


Large enterprise: Security Baseline evolution

02/11/2019 • 13 minutes to read • Contributors 

In this article

[Evolution of the narrative](#)

[Evolution of tangible risks](#)

[Evolution of the policy statements](#)

[Evolution of the best practices](#)

[Conclusion](#)

[Next steps](#)

This article evolves the narrative by adding security controls that support moving protected data to the cloud.

Evolution of the narrative

The CIO has spent months collaborating with colleagues and the company's legal staff. A management consultant with expertise in cybersecurity was engaged to help the existing IT Security and IT Governance teams draft a new policy regarding protected data. The group was able to foster board support to replace the existing policy, allowing PII and financial data to be hosted by approved cloud providers. This required adopting a set of security requirements and a governance process to verify and document adherence to those policies.

For the past 12 months, the cloud adoption teams have cleared most of the 5,000 assets from the two datacenters to be retired. The 350 incompatible assets were moved to an alternate datacenter. Only the 1,250 virtual machines that contain protected data remain.

Evolution of the Cloud Governance team

The Cloud Governance team continues to evolve along with the narrative. The two founding members of the team are now among the most respected cloud architects in the company. The collection of configuration scripts has grown as new teams tackle innovative new deployments. The Cloud Governance team has also grown. Most recently, members of the IT Operations team have joined Cloud Governance team activities to prepare for cloud operations. The cloud architects who helped foster this community are seen both as cloud guardians and cloud accelerators.

While the difference is subtle, it is an important distinction when building a governance-focused IT culture. A cloud custodian cleans up the messes made by innovative cloud architects, and the two roles have natural friction and opposing objectives. A cloud guardian helps keep the cloud safe, so other cloud architects can move more quickly with fewer messes. A cloud accelerator performs both functions but is also involved in the creation of templates to accelerate deployment and adoption, becoming an innovation accelerator as well as a defender of the Five Disciplines of Cloud Governance.

Evolution of the current state

In the previous phase of this narrative, the company had begun the process of retiring two datacenters. This ongoing effort includes migrating some applications with legacy authentication requirements, which required an evolution of the Identity Baseline, described in the [previous article](#).

Since then, some things have changed that will affect governance:

- Thousands of IT and business assets have been deployed to the cloud.

- The application development team has implemented a continuous integration and continuous deployment (CI/CD) pipeline to deploy a cloud-native application with an improved user experience. That application doesn't interact with protected data yet, so it's not production ready.
- The Business Intelligence team within IT actively curates data in the cloud from logistics, inventory, and third-party data. This data is being used to drive new predictions, which could shape business processes. However, those predictions and insights are not actionable until customer and financial data can be integrated into the data platform.
- The IT team is progressing on the CIO and CFO's plans to retire two datacenters. Almost 3,500 of the assets in the two datacenters have been retired or migrated.
- The policies regarding PII and financial data have been modernized. However, the new corporate policies are contingent on the implementation of related security and governance policies. Teams are still stalled.

Evolution of the future state

- Early experiments from the application development and BI teams have shown potential improvements in customer experiences and data-driven decisions. Both teams would like to expand adoption of the cloud over the next 18 months by deploying those solutions to production.
- IT has developed a business justification to migrate five more datacenters to Azure, which will further decrease IT costs and provide greater business agility. While smaller in scale, the retirement of those datacenters is expected to double the total cost savings.
- Capital expense and operating expense budgets have approved to implement the required security and governance policies, tools, and processes. The expected cost savings from the datacenter retirement are more than enough to pay for this new initiative. IT and business leadership are confident this investment will accelerate the realization of returns in other areas. The grassroots Cloud Governance team became a recognized team with dedicated leadership and staffing.
- Collectively, the cloud adoption teams, Cloud Governance team, IT Security team, and IT Governance team will implement security and governance requirements to allow cloud adoption teams to migrate protected data into the cloud.

Evolution of tangible risks

Data breach: There is an inherent increase in liabilities related to data breaches when adopting any new data platform. Technicians adopting cloud technologies have increased responsibilities to implement solutions which can decrease this risk. A robust security and governance strategy must be implemented to ensure those technicians fulfill those responsibilities.

This business risk can be expanded into a few technical risks:

- Mission-critical apps or protected data might be deployed unintentionally.
- Protected data might be exposed during storage due to poor encryption decisions.
- Unauthorized users might access protected data.
- External intrusion could result in access to protected data.
- External intrusion or denial of service attacks could cause a business interruption.
- Organization or employment changes could allow for unauthorized access to protected data.
- New exploits might create opportunities for intrusion or unauthorized access.
- Inconsistent deployment processes might result in security gaps that could lead to data leaks or interruptions.
- Configuration drift or missed patches might result in unintended security gaps that could lead to data leaks or interruptions.
- Disparate edge devices might increase network operations costs.
- Disparate device configurations might lead to oversights in configuration and compromises in security.
- The Cybersecurity team insists there is a risk of vendor lock-in from generating encryption keys on a single cloud provider's platform. While this claim is unsubstantiated, it was accepted by the team for the time being.

Evolution of the policy statements

The following changes to policy will help remediate the new risks and guide implementation. The list looks long, but the adoption of these policies may be easier than it would appear.

1. All deployed assets must be categorized by criticality and data classification. Classifications are to be reviewed by the Cloud Governance team and the application before deployment to the cloud.
2. Applications that store or access protected data are to be managed differently than those that don't. At a minimum, they should be segmented to avoid unintended access of protected data.
3. All protected data must be encrypted when at rest.
4. Elevated permissions in any segment containing protected data should be an exception. Any such exceptions will be recorded with the Cloud Governance team and audited regularly.
5. Network subnets containing protected data must be isolated from any other subnets. Network traffic between protected data subnets will be audited regularly.
6. No subnet containing protected data can be directly accessed over the public internet or across datacenters. Access to those subnets must be routed through intermediate subnets. All access into those subnets must come through a firewall solution that can perform packet scanning and blocking functions.
7. Governance tooling must audit and enforce network configuration requirements defined by the Security Management team.
8. Governance tooling must limit VM deployment to approved images only.
9. Whenever possible, node configuration management should apply policy requirements to the configuration of any guest operating system. Node configuration management should respect the existing investment in Group Policy Object (GPO) for resource configuration.
10. Governance tooling will audit that automatic updates are enabled on all deployed assets. When possible, automatic updates will be enforced. When not enforced by tooling, node-level violations must be reviewed with operational management teams and remediated in accordance with operations policies. Assets that are not automatically updated must be included in processes owned by IT Operations.
11. Creation of new subscriptions or management groups for any mission-critical applications or protected data requires a review from the Cloud Governance team to ensure proper blueprint assignment.
12. A least-privilege access model will be applied to any subscription that contains mission-critical applications or protected data.
13. The cloud vendor must be capable of integrating encryption keys managed by the existing on-premises solution.
14. The cloud vendor must be capable of supporting the existing edge device solution and any required configurations to protect any publicly exposed network boundary.
15. The cloud vendor must be capable of supporting a shared connection to the global WAN, with data transmission routed through the existing edge device solution.
16. Trends and exploits that could affect cloud deployments should be reviewed regularly by the security team to provide updates to Security Baseline tooling used in the cloud.
17. Deployment tooling must be approved by the Cloud Governance team to ensure ongoing governance of deployed assets.
18. Deployment scripts must be maintained in a central repository accessible by the Cloud Governance team for periodic review and auditing.
19. Governance processes must include audits at the point of deployment and at regular cycles to ensure consistency across all assets.
20. Deployment of any applications that require customer authentication must use an approved identity provider that is compatible with the primary identity provider for internal users.
21. Cloud Governance processes must include quarterly reviews with Identity Baseline teams to identify malicious actors or usage patterns that should be prevented by cloud asset configuration.

Evolution of the best practices

This section of the article will evolve the governance MVP design to include new Azure policies and an implementation of Azure Cost Management. Together, these two design changes will fulfill the new corporate policy statements.

The new best practices fall into two categories: Corporate IT (hub) and Cloud Adoption (spoke).

Establishing a corporate IT hub and spoke subscription to centralize the Security Baseline: In this best practice, the existing governance capacity is wrapped by a [hub and spoke topology with shared services](#), with a few key additions from the Cloud Governance team.

1. Azure DevOps repository. Create a repository in Azure DevOps to store and version all relevant Azure Resource Manager templates and scripted configurations.
2. Hub and spoke template.
 - a. The guidance in the [hub and spoke topology with shared services](#) reference architecture can be used to generate Resource Manager templates for the assets required in a corporate IT hub.
 - b. Using those templates, this structure can be made repeatable, as part of a central governance strategy.
 - c. In addition to the current reference architecture, it is advised that a network security group template should be created capturing any port blocking or whitelisting requirements for the VNet to host the firewall. This network security group differs from prior groups, because it will be the first network security group to allow public traffic into a VNet.
3. Create Azure policies. Create a policy named Hub NSG Enforcement to enforce the configuration of the network security group assigned to any VNet created in this subscription. Apply the built-in Policies for guest configuration as follows:
 - a. Audit that Windows web servers are using secure communication protocols.
 - b. Audit that password security settings are set correctly inside Linux and Windows machines.
4. Corporate IT blueprint
 - a. Create an Azure blueprint named corporate-it-subscription.
 - b. Add the hub and spoke templates and Hub NSG Enforcement policy.
5. Expanding on initial management group hierarchy.
 - a. For each management group that has requested support for protected data, the corporate-it-subscription-blueprint blueprint provides an accelerated hub solution.
 - b. Because management groups in this fictional example include a regional hierarchy in addition to a business unit hierarchy, this blueprint will be deployed in each region.
 - c. For each region in the management group hierarchy, create a subscription named Corporate IT Subscription.
 - d. Apply the corporate-it-subscription-blueprint blueprint to each regional instance.
 - e. This will establish a hub for each business unit in each region. Note: Further cost savings could be achieved, but sharing hubs across business units in each region.
6. Integrate group policy objects (GPO) through Desired State Configuration (DSC):
 - a. Convert GPO to DSC – The [Microsoft Baseline Management project](#) in Github can accelerate this effort. * Be sure to store DSC in the repository in parallel with Resource Manager templates.
 - b. Deploy Azure Automation State Configuration to any instances of the Corporate IT subscription. Azure Automation can be used to apply DSC to VMs deployed in supported subscriptions within the management group.
 - c. The current roadmap plans to enable custom guest configuration policies. When that feature is released, the use of Azure Automation in this best practice will no longer be required.

Applying additional governance to a Cloud Adoption Subscription (Spoke): Building on the Corporate IT Subscription, minor changes to the governance MVP applied to each subscription dedicated to the support of application archetypes can produce rapid evolution.

In prior evolutions of the best practice, we defined network security groups to block public traffic and whitelisted internal traffic. Additionally, the Azure blueprint temporarily created DMZ and Active Directory capabilities. In this evolution, we will tweak those assets a bit, creating a new version of the Azure blueprint.

1. Network peering template. This template will peer the VNet in each subscription with the Hub VNet in the Corporate IT subscription.
 - a. The reference architecture from the prior section, [hub and spoke topology with shared services](#), generated a Resource Manager template for enabling VNet peering.
 - b. That template can be used as a guide to modify the DMZ template from the prior governance evolution.
 - c. Essentially, we are now adding VNet peering to the DMZ VNet that was previously connected to the local edge device over VPN.
 - d. *** It is also advised that the VPN should be removed from this template as well to ensure no traffic is routed directly to the on-premises datacenter, without passing through the corporate IT subscription and Firewall solution.
 - e. Additional [network configuration](#) will be required by Azure Automation to apply DSC to hosted VMs.
2. Modify the network security group. Block all public **and** direct on-premises traffic in the network security group. The only inbound traffic should be coming through the VNet peer in the corporate IT subscription.
 - a. In the prior evolution, a network security group was created blocking all public traffic and whitelisting all internal traffic. Now we want to shift this network security group a bit.
 - b. The new network security group configuration should block all public traffic, along with all traffic from the local datacenter.
 - c. Traffic entering this VNet should only come from the VNet on the other side of the VNet peer.
3. Azure Security Center implementation:
 - a. Configure Azure Security Center for any management group that contains protected data classifications.
 - b. Set Automatic provisioning to on by default to ensure patching compliance.
 - c. Establish OS security configurations. IT Security to define the configuration.
 - d. Support IT Security in the initial use of Azure Security Center. Transition use of security center to IT security, but maintain access for governance continuous improvement purposes.
 - e. Create a Resource Manager template reflecting the changes required for Azure Security Center configuration within a subscription.
4. Update Azure Policy for all subscriptions.
 - a. Audit and enforce criticality and data classification across all management groups and subscriptions to identify any subscriptions with protected data classifications.
 - b. Audit and enforce use of approved OS images only.
 - c. Audit and enforce guest configurations based on security requirements for each node.
5. Update Azure Policy for all subscriptions that contains protected data classifications.
 - a. Audit and enforce use of standard roles only
 - b. Audit and enforce application of encryption for all storage accounts and files at rest on individual nodes.
 - c. Audit and enforce the application of the new version of the DMZ network security group.
 - d. Audit and enforce use of approved network subnet and VNet per network interface.
 - e. Audit and enforce the limitation of user-defined routing tables.
6. Azure blueprint:
 - a. Create an Azure blueprint named protected-data.
 - b. Add the VNet peer, network security group, and Azure Security Center templates to the blueprint.
 - c. Ensure the template for Active Directory from the previous evolution is NOT included in the blueprint. Any dependencies on Active Directory will be provided by the corporate IT subscription.
 - d. Terminate any existing Active Directory VMs deployed in the previous evolution.
 - e. Add the new policies for protected data subscriptions.
 - f. Publish the blueprint to any management group intended to host protected data.
 - g. Apply the new blueprint to each affected subscription along with existing blueprints.

Conclusion

Adding these processes and changes to the governance MVP helps remediate many of the risks associated with security governance. Together, they add the network, identity, and security monitoring tools needed to protect data.

Next steps

As cloud adoption continues to evolve and deliver additional business value, risks and cloud governance needs also evolve. For the fictional company in this journey, the next step is to support mission-critical workloads. This is the point when Resource Consistency controls are needed.

Resource Consistency evolution