Cloud-native Security Baseline policy

02/11/2019 • 6 minutes to read • Contributors

In this article

Security Baseline is one of the Five Disciplines of Cloud Governance. This discipline focuses on general security topics including protection of the network, digital assets, data, etc. As outlined in the policy review guide, the Cloud Adoption Framework includes three levels of **sample policy**: Cloud-Native, Enterprise, and Cloud Design Principle Compliant for each of the disciplines. This article discusses the Cloud-Native sample policy for the Security Baseline Discipline.

> **Note**
>
> Microsoft is in no position to dictate corporate or IT policy. This article is intended to help you prepare for an internal policy review. It is assumed that this sample policy will be extended, validated, and tested against your corporate policy before attempting to use it. Any use of this sample policy, as is, is discouraged.

Policy alignment

This sample policy synthesizes a cloud-native scenario, meaning that the tools and platforms provided by Azure are sufficient to manage business risks involved in a deployment. In this scenario, it is assumed that a simple configuration of the default Azure services provides sufficient asset protection.

Cloud security and compliance

Security is integrated into every aspect of Azure, offering unique security advantages derived from global security intelligence, sophisticated customer-facing controls, and a secure, hardened infrastructure. This powerful combination helps protect your applications and data, support your compliance efforts, and provide cost-effective security for organizations of all sizes. This approach creates a strong starting position for any security policy, but does not negate the need for equally strong security practices related to the security services being used.

Built-in security controls

It's hard to maintain a strong security infrastructure when security controls are not intuitive and need to be configured separately. Azure includes built-in security controls across a variety of services that help you protect data and workloads quickly and manage risk across hybrid environments. Integrated partner solutions also let you easily transition existing protections to the cloud.

Cloud-native identity policies

Identity is becoming the new boundary control plane for security, taking over that role from the traditional network-centric perspective. Network perimeters have become increasingly porous and that perimeter defense cannot be as effective as it was before the evolution of bring your own device (BYOD) and cloud applications. Azure identity management and access control enable seamless, secure access to all your applications.

A sample cloud-native policy for identity across cloud and on-premises directories, could include requirements like the following:

- Authorized access to resources with role-based access control (RBAC), multi-factor authentication, and single sign-on (SSO).
- Quick mitigation of user identities suspected of compromise.
- Just-in-time (JIT), just-enough access granted on a task-by-task basis to limit exposure of overprivileged admin credentials.
- Extended user identity and access to policies across multiple environments through Azure Active Directory.

While it is important to understand Identity Baseline in the context of Security Baseline, the Five Disciplines of Cloud Governance calls out Identity Baseline as its own discipline, separate from Security Baseline.

Network access policies

Network control includes the configuration, management, and securing of network elements such as virtual networking, load balancing, DNS, and gateways. The controls provide a means for services to communicate and interoperate. Azure includes a robust and secure networking infrastructure to support your application and service connectivity requirements. Network connectivity is possible between resources located in Azure, between on-premises and Azure hosted resources, and to and from the internet and Azure.

A cloud-native policy for network controls may include requirements like the following:

- Hybrid connections to on-premises resources (While technically possible in Azure), might not be allowed in a cloud-native policy. Should a hybrid connection prove necessary, a more robust Enterprise Security Policy sample would be a more relevant reference.
- Users can establish secure connections to and within Azure using virtual networks and network security groups.
- Native Windows Azure Firewall protects hosts from malicious network traffic by limited port access. A good example of this policy would be the requirement to block (or not enable) traffic directly to a VM over RDP - TCP/UDP port 3389.
- Services like the Azure Application Gateway web application firewall (WAF) and Azure DDoS Protection safeguard applications and ensure availability for virtual machines running in Azure. These features should not be disabled or misused.

Data protection

One of the keys to data protection in the cloud is accounting for the possible states in which your data may occur, and what controls are available for each state. For the purpose of Azure data security and encryption best practices, recommendations focus on the following data states:

- Data encryption controls are built into services from virtual machines to storage and SQL Database.
- As data moves between clouds and customers, it can be protected using industry-standard encryption protocols.
- Azure Key Vault enables users to safeguard and control cryptographic keys and other secrets used by cloud apps and services.
- Azure Information Protection will help classify, label, and protect your sensitive data in apps.

While these features are built into Azure, each of the above requires configuration and could increase costs. Alignment of each cloud-native feature with a data classification strategy is highly suggested.

Security monitoring

Security monitoring is a proactive strategy that audits your resources to identify systems that do not meet organizational standards or best practices. Azure Security Center provides unified Security Baseline and advanced threat protection across hybrid cloud workloads. With Security Center, you can apply security policies across your workloads, limit your exposure to threats, and detect and respond to attacks, including:

- Unified view of security across all on-premises and cloud workloads with Azure Security Center.
- Continuous monitoring and security assessments to ensure compliance and remediate any vulnerabilities.
- Interactive tools and contextual threat intelligence for streamlined investigation.
- Extensive logging and integration with existing security information.

Extending cloud-native policies

Using the cloud can reduce some of the security burden. Microsoft provides physical security for Azure datacenters and helps protect the cloud platform against infrastructure threats such as a DDoS attack. Given that Microsoft has thousands of cybersecurity specialists working on security every day, the resources to detect, prevent, or mitigate cyberattacks are considerable. In fact, while organizations were once worried about whether the cloud was secure, most now understand that the level of investment in people and specialized infrastructure made by vendors like Microsoft makes the cloud more secure than most on-premises datacenters.

Even with this investment in a cloud-native Security Baseline, it is suggested that any Security Baseline policy extend the default cloud-native policies. The following are examples of extended policies that should be considered, even in a cloud-native environment:

- **Secure VMs.** Security should be every organization's top priority, and doing it effectively requires several things. You must assess your security state, protect against security threats, and then detect and respond rapidly to threats that occur.
- **Protect VM contents.** Setting up regular automated backups is essential to protect against user errors. This isn't enough, though; you must also make sure that your backups are safe from cyberattacks and are available when you need them.
- **Monitor VMs and applications.** This pattern encompasses several tasks, including getting insight into the health of your VMs, understanding interactions among them, and establishing ways to monitor the applications these VMs run. All of these tasks are essential in keeping your applications running around the clock.

Next steps

Now that you've reviewed the sample Security Baseline policy for cloud-native solutions, return to the policy review guide to start building on this sample to create your own policies for cloud adoption.

Build your own policies using the policy review guide