SYNCHROWORKS
CONSULTING

SECTION 8

Optimize

Once you've implemented your cloud migration strategy, you'll want to ensure that you're successfully taking advantage of the cloud's performance, scalability, and cost saving benefits.

This will enable you to only pay for the services and resources you use, achieve a greater ROI, and receive additional savings by taking advantage of the latest cloud capabilities. This is also the best time to start looking at new services for modernizing your application, migrating to PaaS and even SaaS, where applicable.

On-premises tools are not built for cloud scale and agility. Plus, they're simply not aligned with the new usage models enabled by the cloud. Continual optimization is a critical third step in your migration journey. Optimization targets two main areas—ensuring peak performance and continual cost efficiency.

Once you migrate, you will need to focus on three priorities:

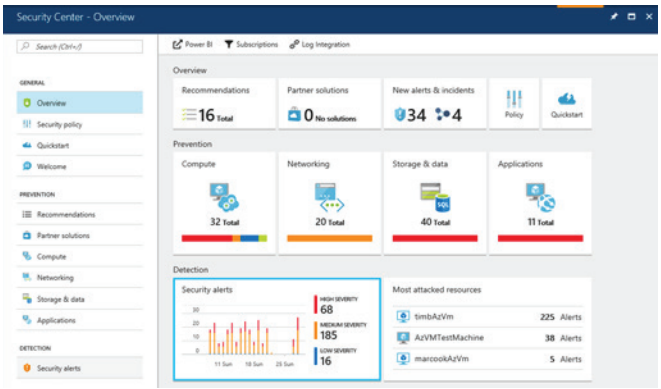
1. Ensure that your virtual machine is continuously secured
2. Protect your data
3. Monitor your cloud health

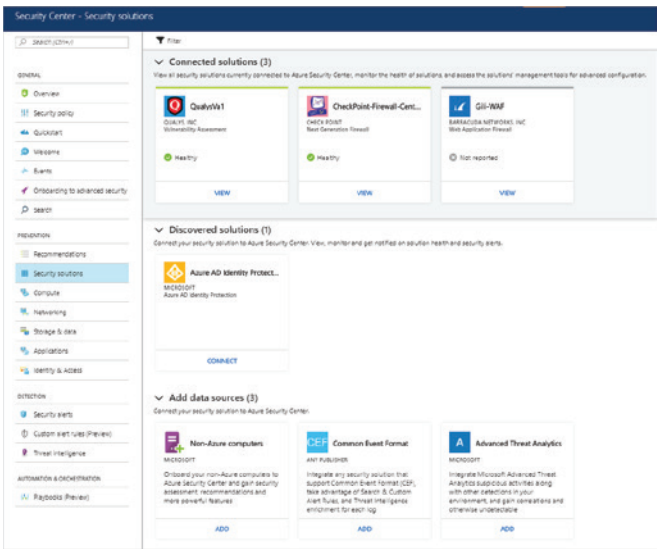
Below are a few areas that you should focus on once you've established a cloud environment within your organization. In order to better emphasize these focus areas, we've used Azure tools and features as examples.

Secure Cloud Resources

Ensuring strong security for your cloud-based resources is a shared responsibility between you and your cloud provider. All cloud service providers are built with a foundation of trust, security, compliance, privacy, and transparency. Their platforms provide a secure foundation to host your infrastructure with built-in security controls and capabilities to help you further protect your data and applications.

For example, Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. The Security Center enables you to take advantage of several capabilities, including:





Centralized Policy Management

Ensure compliance with company or regulatory security requirements by centrally managing security policies across all your hybrid cloud workloads.

Continuous Security Assessment

Monitor the security of machines, networks, applications, and storage and data services, and applications to discover potential security issues.

Actionable Recommendations

Remediate security vulnerabilities before they can be exploited by attackers with prioritized and actionable security recommendations.

Advanced Cloud Defenses

Reduce threats with just-in-time access to management ports and whitelisting 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.

Protecting Data

Azure ensures workloads and data are fully backed up and protected from disasters, while providing encryption of stored data for internal and customer security. Azure can also automatically encrypt your stored data—while allowing full accessibility to all applications and users.

Virtual Machine Disk Encryption
Azure Disk Encryption enables encryption of Windows and Linux Azure Virtual Machine disks. Azure Disk Encryption uses the industry standard BitLocker feature of Windows and the dm-crypt feature of Linux to provide volume encryption for the OS and the data disks. The solution is integrated with Azure Key Vault to help you control and manage the disk encryption keys and secrets in your key vault subscription, while ensuring that all data in the virtual machine disks are encrypted at rest in your Azure storage.

Virtual Machine Backup
Azure Backup is a scalable solution that protects your application data with zero capital investment and minimal operating costs. Application errors can corrupt your data and human errors can introduce bugs into your applications. With Azure Backup, your virtual machines running Windows and Linux are protected.

Azure Site Recovery
An important part of your organization's business continuity and disaster recovery (BCDR) strategy is figuring out how to keep corporate workloads and apps up and running when planned and unplanned outages occur. Azure Site Recovery helps orchestrate replication, failover, and recovery of workloads and apps so that they are available from a secondary location if your primary location goes down.

Monitoring Cloud Health

As with any system, monitoring is important to drive both proactive and reactive analysis. Azure provides many monitoring services targeted at applications, workloads, and core service health to ensure you have full visibility into your current system status—plus, access to important data when working with a break-fix situation. In Azure, you can use either basic or premium monitoring services.

Basic monitoring provides fundamental, required monitoring across Azure resources. These services need minimal configuration and collect core telemetry that the premium monitoring services use.

AZURE MONITOR

Azure Monitor enables basic monitoring for Azure services by allowing the collection of metrics, activity logs, and diagnostic logs. For example, the activity log tells you when new resources are created or modified. Metrics are available that provide performance statistics for different resources, and even the operating system, inside a virtual machine. You can view this data with one of the explorers in the Azure portal, send it to Azure Log Analytics for trending and detailed analysis, or create alert rules to proactively get notifications of critical issues.

SERVICE HEALTH

It's important to be aware of any issues with Azure services concerning any dependent applications. Azure Service Health identifies issues with Azure services that might affect your application. Service Health also helps you plan for scheduled maintenance.

AZURE ADVISOR

Azure Advisor constantly monitors your resource configuration and usage telemetry. It then gives you personalized recommendations based on best practices. Following these recommendations helps you improve the performance, security, and availability of the resources that support your applications.

Premium monitoring services build on basic monitoring and provide powerful analytics with collected data to give you unique insights into your applications and infrastructure. Plus, they present you with data in the context of scenarios that are targeted to different audiences.

APPLICATION INSIGHTS

Application Insights enables you to monitor the availability, performance, and usage of your application, whether it's hosted in the cloud or on-premises. By instrumenting your migrated or rearchitected application to work with Application Insights, you can quickly identify and diagnose errors without waiting for a user to report them. With the information that you collect, you can make informed choices on your application's maintenance and improvements. Application Insights stores its data in a common repository where it can take advantage of shared functionality such as alerts, dashboards, and deep analysis with the Log Analytics query language.

SERVICE MAP

Service Map provides insight into your IaaS environment by analyzing virtual machines with their different processes and dependencies on other computers and external processes. It integrates events, performance data, and management solutions in Log Analytics. You can then view this data in the context of each computer and its relation to the rest of your environment.

NETWORK WATCHER

Network Watcher provides scenario-based monitoring and diagnostics for different network scenarios in Azure. It stores data in Azure metrics and diagnostics for further analysis.

Many premium management solutions are packaged sets of logic that provide insights for an application or service. They rely on log analytics to store and analyze the monitoring data that they collect. **Azure Log Analytics** enables deeper visibility into your hybrid IT environment and allows you to diagnose performance issues from an advanced analytics portal in one click.

Azure Log Analytics enables you to:

ANALYZE DATA

In Log Analytics, you can leverage log searches by constructing queries to analyze the collected data, using pre-existing dashboards that you can customize with graphical views of your most valuable searches. Once you have a defined collection of operational data from your Azure virtual machines and activity logs, you can perform powerful searches.

VISUALIZE DATA

Log Analytics dashboards can visualize all your saved log searches, giving you the ability to find, correlate, and share IT operational data in your organization.

ALERT DATA

Alerts in Log Analytics identify important information in your repository. They are created by alert rules that automatically run log searches at regular intervals and match certain criteria. With Alert Action, you can perform advanced actions with alerts, such as create an email notification, launch an automation runbook, or create an incident record in your ITSM incident management system.

SYNCHROWORKS
CONSULTING

2-3000 Langstaff Rd
Concord, Ontario
L4K 4R7

1.866.960.9409
info@synchroworks.net
www.synchroworks.net

V.210222