


Secure monitoring and management tools

04/04/2019 • 2 minutes to read • Contributors 

In this article

[Monitoring](#)

[Security monitoring](#)

[Protect assets and data](#)

After a migration is complete, migrated assets should be managed by controlled IT operations. This article is not intended to suggest a deviation from operational best practices. Instead, the following should be considered a minimum viable product for securing and managing migrated assets, either from IT operations or independently as IT operations come online.

Monitoring

Monitoring is the act of collecting and analyzing data to determine the performance, health, and availability of your business workload and the resources that it depends on. Azure includes multiple services that individually perform a specific role or task in the monitoring space. Together, these services deliver a comprehensive solution for collecting, analyzing, and acting on telemetry from your workload applications and the Azure resources that support them. Gain visibility into the health and performance of your apps, infrastructure, and data in Azure with cloud monitoring tools, such as Azure Monitor, Log Analytics, and Application Insights. Use these cloud monitoring tools to take action and integrate with your service management solutions:

- **Core monitoring.** Core monitoring provides fundamental, required monitoring across Azure resources. These services require minimal configuration and collect core telemetry that the premium monitoring services use.
- **Deep application and infrastructure monitoring.** Azure services provide rich capabilities for collecting and analyzing monitoring data at a deeper level. These services build on core monitoring and take advantage of common functionality in Azure. They provide powerful analytics with collected data to give you unique insights into your applications and infrastructure.

Learn more about [Azure Monitor](#) for monitoring migrated assets.

Security monitoring

Rely on the Azure Security Center for unified security monitoring and advanced threat notification across your hybrid cloud workloads. The Security Center gives full visibility into and control over the security of cloud applications in Azure. Quickly detect and take action to respond to threats and reduce exposure by enabling adaptive threat protection. The built-in dashboard provides instant insights into security alerts and vulnerabilities that require attention. Azure Security Center can help with many functions, including:

- **Centralized policy monitoring.** Ensure compliance with company or regulatory security requirements by centrally managing security policies across hybrid cloud workloads.
- **Continuous security assessment.** Monitor the security of machines, networks, storage and data services, and applications to discover potential security issues.
- **Actionable recommendations.** Remediate security vulnerabilities before they can be exploited by attackers. Include prioritized and actionable security recommendations.
- **Advanced cloud defenses.** Reduce threats with just-in-time access to management ports and safe lists to control applications running on your VMs.

- **Prioritized alerts and incidents.** Focus on the most critical threats first, with prioritized security alerts and incidents.
- **Integrated security solutions.** Collect, search, and analyze security data from a variety of sources, including connected partner solutions.

Learn more about [Azure Security Center](#) for securing migrated assets.

Protect assets and data

Azure Backup provides a means of protecting VMs, files, and data. Azure Backup can help with many functions, including:

- Backing up VMs.
- Backing up files.
- Backing up SQL Server databases.
- Recovering protected assets.

Learn more about [Azure Backup](#) for protecting migrated assets.