MAKING PEOPLE PRODUCTIVE

Remote Worker Monitoring with GroundWork Monitor

GroundWork White Paper by Thomas Stocking

GroundWork Monitor is not an EMS

We believe in enabling workers to be productive remotely, and in trusting them to do so. Instead of enforcing some Big Brother scheme and watching remote worker's every move, we think it's far better to monitor the availability and performance of the critical resources that make people productive. If those are all good, then productivity is up to the employee. And the best booster of productivity we have found isn't even a technology: it's trust.

Request a Demo

For more information or to request a demo of GroundWork Monitor Enterprise please call 1-415-992-4500 or email us sales@gwos.com.

Keeping Track of Resources to Support Remote Worker Styles

The remote worker lifestyle has been with us for some time now. With the advent of the recent COVID-19 pandemic and the stay-at-home orders, remote work is now the only work many of us can do. While there are advantages like a lower carbon footprint, there are disadvantages too. Not only do you not have a reason to drive your pickup truck, but you also are using broadband Internet, and probably also VPN technologies, which are points of failure in getting your work done. You may use a remote desktop to connect to a computer on your actual desk in the office, or maybe you use virtual desktop technology like Citrix.

Whatever your remote worker style is, at the moment, it's front and center, and your IT department needs to keep track of the resources that support it.

GroundWork can help with monitoring that infrastructure. Your IT department can set up monitoring and access it from remote sites, allowing monitoring of your Citrix server, your VPNs, and even your desktops. Monitoring these assets provides you with the assurance you need for knowing you have connectivity and performance from your email systems, your VPNs, and your remote desktops. This article is about how that works, and the features GroundWork provides that are the most useful in the context of remote worker support.

What do you need to access?

So if you are working remotely, what do you need to access? The answer to this question depends on what your role is - what type of remote worker you are. We have found many different ideas about remote worker types out there. We decided that for monitoring purposes we would keep it simple and mapped the resources that people typically need into three basic categories:

Online Only

This kind of worker is a consumer of open online resources like email, Salesforce, Slack or other chat platforms, and company portals. There's no need for an Online Only worker to access resources behind the firewall to do their job. Many sales associates, executives, and customer service representatives fall into this category. The advent of SaaS offerings has made this type of worker able to be quite productive with minimal IT infrastructure supplied by the company they work for, and hence a minimal monitoring requirement.

Remote Desktop

The next level of a remote worker is one who needs access to more than just online, public-facing portals, and services. Not that they don't use those, however, they also need to access confidential files and information that doesn't commonly go off-site. For example, executives frequently need access to personnel or financial data that would be inappropriate to store on a laptop at home.

Remote desktop is enabled by technologies such as Citrix, which virtualizes the MS Windows desktop in servers as a virtual machine, fully loaded with the software you need to be productive, with access rights assigned according to your user and role. There's more to it than that, of course, but this kind of remote desktop is distinct from accessing your desktop remotely.

If you have a desktop machine sitting in your office, it's already set up the way you want it since you have used it there for some time. You just need to access it. Technologies like Microsoft Remote Desktop or VNC can (with enough bandwidth) make it seem almost as fast as being at your desk.

Remote desktop workers also rely on a Virtual Private Network (VPN) connection to secure and encrypt their traffic.

Remote Administration

The remote administrator is a privileged user who has access to more than just their standard desktop. Administrators typically have a second VPN connection for emergencies and can log in to the core networking and server systems (like the monitoring system) that the company runs on.

What to Monitor?

When considering what to monitor to enable remote workers, one has to think about what resources those workers need.

Online Only workers need the least:

- Internet Connectivity
- Access to email
- Access to company portals
- Access to SaaS portals

If you consider monitoring these resources, it makes sense to do so from the point of view of the remote user, that is, from their remote system. It's pretty apparent when the Internet is down, but what if latency is high to the company portal? That might make it harder to work and should be considered. Latency and availability data for all critical online resources should be gathered and tracked.

How to Monitor?

Setting this up is trivial to do, as long as there's a way to get the information back to the monitoring server securely. The use of https transport from GDMA (GroundWork Distributed Monitoring Agent) with assigned certificates can make this at least as secure as regular web traffic.

To cover remote desktop workers, you can adjust coverage from the desktop perspective to include availability monitoring of the VPN endpoint which provides access to the remote desktop itself.

You should also consider that in the remote virtual desktop case, there are servers that serve up those desktops which should be monitored. If you are running Citrix, you can use the GroundWork Citrix profile to monitor those servers directly. The GroundWork Citrix profile keeps track of user sessions, memory, CPU resources, and other performance and load factors that help you optimize the experience of users accessing them.

When remote desktop users are frequently working with a personal office desktop or laptop, we recommend measuring the same sorts of latency factors for public online resources, as well as for the usual internal resources like ticketing systems, databases, and file servers. There isn't much of a need to place a GDMA agent on the office desktop, though, since the GroundWork server can collect the same data (or a close approximation) by checking those resources directly, as long as it is in or near the same network location as the workstations.

Common to remote desktop and remote administrator workers are the essential VPN endpoints. These systems are networking gear, typically fairly sophisticated from a security point of view, with

secure encryption and authentication features. Most networking gear is easily monitorable with SNMP, and GroundWork Monitor includes many firewalls and VPN endpoint profiles, so getting user session data, throughput, and access logs from these devices is a common practice. It's also crucial to monitor not just the primary VPN endpoints, but the administrator's emergency endpoints as well, to make sure you aren't locked out when you are least able to run into the office.

There's more you can do to ensure the productivity of your remote workforce. Some organizations may find the remaining considerations here more valuable than those above. Read on and see for yourself.

Network Policy Monitoring

One of the critical things to do in building trust in an organization is to establish policies. I'm not talking about the dress policy or the travel or expense reimbursement policy. I'm referring to network utilization policies. Having policies in place that are clear, fair, and communicated to everyone builds trust. But how to enforce those policies without turning into Big Brother? Well, every organization is different, but there is a flexible tool in GroundWork Monitor to do precisely this - the NeDi policy engine.

If you implement NeDi (usually just a matter of typing in the SNMP credentials) and enable the NetFlow and/or sniffer functions, you can get a pretty good idea of where your bandwidth is being consumed, and where each computer is connected to the network, and how. If people start streaming video to their office desktops, it shows clearly on the graph where the data is coming from, and where it's going. You can also find out if data is flowing out through unauthorized channels you might not notice otherwise. No one likes data exfiltration. You can then take the appropriate actions to enforce your policies.

Have questions?
Email us at support@gwos.com