eG Innovations

7 Myths of AVD Monitoring

How to avoid common misconceptions that limit AVD administrators

© 2026 eG Innovations. All rights reserved. | www.eginnovations.com

Avoid AVD Monitoring Myths

Azure Virtual Desktop (AVD) is a powerful and increasingly popular solution that allows businesses to provide secure, scalable, and cloud-based desktop virtualization, usually without the overhead of on-prem infrastructure.

However, many organizations underestimate the importance of monitoring, leading to performance, compliance, and cost issues.

This eBook quickly debunks several common myths surrounding AVD monitoring and will help you adopt a proactive approach that will save you time, stress and billing costs.

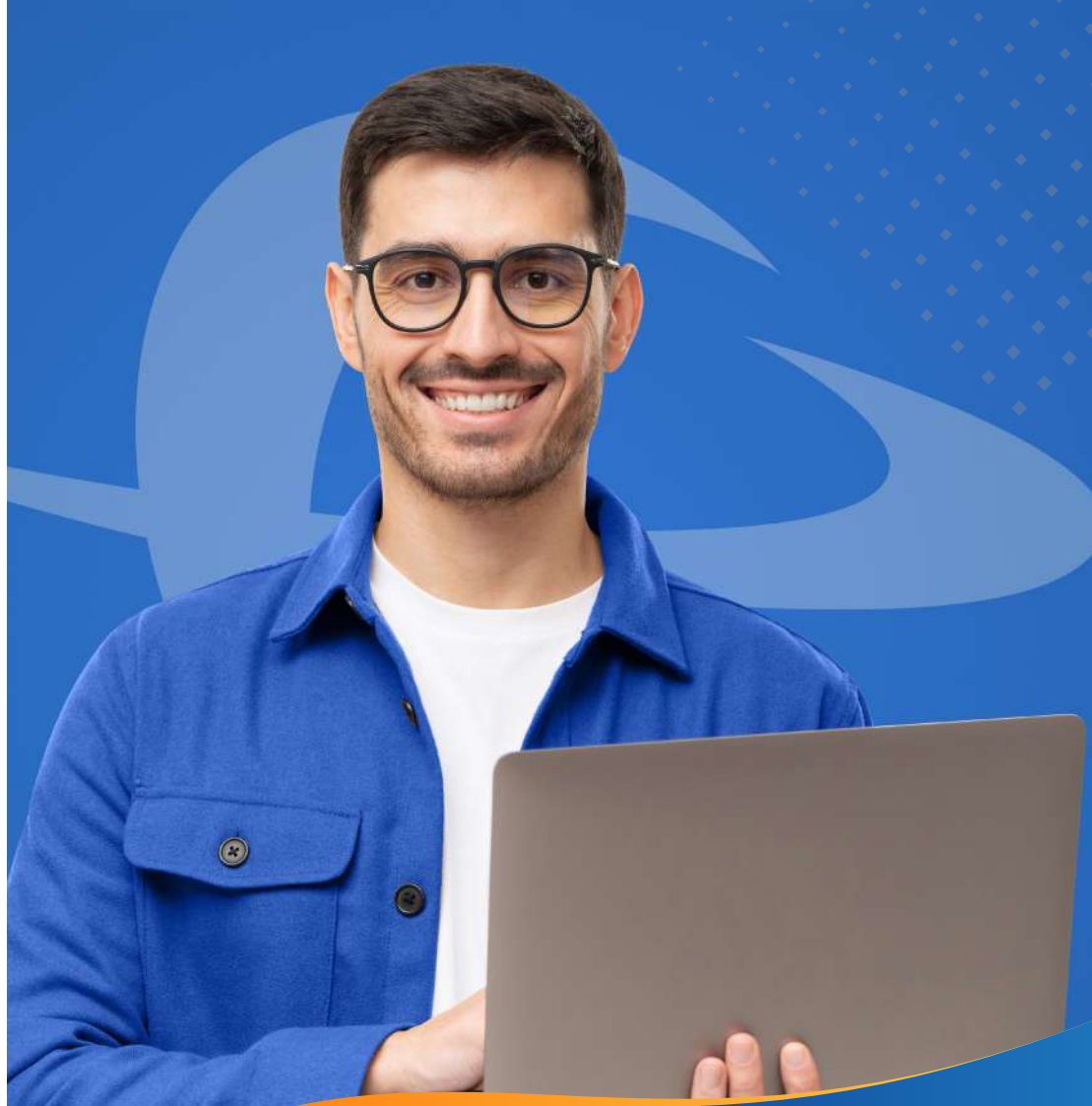
 © 2026 eG Innovations. All rights reserved.

Myth #1. "AVD is a cloud service. Microsoft manages it. I don't need to worry about monitoring and analytics."

AVD in the cloud doesn't mean Microsoft runs your workspace for you and they certainly won't pay your cloud usage costs. They keep the lights on; you own the user experience. Apps, profiles, integrations, technology choice—it's all on you.

Users don't care if it's AVD, Citrix, or Horizon; they care if it's fast and available.

When logons are slow, apps fail, or sessions drop, they call you—not Microsoft. You need the tools to pinpoint if it's Azure, the network, storage, the app, or even just bad home Wi-Fi. That's why always-on monitoring is critical—both to fix issues before they blow up and to control AVD's usage-based costs.



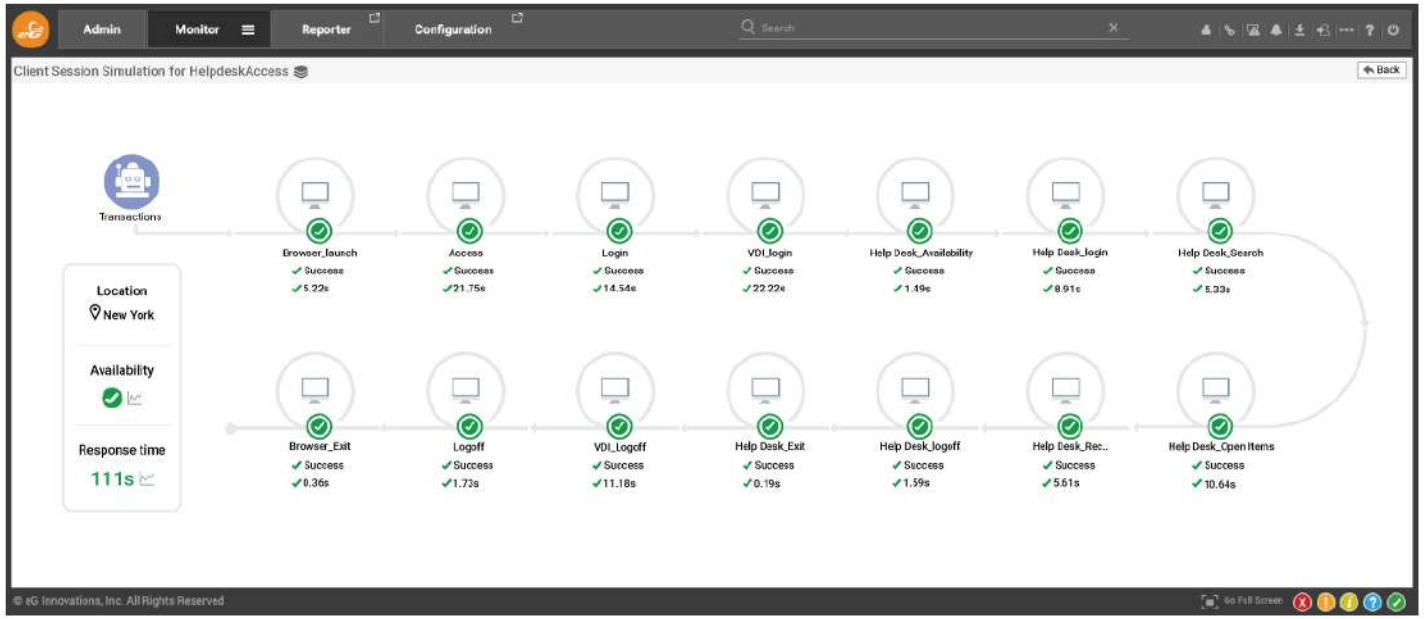
Ultimately if your AVD users can't access the apps they need to do their jobs—they will call you, not Microsoft!

 © 2026 eG Innovations. All rights reserved.

Myth #2. "Azure Service Health allows customers to track the status of Azure services. That's enough."

Microsoft's Azure Service Health dashboard shows overall platform status, but updates are generic, delayed, and not tailored to your AVD subscription. It won't flag configuration errors, authentication failures, FSLogix/storage problems, or app issues in your environment—even if the portal says AVD is "operational."

To manage AVD effectively, you need proactive monitoring. **Synthetic monitoring** runs simulated logins and workflows 24×7, tracking login times, app responsiveness, and workflow success. This detects issues the Azure portal issues and can even test access from specific locations, revealing performance or network problems before they impact users.



Synthetic monitoring allows you to continually test complex user workflows and application performance within AVD

 © 2026 eG Innovations. All rights reserved.

Myth #3. "I have configured auto-scaling. This is sufficient for my AVD service to operate well."

Auto-scaling in AVD is powerful, but it's not a replacement for monitoring. It reacts to higher demand by adding session hosts, yet it doesn't diagnose why usage spiked. If CPU or memory surges stem from a misconfigured or broken application, auto-scaling only adds capacity—and cost—without fixing the root cause issue.

Continuous 24×7 monitoring identifies whether demand is legitimate or caused by inefficiencies, helping you scale intelligently, control costs, and resolve root problems rather than masking them.

Identify the root-cause of a problem: is it a large user profile, memory leak in an application, poor Wi-Fi connectivity for a user, a faulty application, etc., rather than just adding resources and cost.

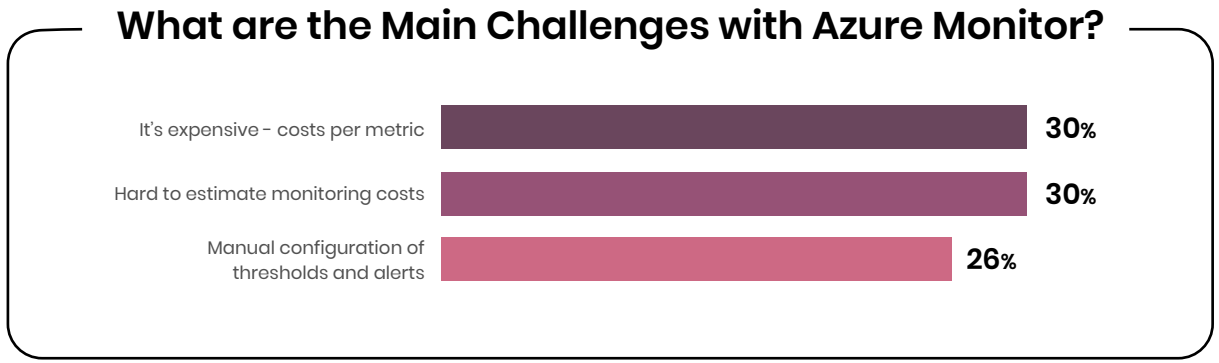
"Identifying the root-cause of resource demands rather than auto-scaling to accommodate demand cuts costs and raises operational quality"

 © 2026 eG Innovations. All rights reserved.

Myth #4. “Azure Monitor gives me all I need for monitoring the AVD service.”

Azure Monitor provides visibility and alerts for Azure and AVD, but setup is manual and time-consuming—configuring log analytics, dashboards, thresholds, and alerts takes effort. It’s also pay-per-metric/alert, so costs can spike in large environments, and budgeting is tricky. Despite being in the Azure stack, it’s not free—usage costs add up fast.

It is very common for organizations to use multiple digital workspace technologies — e.g., Citrix for legacy apps and AVD for offshore teams — Azure Monitor lacks cross-platform visibility. This forces teams to juggle multiple tools or add third-party solutions. A unified monitoring platform delivers consistent dashboards, reduces the learning curve, and gives a complete view of performance across all workspaces.



When we surveyed users their top three challenges with Azure Monitor were around costs and the manual effort required.

Source: *Azure Virtual Desktop (AVD) Adoption Trends*

 © 2026 eG Innovations. All rights reserved.

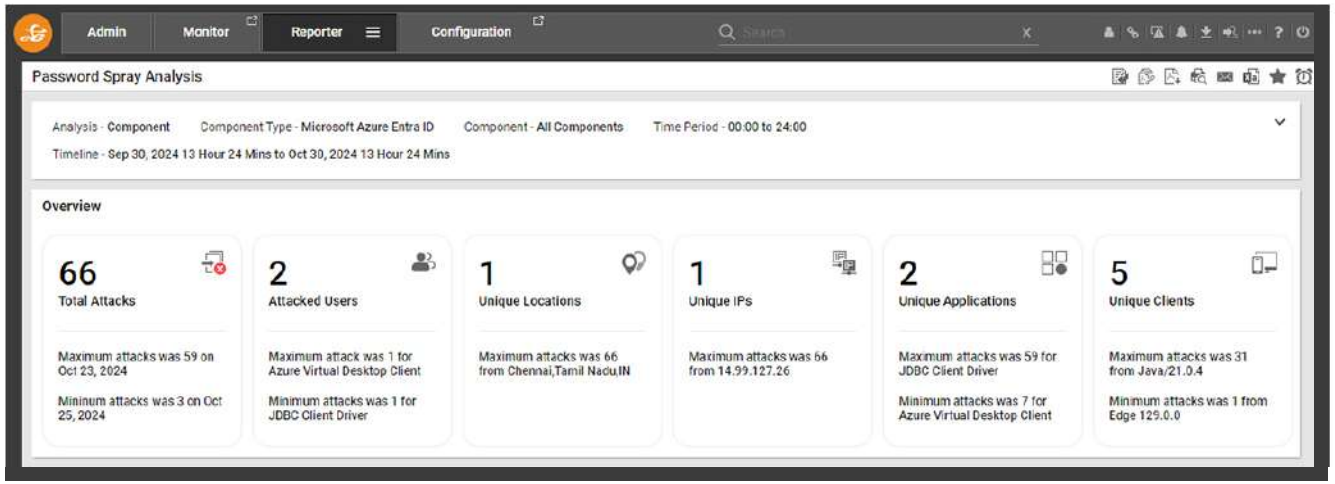
Myth #5. “Monitoring is needed only to troubleshoot when AVD problems occur.”

Monitoring ≠ Just Troubleshooting

Modern AVD monitoring delivers far more value:

- Compliance – Track logins, session durations, app access, and resource use for audit readiness.
- Security – Detect brute-force, password spraying, and suspicious logins via real-time Entra ID monitoring.
- Cost Control – Spot under/over-provisioned hosts, wasteful apps, and inappropriate activity to avoid unnecessary scaling and spend.
- Capacity Planning – Use real usage data to plan growth and right-size infrastructure.
- Management Insight – Share clear performance and adoption reports to guide investment decisions.

Monitoring is a strategic enabler—not just a break-fix tool.



Monitoring Entra ID sign-in logs can identify malicious attacks on your AVD deployments such as brute force and password spraying attacks.

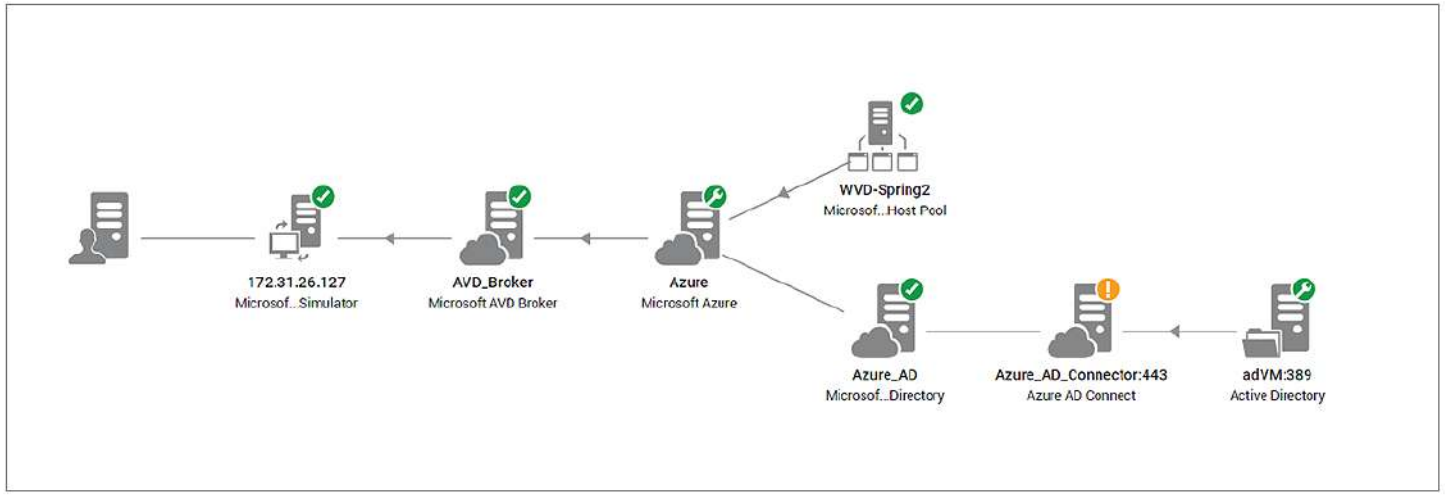
 © 2026 eG Innovations. All rights reserved.

Myth #6. “Monitoring of AVD is about monitoring your session hosts.”

Session hosts matter—they run user sessions and apps—but they’re only part of the story. Key components such as Entra ID (Azure AD), networking, FSLogix profiles, Azure Storage, the Azure subscription, and the connection broker all affect user access and experience.

For instance, Entra ID issues can block logins, and connection broker problems cause logon delays—these won’t show up if you only watch session hosts.

True visibility means monitoring every layer of AVD, including provisioning, authentication and brokering services.



Rich topology maps within eG Enterprise visualize the components of authentication and brokering

 © 2026 eG Innovations. All rights reserved.

Myth #7. "Monitoring can be added later after the AVD service is operational."

Before and during AVD deployment, the focus is often on apps, desktop setup, session host sizing, profiles, and automation—while monitoring is sometimes an afterthought. Often, monitoring only gets attention after costs spike or users complain.

A proactive monitoring strategy from day one is key. Benchmark performance before and after migration to track improvements and keep all stakeholders aligned.

Early monitoring gives visibility into performance, usage, cost, and user experience—so when issues arise, you know what changed. Skipping this leads to cost overruns, slowdowns, and blame games between teams.

Integrating monitoring within your AVD planning will help ensure success and cross-team cooperation throughout your organization

 © 2026 eG Innovations. All rights reserved.

Start Monitoring AVD Today!

AVD observability delivers tangible, measurable benefits. From improved system reliability, better application performance and enhanced user experience to time and cost savings, the impact on IT operations is substantial and quantifiable.

Learn more about how eG Enterprise can help you unlock the full power of AVD without complexity,
contact us via info@eginnovations.com

Embrace the transformative power of AIOps monitoring technologies to enhance your AVD environment's performance, to stay ahead of the curve and to cut out unnecessary manual troubleshooting!

 © 2026 eG Innovations. All rights reserved.

Free Trial

Click Here

eG Innovations

For more information

Visit: www.eginnovations.com

Contact: info@eginnovations.com

© 2026 eG Innovations. All rights reserved. | www.eginnovations.com