, and remote desktop sharing software. Overlooked and default configurations pave way for a misconfiguration that can be exploited easily. It is cardinal to audit configurations proactively to keep cyberattacks at bay.

Configure profiles to impose stringent policies on mobile devices

Publish profiles for implementing Wi-Fi policies to prevent mobile devices from automatically joining Wi-Fi networks, configuring VPN settings to authenticate every connection to the corporate network, and restricting device features such as Bluetooth and camera.

Best practices

to manage your

remote users

Group the rudimentary configurations as a single collection of configurations

Group baseline configurations for securing browsers, USBs, and firewalls; mapping drivers; managing files, folders, permissions, and power; and standardizing the display of monitors. Ensure that every new system that joins this domain has these configurations in place.

Tailor the process of deploying business-critical applications

Ensure that the recommended versions of business applications are present on all endpoints. Customize the process of deploying applications by defining pre-deployment activities such as checking the free disk space and previously installed versions, and post-deployment activities such as creating a shortcut.

Centralize the management of browser add-ons

Detect the presence of harmful add-ons, and disable extensions that use permissions that could lead to exfiltration of data. Distribute extensions from a central repository, and spot outdated add-ons.

Deploy appropriate geofencing policies depending on the location of devices

Create virtual fences, and configure relevant geofencing policies to determine the degree of access to corporate data depending on the location of the remote endpoint. Define a compliance rule, and take necessary action on non-compliant devices.

Best practices to

ensure productivity

Prohibit the use of blacklisted applications, and uninstall them automatically

Compile a list of applications to be blacklisted that hamper productivity and instigate compliance issues while telecommuting. Uninstall them automatically if detected, and enable users to raise a request if they require access to any particular application.

Empower users to install or uninstall applications at their disposal

Silent installation of applications might not prove to be a boon during remote work, owing to the varying bandwidths of the users. Instead, publish software on the self-service portal, and empower users to install applications based on what they need and the bandwidth available to them.

Track web activity of users and apply a web filter to restrict access

The use of the internet is ubiquitous and tends to put the users off their stroke,wherein the users might start browsing sites that are not related to work,and could be malicious.Track the web activity of users, and apply a web filter to restrict access to unproductive and malicious websites.

Best practices for

remote troubleshooting

Transfer dependent files during a live session

Instead of resorting to traditional file transfer methods, transfer the necessary files onto the target machine while troubleshooting. You can use the integrated two-way file transfer tool to ensure all the dependent files are present on the target machine for faster resolution.

Seek the guidance of adept technicians for quicker resolution

Often times, more than one technician works on a ticket. It's recommended technicians collaborate with each other to procure necessary insights. Furthermore, you should seek the guidance of adept technicians to resolve complex issues more swiftly.

Shadow novice users and intervene when required

Remote work makes training a cumbersome process. You can give new technicians a hands-on experience while shadowing them silently. For demonstration purposes, you can intervene and take over.

Leverage built-in communication channels

Expedite your troubleshooting process by leveraging built-in communication channels such as text-based chat and voice and video calls. This will help you in acquiring the necessary information from the end users. Moreover, you can keep end users in the loop about every action that's been taken on their endpoints.

Record remote sessions and maintain a history of chat scripts

Automatically record remote sessions for auditing and training purposes. Additionally, if your organization is attentive to compliance, you can export the chat scripts, and request the user's approval every time you initiate a remote session.

Best practices

to safeguard your corporate resources

Securely distribute and manage corporate documents

Create a content repository, and distribute the necessary corporate documents from this repository to keep tabs on the resources accessed. Prevent users from sharing the content with other devices or copying it to other apps to help prevent data leak.

Distribute your certificates from the repository to manage expiration and renewal

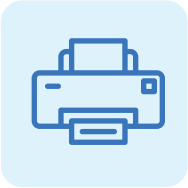
Distribute your certificates from a central repository to simplify the management of certificate expiration and renewal. In addition, enable certificate-based authentication for corporate data security.

Oversee admin privileges to keep privilege elevation attacks at bay

While installing software, it is important for organizations to grant administrative privileges as and when needed. There is no limit to which user requires what degree of access. Always keep tabs on the admin privileges granted, and ensure to revoke them when no longer needed.

Isolate your browsers, and render unproductive sites in a virtual browser

While using browsers for work, users tend to get sidetracked and browse sites that are not related to work. Whitelist all the work-related websites that will be rendered in a normal browser, while anything that deviates from this list will be rendered in a virtual browser to secure the organization against the risks non-work-related sites carry.



Regulate the use of external devices to prevent exfiltration of data

External devices are an integral part of every organization, the use of which is inevitable. Implement a Zero Trust approach, wherein you block the use of most external devices, especially USBs, and allow the device only if it’s from a trusted vendor.

Ensure that you run only enterprise-approved apps on mobile devices

Bring your own device (BYOD) policies eliminate the need to provision remote work devices. To ensure data security, it's important to run only enterprise-approved apps on such devices. Distribute apps from the app repository, and store the corporate apps on a separate encrypted container.

Other best practices you should follow include auditing event logs to detect anomalies proactively, automating the generation of predefined reports, and exporting reports to analyze the current structure and to make necessary amendments.

The proliferation of endpoints and users makes it overwhelming to keepa track of events. This is where alerts for real-time management of your endpoints comes in handy. Break the bandwidth bottleneck by associating different deployment policies for different group of users that cater to their circumstance.

Integrate your help desk with an endpoint management solution to equip your help desk technicians, so they can offer speedy resolution of issues right from the ticket window, because one of the last things any technician wants is a flooded help desk.

Implement these best practices right away!