

maxwellbond

CLOUD MONITORING, SECURITY, & CI/CD TOOLING

The best way to monitor, secure, and optimise your cloud network
in AWS and Azure



Jamie Shields
Lead Cloud Architect



Joe Hodkinson
Cloud Architect



Lloyd Lawson
Cloud & DevOps Consultant
lloyd.lowson@maxwellbond.co.uk
0161 359 3260

Introduction

Cloud technology has consistently grown in popularity over a number of years, with an increasing number of businesses migrating to the cloud year on year. However, the COVID-19 pandemic prompted an even bigger push to the cloud because of the rapidly expanded work-from-home and remote requirements and the need for touchless procurement, sales and service. After this unprecedented global event, the pressure is really on businesses to adapt and migrate to cloud-based technology and those that don't embrace the cloud over the next 12-18 months are likely to be left behind in the race of agility and innovation.

Now that the initial major rush to integrate cloud technology has passed for most businesses, it's time to dive deeper and start to assess and address questions around cloud monitoring, cloud security, CI/CD and DevOps enablement, and cloud tooling. The following whitepaper, which is based on a recent webinar "Clash of Clouds" with Jamie Shields and Joe Hodgkinson, explores these topics in more detail. Alternatively, the full webinar recording is now available on our YouTube channel, or via our website.

Cloud Monitoring

As with any business tool or platform, being able to monitor and assess performance is fundamental. There are a number of tools available to AWS and Microsoft Azure, which are covered in more detail below.

AWS Cloud Monitoring

AWS users can utilise tools such as CloudWatch and use Elasticsearch for logging and monitoring capabilities. For example, users can leverage Logstash as a method for streaming logs from multiple platforms into Elasticsearch and then wrapping dashboard tools like Kibana and Grafana round those to create that dashboard element for user feedback.

Recently AWS have launched the Grafana service and the new Time Series database services which help to build out those monitoring and alerting platform. Equally, from a monitoring across the organisation, you can use tools like Cloud Trail Security Hub.

Azure Cloud Monitoring

Azure Monitor is the central place to look at logs and metrics in Azure. Underpinned by Log Analytics which is the central database where users can stream all data to. Within Azure, users can monitor metrics (CPU, memory), logs, and what is actually happening in the environment. Businesses can use Application Insights to monitor the performance of web applications. Application Insights provides live performance analytics monitoring which quickly detects errors so that users can fix them. This can all then be streamed into visual dashboards.

When it comes to alerting, Azure can be linked into emails and ITSMs so businesses can stream all alerts directly into the appropriate service tools.

Microsoft is now really flexible, compared to what it used to be. This means that if businesses want to integrate third party, open-source platforms from outside of Microsoft and use them with Azure, they are able to do so.

Cloud Security

Security is fundamental to any business from any perspective. Security became more complex as COVID-19 accelerated migrations to the Cloud. So, how do Azure and AWS users secure their cloud networks and what tools do they use?

AWS Cloud Security

There have been a number of services released including GuardDuty, CloudTrail, and Security Hub. Broken down into different succinct services which each offer different focus points. They are made to work side by side and complement each other. For example:

[Amazon GuardDuty](#) is a threat detection service that continuously monitors for malicious activity and unauthorized behaviour to protect your AWS accounts, workloads, and data stored in Amazon S3. GuardDuty tends to target vulnerability management.

[AWS CloudTrail](#) is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account.

AWS also has a range of Firewall products. [AWS WAF](#) is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to an Amazon CloudFront distribution, an Amazon API Gateway REST API, an Application Load Balancer, or an AWS AppSync GraphQL API. Then there is AWS Shield Standard and Advanced. AWS Shield Standard is automatically included at no extra cost beyond what you already pay for AWS WAF and your other AWS services.

[AWS Shield Advanced](#) provides expanded DDoS attack protection for your Amazon EC2 instances, Elastic Load Balancing load balancers, CloudFront distributions, Route 53 hosted zones, and AWS Global Accelerator accelerators. Finally, the AWS Firewall Manager simplifies your administration and maintenance tasks across multiple accounts and resources for AWS WAF rules, AWS Shield Advanced protections, and Amazon VPC security groups.

To help access and analyse all this data, is [AWS Security Hub](#). This provides a comprehensive view of security alerts and security posture across AWS accounts. AWS Security Hub is a single place that aggregates, organizes, and prioritizes security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, AWS Systems Manager, and AWS Firewall Manager, as well as from AWS Partner Network (APN) solutions.

These services are becoming increasingly integrated into automated processes so that AWS should be able to identify, analyse, and mitigate risks for the user.

Azure Cloud Security

[Azure Sentinel](#) is a cloud-native security information and event management (SIEM) platform that uses Artificial Intelligence (AI) to help analyse large volumes of data across enterprises. Businesses can stream all of their security events into one place which is underpinned by Log Analytics. Sentinel allows users to run all security queries in one place and respond to any security events in the environment. Sentinel also has automated responses, so that it can automatically identify and respond to security events immediately.

There is also [Azure Defender](#). Integrated with Security Center, Azure Defender protects your hybrid data, cloud native services and servers from threats; and integrates with your existing security workflows such as your SIEM solution and Microsoft's vast threat intelligence to streamline threat mitigation.

Additionally, [Azure Arc](#) offers simplified management, faster app development and consistent Azure services. It helps to standardise visibility, operations and compliance across a wide range of resources and locations by extending the Azure control plane, which means you can use Azure Arc to manage platforms that are not rooted in Azure.

[Azure Firewall](#) is another security product available. There are different levels of Firewall. There is the Network Security Group (NSG) which is a Level 4 Firewall. Then you have the full Level 7 Azure Firewall which wraps around the perimeter.

Microsoft is increasingly focusing on its security and has approximately 90 connectors into different tools such as Firewalls, Junipers, Office 365, and Azure Security Centre. Data from all of these places is streamed into Sentinel, which allows security analysts to conduct deep dive analysis across all of these.

Cloud Security Cost

Regardless of whether a user is working in Azure or AWS, ensuring compliance and monitoring security can come at a cost, and whilst subscription services used to be really simple, the complex payment structures mean it's now much easier to build up costs.

This is why it is imperative to have a clearly structured Cloud strategy, with clearly defined pillars of how teams should approach different areas of the Cloud and areas of focus. Users should also be smart about what functions they really need turned on and what areas of the business really needs monitoring. Realistically, not everything in a business will need monitoring as closely, so it's important to prioritise.

CI/CD Pipelining

Continuous Integration (CI) and Continuous Development (CD) is fundamental to keeping businesses competitive and innovative. CI allows businesses to continuously integrate code into a shared, accessible repository, whilst CD allows that code to be taken and continuously delivered into production. CI/CD therefore creates an efficient process of getting a product to market before competitors, whilst continuously fixing bugs and issues to keep customers happy.

AWS CI/CD Pipelining

CI/CD in AWS can be agnostic in approach. This might include coming forward with a Jenkins offering (open-source platform) that might include deploying from other providers such as Azure. Users of AWS often leverage Gitlab CI/CD and Github Actions for CI/CD processes. Within AWS there are tools including AWS CodeCommit, AWS CodeBuild, AWS CodeDeploy, and AWS CodePipeline.

AWS CodeCommit: source control service that hosts secure git-based repositories, enabling teams to collaborate on code in a secure and scalable environment. This can be used to store application and deployment codes.

AWS CodeBuild: continuous integration service that collates source code, runs tests, and produces software packages that are ready to deploy on a dynamically created build server. This can be used to build and test code.

AWS CodeDeploy: development service which automates software deployments to a variety of services such as Amazon EC2, AWS Lambda, AWS Fargate, and on premises services.

AWS CodePipeline: continuous delivery service that automates release pipelines for fast application and infrastructure updates. You can use CodePipeline to create end-to-end pipelines that fetch the application code from CodeCommit, builds and tests using CodeBuild, and deploys using CodeDeploy.

AWS CloudWatch Events: can schedule automated actions that self-trigger at certain times

Amazon S3: offers scalability, data availability, security, and performance, and can be used to store the build and deployment artefacts created during the pipeline run.

AWS KMS: enables the creation and management of cryptographic keys and control their use across AWS services and in applications.

Azure CI/CD Pipelining

Azure can be managed agnostically and can be configured and managed through code. There are many CI/CD tooling options available to Azure users, but popular choices include Azure PowerShell and Azure CLI (command-line interface). Both are available in the Azure cloud or you can use them remotely from your workstation. On your workstation, you will have to install a module, but both are available in Azure Cloud Shell.

[Azure PowerShell](#) is an interface that allows users to automate and manage Windows Azure services. It is a command line tool that uses the scripts or cmdlets to perform tasks such as creating and managing storage accounts or Virtual Machines using the pre-set commands. Azure CLI is a set of commands used to create and manage Azure resources that is underpinned by a focus on automation.

There are also [Azure Resource Manager \(ARM\) Templates](#). ARM Templates are JavaScript Object Notation (JSON) files that define the infrastructure and configuration for your project. This enables users to roll out Azure "Infrastructure as code" easily and repeatedly, by creating and deploying an entire Azure infrastructure declaratively.

[Terraform](#) can also be used in conjunction with Azure, and is an "infrastructure as code" tool, similar to AWS CloudFormation, which enables users to create and update your AWS infrastructure.

By using these tools, by conducting thorough code reviews, and pre-defining objects, human error is reduced the processes are made more repeatable.

Kubernetes: Pros and Cons

Kubernetes has been rapidly scaling since its inception and has become a real buzzword in the DevOps landscape. Like with many other business decisions, the use of Kubernetes is predominantly down to preference, but here we take a look at the advantages and disadvantages.

Advantages

- Can increase productivity
- Can help attract talent
- Future proof solution
- Can improve application stability
- Can be cheaper than alternatives

Disadvantages

- Can be too much for simple applications
- Complexity can reduce productivity
- Transitioning to Kubernetes can be laborious
- Can be more expensive than alternatives

When considering Kubernetes for a business, it's important to review the specific business needs, goals, priorities, and available resources. If appropriate for the business, Kubernetes can improve service quality and productivity. However, poor implementation can lead to excessive costs and lots of time being wasted on training for a tool that is overkill for certain businesses.

Tooling Spotlights

AWS Cloud Development Kit (CDK)

AWS CDK is a framework for defining cloud infrastructure in code and driving this through development teams, pipelines, and processes. This enables users to define all cloud resources in a familiar programming language such as TypeScript, JavaScript, Python, Java, and C# / .NET. Developers can then use their preferred languages to define reusable cloud components which can be composed together in Stacks and Apps.

Azure DevOps

Azure DevOps is a completely agnostic platform which provides version control, reporting, requirements management, project management, automated builds, testing, and release management capabilities, covering the full application lifecycle. It is built to enable and support DevOps capabilities, through the setup of processes that underpin a culture bringing development, operations, project management, and other contributors, closer together to complete software development and delivery more efficiently.

Summary

Both AWS and Azure are popular Cloud Tech providers and each cover very similar products, just with their own tooling. Like with any other major business decision, the best choice for cloud tech really varies depending on the business requirements, size, goals, and available resources.

With pressure increasing for businesses to migrate towards cloud platforms, it's more important than ever for businesses to assess their current position and start planning ahead, taking into consideration the accessibility, security, and tooling of each cloud platform provider, to decide which is best for their business.

For support building your Cloud and DevOps team to support migration or to improve your current Cloud network, get in touch with Lloyd Lawson at Maxwell Bond, the recruitment partner of choice for all technology and digital hiring across the UK and Germany.

Contact Us

Build high performing teams through exceptional staffing solutions and business advice with Maxwell Bond, the recruitment partner of choice across the UK and Germany.



Lloyd Lawson
Cloud & DevOps Consultant at Maxwell Bond
lloyd.lowson@maxwellbond.co.uk
0161 359 3260