White Paper

ITSBU

Remote Device Management Services: The benefits for Organizations

Remote Device Management (or RDM for short) is a way for organizations to outsource the ongoing administration of device security, monthly deployment of Windows updates, and the selection of third-party application patches across laptops, desktops, and servers. This offers a layer of protection that keeps servers and devices secure against all kinds of online threats.

Because of ongoing, relentless digital attacks and threats to servers and devices, it's imperative to create and execute an effective remote device management program. A program like this adds multiple layers of security to systems and networks, all while reducing the likelihood of attack vectors.

In this white paper, we'll cover:

Why it's beneficial to invest your dollars into a strong RDM approach

The various types of digital shielding that RDM includes

How this kind of management works to keep your organization protected

Why Organizations Need Remote Device Management

First, you might be wondering if this kind of setup is even necessary. After all, most applications have their own updates. Or you might even already have anti-virus software or resources in place. That should be enough, right? It's important, however, to keep in mind that the **cybersecurity landscape is everchanging,** and to keep up with the shifts that occur on a constant basis, you'll need to be aware of what kinds of threats are out there that would demand this kind of approach from your organization.

Get up to speed with these quick stats and facts about the kinds of threats that were reported in 2024 alone:

- Cisco reported over half (54%) of organizations experienced cybersecurity incidents surrounding phishing and credentials stuffing.
- Sophos and CrowdStrike saw a notable uptick in measures and malware updates designed to aid in credentials theft.
- Speaking of CrowdStrike, their July 2024 global outage halted major airlines and disrupted banks, amongst other things— a sign that reactive approaches are no longer sufficient to keep your organization and its data safe.

Keeping this data in mind, it's crucial to not only know the "why" behind the digital threats present in any organizational environment, but also, the "why" behind the benefits of proper remote device management.

> “
>
> ***PROTIP:*** Be aware that the software and tools required for organized, effective RDM are typically leveraged by MSPs - because too many individual organizations ***cannot*** justify the resources required for a 'single pane of glass' view over ***all*** RDM activities.

Here are some of the positive aspects we've seen as a third-party RDM provider that circumnavigate some of these common pitfalls:

• By having an ironclad **device management plan** in place, you can benefit from **scheduled and automated patching** that helps keep all machines compliant and up to date.

• **Network traffic scans, behavioral analysis, anti-phishing, DNS filtering, disk encryption, and document backup** complement the other pieces to create a stronger shield for the organization.

• You'll enjoy **savings on headcount and infrastructure costs**, with more time to commit to strategic projects and growth versus constant patching.

• In case of an emergency, secure backup can be another benefit of RDM. Whether it be a natural disaster or global IT outage, **backing up your data with a great RDM approach will prepare you for when an emergency inevitably occurs.**

Based on what you know so far, you'll want a strategically sound approach to easy remote device management— and, in a way that proactively anticipates the kinds of threats and obstacles you'll face as you manage your tech stack and data.

The Kinds of Protection that Remote Device Management Provides

Think about going out on a cold winter's day: You're going to need ample amounts of layers you can easily manage to protect yourself not only from the cold itself, but also, other elements that nature may throw your way. This can range from the outerwear you choose to the way you protect your immune system from the seasonal flu with vitamins and good dietary choices.

The same is true for your organization's server and related devices. And while no solution is foolproof, adding the right digital layers of protection makes attacking and hacking that much more difficult. In short, it hardens your organization's digital "immune system" against possible threats or infections.

First, it's important to know what the current landscape looks like when it comes to cybersecurity threats. Do any of these threats sound familiar? Has your organization dealt with managing the fallout?

1. Inconsistency in cybersecurity enforcement

2. Negligence in user awareness training

3. Shortsightedness in the application of cybersecurity technologies

4. Complacency in vulnerability reporting

5. Inflexibility in adaptation after a breach

6. Stagnation in the application of key prevention techniques

7. Lethargy around detection and response

While these obstacles can certainly be a thorn in your side, they do not have to be. Knowing exactly what threats you're exposed to daily can make selecting the right RDM partner a strategic breeze.

Here's a convenient list of layers that you'll want to consider when choosing an in-house solution or partner-provided RDM solution that can meet your unique security needs:

- **Anti-malware measures**
- **AI-based behavioral analyses**
- **Network traffic scans**
- **DNS-based filtering, including:**
    - Content control
    - Anti-phishing
    - Blocking malicious threats/scripts at the DNS level before rendering to any browsers.
- **Firewall management**
- **Disk encryptions**
- **Endpoint backups**
- **Ready-to-follow Document Incident Response plans**
- **Proactive monitoring and incident management, including:**
    - Smart status (impending disk failure)
    - Low disk space
    - High resource utilization

Wondering about what solutions will work best for the security you need? You're likely already aware of solutions like endpoint detection and response (EDR) and Domain Name System filtering (DNS filtering).

But, as we've already seen, relying on just one or two of these kinds of solutions won't be enough to truly protect your organization. Look at the table below, which compares the benefits of security integrated into the Operating System (OS) versus layering on solutions including traditional anti-virus, EDR and the enhanced benefits of DNS filtering:

Program Features	OS Level Protection	Traditional Anti-virus	EDR	DNS Filter
DNS level blocking of malicious threats/scripts				X
Domain name Allow/Block list policy				X
Heuristic blocking of suspicious domains				X
DNS level blocking of botnet and cryptomining sources				X
Application traffic content control				X
Website content control		X		X
Anti-phishing	X*	X		X
Disk Encryption Control	X	X		
Anti-ransomware	X**	X	X	
Software firewall	X	X	X	
Malware detection using heuristics	X**	X	X	
Threat behavioral analysis		X	X	
Pre-Execution program analysis			X	
Machine Learning / AI enabled threat dection			X	
Enhanced quarantine (”Disconnect from network”)			X	
Automatic file rollback (Whindows OS only)			X	
Real time file analysis			X	
Signatureless detection engine			X	

*Windows only, provided by Microsoft Defender Smartscreen

**Windows only, provided by Microsoft Defender Antivirus

How Remote Device Management Works

Once you strategically determine what your remote device management plan will cover, you’ll need to identify how your plan will work to your organization’s overall benefit. At Mechdyne, we believe that knowledge is power, so we recommend saving this handy graphic to quickly reference how this process works as you create your ideal strategic plan for RDM at your organization.

01

Deploy probe software to select devices within an organizations digital environment.

* Probes should be able to scan the entirety of the network looking for new devices to the environment that should be added to managed patching and security to reduce gaps in coverage.

* If you have a comprehensive plan, your RDM solution should cover these activities fully.

02

Poll all devices with probes, with a comprehensive suite of data reported back to the Central Management Server (CMS)

* Your CMS setup should allow devices to be discovered and subsequently mapped/categorized in a way you can easily access and understand.

* Generally requiring installation of an administrative agent and protective software onto laptops/desktops, there are other management solutions for phones and tablets such as Microsoft Intune or JamF.

03

Transfer responsibility of security updates to automation via the CMS.

* The CMS program you choose should have the ability to commant devices to run various administrative updates such as anti-virus scans, update definitions, application deployment, and the execution of reboots.

04

Maintain and monitor your chosen cybersecurity layers, all while gathering pertinent data for ongoing strategic updates.

* As you monitor your devices for any issues, your CMS approach should be able to help you detect any issues or obstacles as they arise.

* The right strategy can also factor in the need for backing up end-user files while also securely storing data within an encrypted, cloud-based vault, all for the purpose of on-demand recovery.

While you may have your own in-house solution for managing your service desk, it's important to remember the objective, third-party eye that an outsourced IT solution can provide in this case. A partner like Mechdyne can identify gaps and obstacles in your current oversight of your tech stack to provide an unbiased analysis of where you're at, and a recommendation of how you can get to where you want to be.

Closing the Gaps with Remote Device Management

Choosing the right RDM approach for your organization will require you to know where the cybersecurity industry has been, and where it's going in the future. It also demands a realistic and honest picture of where your organization currently stands with its own cybersecurity strategies. No two threats are the same, so flexibility and adaptability are key in managing how you respond to threats and obstacles. By adopting a partner-provided RDM solution, you'll be able to adopt a process that can halt or mitigate threats as they arise, all while enjoying maximizing your set budget. The digital landscape might be uncertain, but your RDM plans don't have to be!