Reblaze

Securely Using Microsoft Azure

Reblaze Technologies LTD

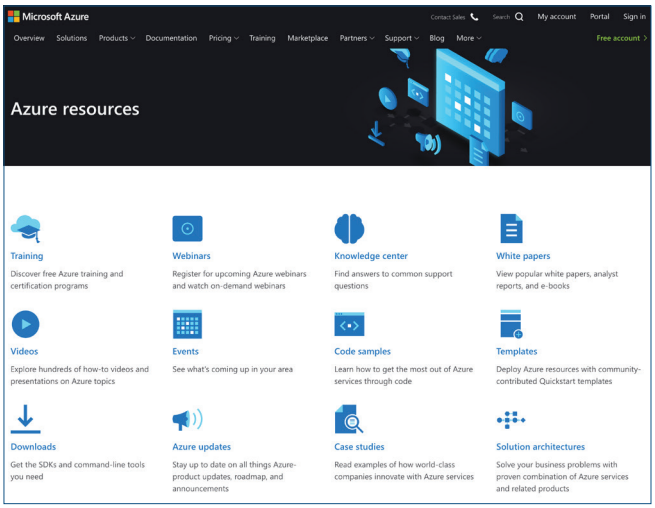
Introduction

In today's fast-paced and quickly evolving cloud environment, adopting a strong security strategy is critical to ensuring your infrastructure remains protected and reliable. As more organizations adopt strategies such as DevOps, this rapid development and change can become difficult to manage without a comprehensive understanding of the security tools and configurations available.

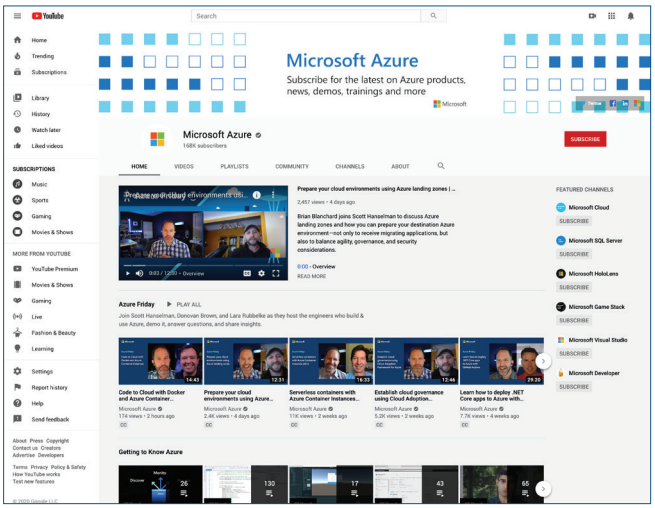
Microsoft Azure offers many security services and capabilities that can underpin your infrastructure, and learning to manage and integrate them is crucial to succeeding in this environment.

This white paper will discuss the security tools currently available in the increasingly popular Azure platform. If your organization has not (yet) migrated to Azure and is considering doing so, you might be interested in these articles: Securely Migrating to the Cloud and Securely Migrating to Microsoft Azure.

Cloud security is of course a large subject. After reading this white paper, you will probably want a deeper dive into one or more specific topics. A variety of good materials are available on the Azure resources page, and another good source is the Azure YouTube channel.



https://azure.microsoft.com/en-us/resources/



https://www.youtube.com/user/windowsazure

Shared Responsibility

In the past, organizations owned their server infrastructure. Among other implications, this meant that organizations were solely responsible for their web security.

One of the significant advantages of using a cloud provider such as Azure is the model of "shared responsibility." Azure provides a secure cloud infrastructure, and devotes considerable financial and engineering resources to this task. However, this does not relieve its customers of all responsibility; they must secure the resources they use within it. Shared responsibility is often expressed like this: Azure provides security "of" the cloud, while customers are responsible for security "in" the cloud.

As noted on Microsoft's page about Azure's division of responsibilities:

> "In an on-premises datacenter, you own the whole stack. As you move to the cloud some responsibilities transfer to Microsoft… according to the type of deployment of your stack."

It further explains that:

- Some security-related tasks are always performed by Azure (e.g., providing secure hosts).
- Some tasks are always performed by customers (e.g., ensuring that data is stored securely).
- Some tasks vary depending on the service type (e.g., for IaaS the customer is responsible for the security of the operating system, while for SaaS Azure retains responsibility).

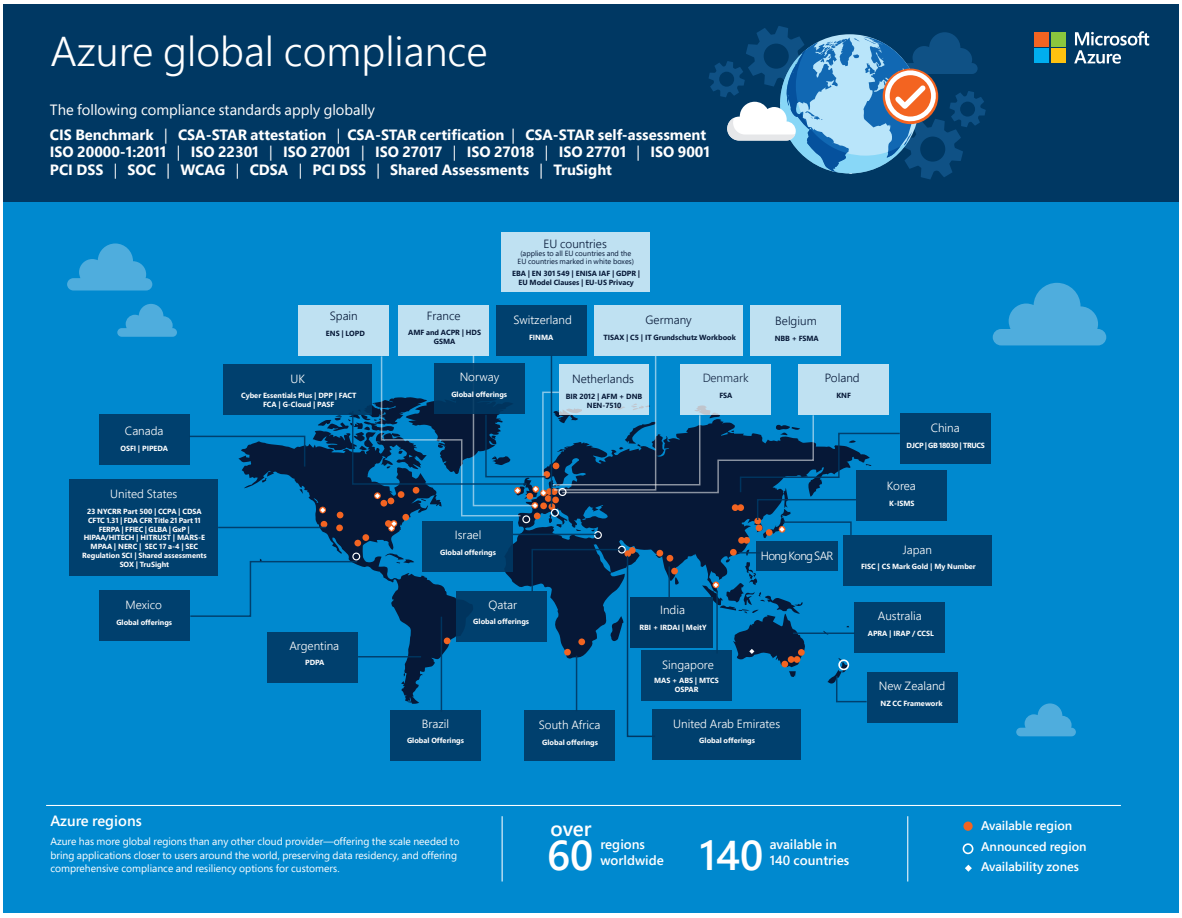
For more in-depth coverage of this topic, see Microsoft's white paper on Shared Responsibilities for Cloud Computing.

Compliance

Azure is compliant with a wide variety of security and privacy standards. Microsoft provides an overview of its compliance here. To look up a specific standard, you can also see the Compliance Offerings page, which includes a long list of standards to which Microsoft's offerings (not just Azure) comply. Selecting one of them will display a page describing the specific products and services that are compliant with it.

Note that compliance is also a shared responsibility. Even though a cloud provider is compliant, you do not automatically inherit that compliance. It only means that the underlying infrastructure is compliant, and it provides a baseline for Azure users to build upon as they seek to achieve compliance for their own products and services.

The infographic below shows Azure's Global Compliance Map, updated on August 21, 2020. For the current version, visit https://azure.microsoft.com/en-us/resources/azure-global-compliance-map/.



Azure's Cloud Security Offerings

As with any major cloud provider, Azure offers many tools to facilitate best practices and secure your infrastructure. Of course, technology alone cannot mitigate every threat, so you also need a robust set of operational policies and procedures.

Microsoft has generally organized Azure's cloud security offerings into six categories, listed below. Each category encompasses a number of tools and services intended to give you visibility and control over your cloud resources.

- **Operations**: includes the Security and Audit dashboard, Azure Resource Manager, Application Insights, Azure Monitor, Azure Monitor Logs, Azure Advisor, and Azure Security Center.
- **Applications**: includes penetration testing, Application Gateway WAF, authentication and authorization in Azure App Service, a layered service architecture, and web server and application diagnostics.
- **Compute**: includes anti-malware and anti-virus software, a hardware security module, Azure Backup for Azure VMs, Azure Site Recovery, Azure Disk encryption for VMs, and virtual networking.
- **Networking**: includes network security groups, route control and forced tunneling, Azure Virtual Network (VNet), Traffic Manager, Azure Application Gateway, and Azure DNS.
- **Storage**: includes role-based access control (RBAC), shared access signature (SAS), encryption in transit, encryption at rest, storage analytics, and CORS configurations for browser-based access.
- **Identity and access management**: primarily provided by Azure Active Directory, which includes features such as multi-factor, role-based, token-based, and hybrid authentication.

Each category will be discussed separately below.

Operations Security

Azure Security Center

A real-time overview of your entire environment is critical to maintaining a secure infrastructure. Azure Security Center plays a prominent role in securing an Azure network. Along with the Security and Audit dashboard, it provides a broad view of your organization and its security posture.

Additionally, Azure provides recommended controls and suggestions across all of your resources, which you can apply through the dashboard. The ability to quickly identify and remediate outstanding security issues will allow you to respond to problems promptly—and, ideally, prevent future issues from occurring.

Incorporating top-level policy and compliance management allows you to craft the appropriate policies to maintain information security. When you utilize Azure's Network map to discover and graph all of your Azure-connected systems, Azure can then assign a Secure score. This gives you the snapshot required to assess what areas need improvement or further attention.

Other useful services are Azure Advisor for personalized best practice recommendations about your overall environment, and Azure Network Watcher for performance monitoring and diagnostics of network traffic. These and other tools allow you to monitor and investigate any issues, which will help you quickly remediate and handle incoming threats.

Azure Regions and Availability Zones

Azure offers the ability to segment portions of your network for both security and reliability. If a region becomes unavailable, having infrastructure homed in multiple locations ensures a higher chance of uptime and customer availability.

Within each region, there is a minimum of three separate Availability Zones to ensure redundancy. These Availability Zones are physically separated from each other. Zone-redundant services will replicate your applications and data across the Availability Zones to protect against single points of failure. As a best practice, making sure that your resources and infrastructure are spread across Azure regions ensures that you will have the maximum up-time possible.,

Application Security

Most environments have several applications that provide customer services and internal utilities. Naturally, Azure offers tools to help maintain the security and reliability of those customer-facing services and internal applications.

Azure App Service

App Service is a fully managed platform for deploying and hosting web applications. App Service includes a number of security features; it's easy to create or upload SSL certificates, enforce HTTPS, authenticate users or client apps, and more.

When combined with network security groups within an Azure Virtual Network, App Service allows a layered approach to securing the application to only those users and services that require it. Use VNet service endpoints to extend your virtual network private address space over a direct connection. VNets enable you to segment and secure the traffic to your web application, only allowing it access to the resources you define. Otherwise, the traffic will travel over a shared network and will not be as secure.

Application secrets, such as database credentials, tokens, or private keys, should only be exposed via environment variables. Stored in the Azure App Service app settings, these secrets are encrypted. They are only decrypted at application start time and then injected into process memory. The keys are then rotated regularly. You can also use Azure Key Vault to store additional secrets that can be integrated within your application.

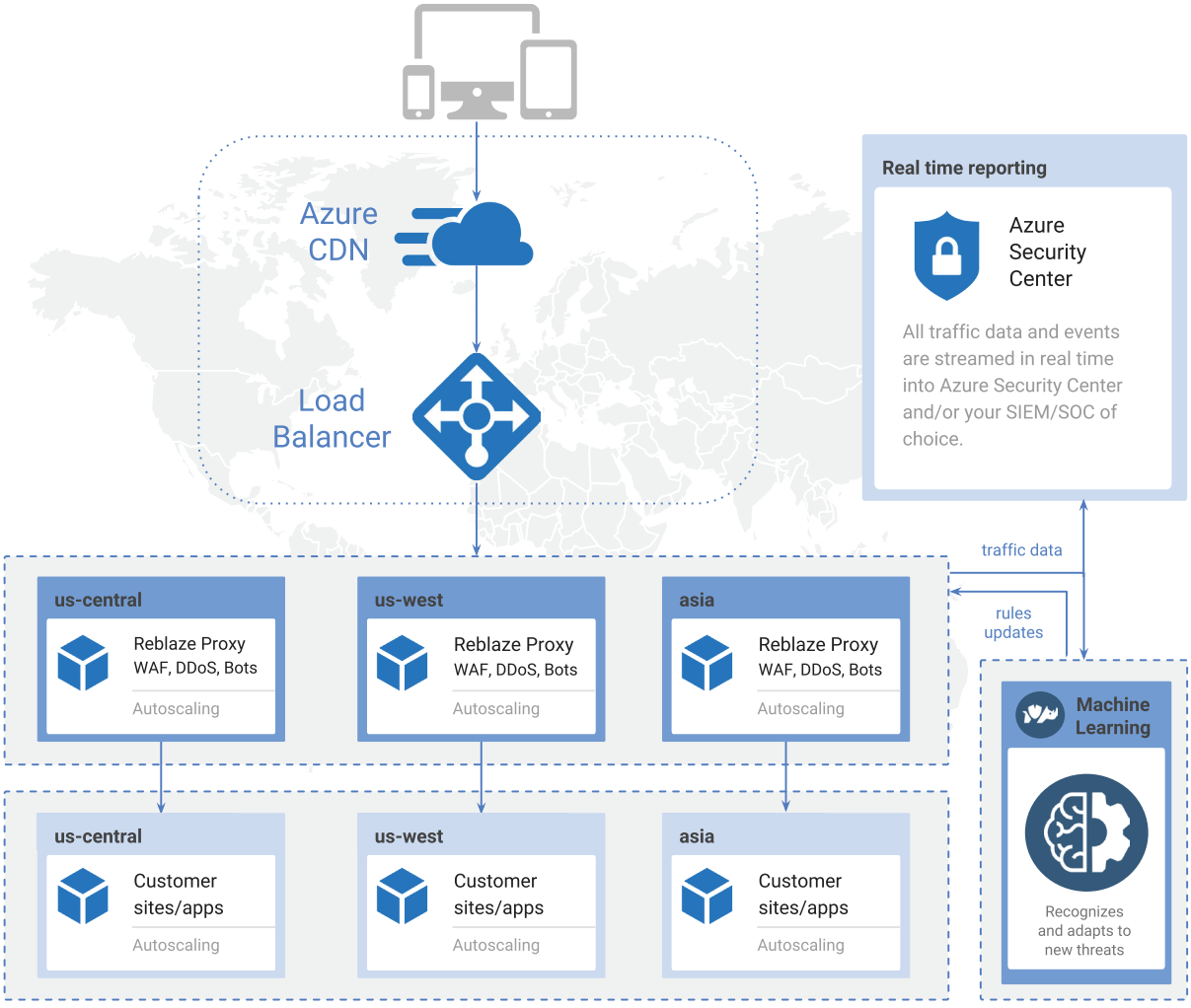
Application Gateway's WAF

Azure Application Gateway includes the Azure WAF (Web Application Firewall). For Internet-facing applications, the WAF can mitigate some common web-based threats. However, the WAF is not comprehensive. It includes and enforces the Core Rule Set from the Open Web Application Security Project (OWASP), but there are many attack vectors which it does not address.

For complete security (including a next-gen WAF, DDoS protection, hostile bot mitigation, etc.), you

should also include a comprehensive third-party security solution. Reblaze extends and completes Azure's WAF, providing comprehensive protection for sites and web applications. It includes a next-generation WAF, multi-layer DoS and DDoS protection, industry-leading bot management, precise ACL, real time reporting, full traffic transparency, and more.

Reblaze is fully integrated with Microsoft Azure, and runs natively on autoscaling Azure VMs within a Virtual Private Cloud. It works seamlessly with Azure Security Center: Traffic data and events from Reblaze are streamed into Security Center, with the ability to quickly drill down and display granular details in real time—even headers and payloads of individual HTTP requests. The platform also integrates with a wide variety of SIEM/SOC solutions, to support your existing workflows.



Reblaze running on Microsoft Azure

Compute Resources

Azure Virtual Machines

While there are a number of Azure computer offerings, Azure virtual machines (VMs) are perhaps the most familiar type of compute resource. They provide on-demand and scalable virtualized computers with usage-based pricing, and are available for specific types of computing scenarios. Burstable VMs are the most economical choice, but VMs optimized for raw CPU, memory performance, and general purposes are also available. Both Windows and Linux VMs are also available for use in a wide variety of operating systems and versions.

Best practices for securing virtual machines generally fall into the following categories:

- **Role-based access control** involves scoping just the right amount of access to an individual or group, and is essential for controlling who and what has access to your resources. Azure Resource Manager allows you to script the appropriate permissions for each group to the resources as needed to ensure appropriate access.
- **Azure policies** (link) are defined configurations that are applied to your Windows or Linux VMs. They allow you to configure both internal machine configurations and restrictions to the Azure configuration itself.
- **Disk encryption** for Windows and Linux VMs is also available. Windows is encrypted using BitLocker, while Linux uses dm-crypt. Cryptographic keys are then stored in Azure Key Vault.
- **Microsoft Antimalware for Azure** (link) is a free solution provided for Azure's cloud services and VMs. It is built on the same platform as Microsoft Security Essentials and offers a comprehensive set of scanning and remediation services.
- **Azure Key Vault** (link) is available for storing certificates, keys, and other credentials. Additionally, policies may be used to further limit and restrict user access to specific resources.

Containers

Azure Kubernetes Service (AKS)

Azure has several containerization offerings, the most popular of which is Azure Kubernetes Service. Other options are Azure Service Fabric and Azure Container Instances (ACI). All of them offer the same core container functionality, but with varying degrees of integration, portability, and ease of management.

- **AKS** is Azure's managed Kubernetes service. Kubernetes is a container orchestration framework that assists in the end-to-end management of containerized services.
- **Azure Service Fabric** is similar to Kubernetes, but it's a Microsoft-created orchestration system. With tighter integration with Azure services, it offers additional benefits, but they come with an increased reliance on Microsoft and decreased portability to other container orchestration systems.
- **Azure Container Instances** is a basic container hosting service that allows for quick deployment of containers. If you don't need a full orchestration system, but you don't want to manage a container environment yourself, this is a great option.

When securing containers, it is extremely important to validate the source of your container images. To that end, Azure Container Registry allows you to create a private image registry of validated and tested images. However, you'll still need to continuously scan your images for new vulnerabilities and issues. Using Container Monitoring in Log Analytics, you can take a comprehensive look at the commands that are being run within your containers, as well as their effects.

Storage Resources

Storage is a vital part of a cloud infrastructure, and Azure offers a comprehensive set of solutions for your storage needs. However, you'll still need to secure your data.

Azure Blob Storage

One of the most commonly used storage services is Azure Blob storage. This is an Amazon S3 API equivalent that provides REST-based object storage. Instead of being block-based, like attached virtual disks, Blob storage is an API-accessible, data-storage medium. Policies can be set on "buckets" as a whole, or on individual files themselves.

A common mistake when working with Azure Blob storage is misconfiguring access policies, which leads to a publicly accessible bucket or a set of files that may contain privileged or protected information. Once you've made a bucket private, you have a few options for securing your resources.

For example, using a created storage account key, you can grant and share access to a resource. However, as Microsoft points out, this is essentially giving out the "keys to the kingdom," since access is wide ranging. An alternative is using a shared access signature (SAS). An SAS is a generated token appended to a Blob storage object URI that grants limited-time access to a specific resource. Using these methods will allow you to properly secure access to your Blob storage.

Although we have talked about Azure Blob storage, block storage is most commonly used within VMs—and it's what the operating systems themselves reside on. Azure enables you to encrypt disks at rest within Windows or Linux. Many security standards rely on this ability, and, in general, it's a best practice to follow if you can.

Network Resources

Azure Virtual Network (VNet)

The need to connect cloud services together and to the outside world underpins both storage and VMs. Azure uses the concept of an Azure Virtual Network, along with network security groups (NSGs) to protect and segment traffic as necessary.

When creating VNets, it's recommended to:

- Create fewer large VNets, rather than many small ones, to avoid management overhead. This also decreases the possibility of management mistakes.
- Use NSGs, which are essentially groups of firewall rules, to secure and segment traffic. You can even extend these rules into Application Security Groups, which bundle services together so you don't need to know every IP.
- Secure VNets using NSGs to define inbound and outbound traffic rules.

Azure Load Balancer

For Internet-facing services, using Load Balancer along with Azure DDoS Protection and Traffic Manager can help further protect and secure your applications from unexpected or malicious traffic spikes. With Azuze Bastion, you will be able to manage RDP and SSH access to your machines through the Azure portal without any external exposure.

Setting up proper networking within your environment is crucial to making sure that the resources you want to talk to each other are the only ones that do so. Furthermore, utilizing security groups to limit the available ports and the access they provide is an extremely effective way to protect your various resources (such as virtual machines).

For more information on network resources and security, see Azure network architecture and Microsoft's Azure network security overview.

Identity and Access Management

Azure Active Directory (AD)

Authentication and authorization are critically important to any cloud provider. They define "who" (authentication) can do "what" (authorization). Azure AD is a fundamental service; the original AD is easily one of the most commonly used directory service solutions, and Microsoft has extended it as a managed service to the Azure cloud. Most Azure services integrate tightly with Azure AD and allow you to control accounts and access from a centralized location.

For applications, you can use Azure AD for authentication. This usually consists of Azure AD for employees, Azure AD B2B for guest users and external partners, and Azure AD B2C for customer sign up and sign in. You can also enable Single Sign-On for devices, apps, and services within your environment. By enabling conditional access, you can ensure that only devices and locations that meet your stringent security protocols are allowed to connect and authenticate to your Azure AD instance. If possible, you should also enforce multi-factor authentication for your users.

Best Practices

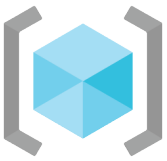
Follow Role-Based Access Control. RBAC is a large subject, but here's a summary: instead of users having assigned permissions, they are assigned to roles which have permissions. By creating the right roles and groups for each of your users, you can easily limit the impact of bad actors and provide just what your users need. Azure includes built-in roles that are excellent for getting started with this.

Always follow the principle of least privilege. Attach policies to the lowest level resource required. For employees, this may be a folder or project. For applications using service accounts that only need a handful of resources, attach policies directly to the resources if possible.

Take advantage of resource management. A well-thought-out resource hierarchy with folders and projects makes it easier to apply IAM policies at the correct level, making the whole organization more secure while also enabling better audits, thorough reporting, and so on.

Making It All Work

The topics discussed previously were primarily about the products and services that Microsoft offers for securing Azure itself. There are some additional services that are useful during operational use of the cloud, especially in the area of automation.



Azure Resource Manager (ARM)

To minimize risks and issues, it is highly recommended to use Azure Resource Manager configurations to automate your infrastructure. There are a number of ways to run configuration commands against Azure within the CLI, such as with PowerShell or within a Linux shell. By implementing automation in nearly every aspect of your organization's infrastructure, you'll benefit from transparency, repeatability, and ease of management.

ARM is a deployment and management layer built on top of Azure to allow for the deployment of templates that configure resources held within Azure. By using this, you can quickly spin up new resources that were built to be secure. ARM templates are well suited for CI/CD integration and they integrate with Azure Policy. Additionally, they allow you to export code, exert version control in products such as GIT, and create any Azure resources necessary.

Azure Automation consists of a set of shared resources that allow you to configure your environment. This service ties together a number of different tools to deploy, remove, and configure your resources. By defining templates, integrating with source control, and utilizing automation, you can create a solid foundation to build upon. This includes the ability to schedule automations that further assist with the constant monitoring and compliance needed in a changing environment.

Recommended Reading

DevOps and DevSecOps have become very popular, and they provide a number of advantages to organizations that adopt them. The following two articles give a number of tips and best practices when using them on Azure:

Using DevSecOps to Strengthen Security on Microsoft Azure

DevSecOps and Azure: A Deep Dive

Conclusion

This white paper has provided a high-level overview of the security issues involved when using Microsoft Azure.

As mentioned in the introduction, for more in-depth information on these topics it's worth the time to browse the Azure YouTube channel and this Azure resources page. Staying current is also important, since Microsoft is continually expanding the Azure product line.

Securely using Azure is a front-loaded process, with much of the work done in the beginning. Much of the necessary setup and configuration is fire-and-forget. However, there is one area for which this is not true: **web security**. Blocking attack traffic that is attempting to access your applications, services, and APIs is an ongoing process, evolving constantly as the threats themselves grow and change.

As mentioned earlier, Reblaze is a fully managed cloud platform, using Machine Learning to provide comprehensive, effective web security for Azure; it automates Azure's inherent security capabilities and adds many more. For more information, or to get a demo, contact us here.

Questions about the content of this white paper? Contact us at hello@reblaze.com.

To receive notifications of future publications, sign up for our newsletter by filling out the form at www.reblaze.com/contact-us/.

Reblaze Technologies, Ltd.
3031 Tisch Way
110 Plaza West
San Jose, CA 95128