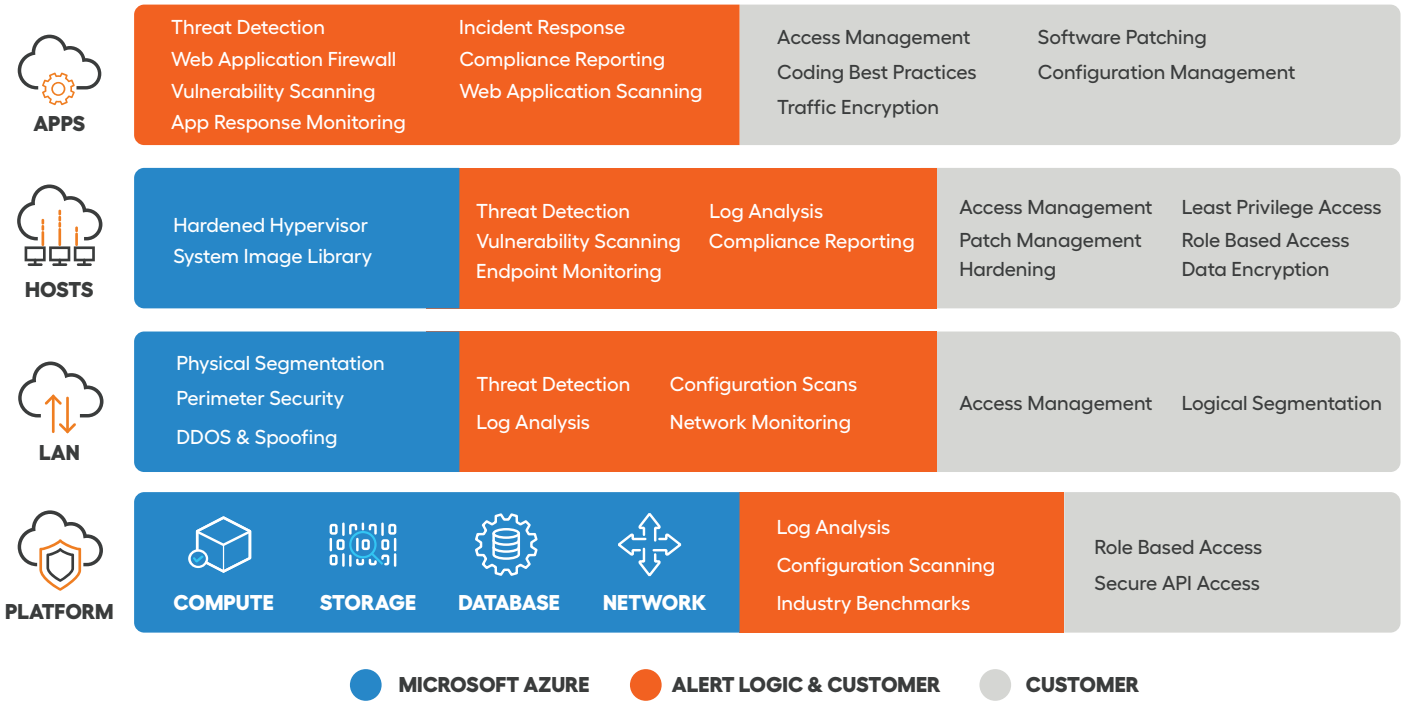
ALERT LOGIC™

SOLUTION BRIEF

# Alert Logic MDR for Microsoft Azure

Microsoft Azure cloud services provides many business and technical benefits for organizations. The ability to quickly build, test, and deploy new applications in Azure allows organizations to get faster time-to-value for their business outcomes. Security professionals understand cloud security is in a constant state of evolution as there are new attack techniques, new threat variants, and an increasing attack surface due to the rising adoption of Azure. When it comes to securing Azure it's important to understand it's a shared responsibility between you and Microsoft.



## Understanding shared security responsibility

At a high level, Microsoft is responsible for security of the cloud which includes physical security, instance isolation, and protection for foundation services. You are responsible for security in the cloud which is the applications and date within Azure. Things can get a little trickier as you dig into the different services within Azure so it's important to better understand the Azure stack to ensure there are no gaps.

For IaaS workloads running on Azure, Microsoft is responsible for securing the foundational services of the cloud, such as compute power, storage, database and networking services, and you are responsible for the configuration of those services and your data on the cloud. You are responsible for network traffic protection, and any incident reporting. The application security components of your site are also your responsibility.

For PaaS workloads, such as Azure AppServices or SQL, Microsoft is responsible for managing the security of the Host Infrastructure (VMs) and Network Controls (Virtual Networks, Endpoints, and Network Security Groups or Access Control Lists).

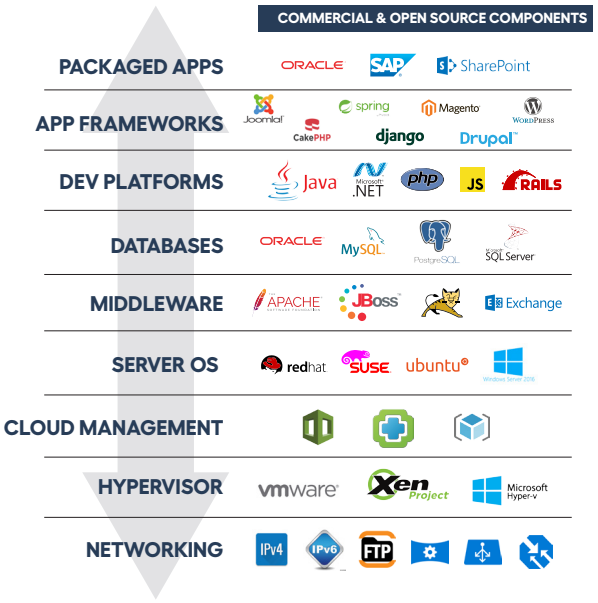
Microsoft's Active Directory and Azure Active Directory can be used to manage the Access Management area, however this is something you have to implement and configure for your IaaS or PaaS deployments. Microsoft is not responsible for things like security monitoring, threat detection, and vulnerability management. This is where Alert Logic can help.

## Protecting the Azure stack

Alert Logic brings together award-winning SaaS delivered security technologies, continuous threat research and analytics, and round-the-clock security experts to address the areas you are responsible for in protecting Azure.

We integrate these unique insights with other global sources of threat intelligence and content to continually enrich vulnerability scanning, threat detection analytics and blocking logic. The result: vulnerability scans, incident reports and live consultations that give you context and confidence to know when and where to act.

Alert Logic includes a managed, in-line Web Application Firewall (WAF), and targets attacks that follow patterns consistent enough to trigger high-confidence millisecond blocking decisions. Web application security experts in our SOC continuously tune your blocking and white-listing logic to each of your applications to avoid false positives. The WAF is load-balanced in Azure to support cloud-scale application performance and availability.




Full-stack security includes continuously updated insights into vulnerabilities of 3rd party frameworks and libraries

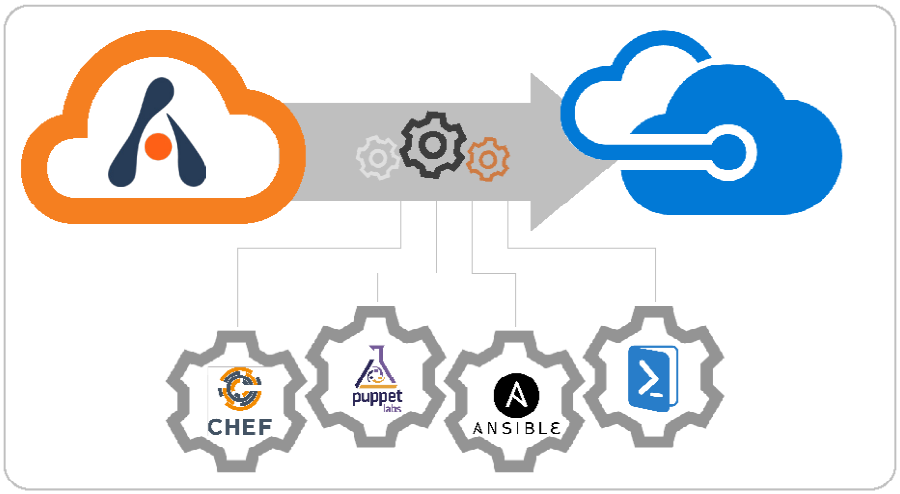
For the remaining majority of attacks, where there is no immediately clear black or white, we apply the gold standard of effective threat detection: analytics and experts together. The Alert Logic security operations team leverages multiple layers of analytics, including machine learning and anomaly detection as well as signatures and rules. Analytics are used and enhanced by experts from a variety of disciplines including security research, threat intelligence, data science, and Security Operations Center (SOC) analysts. Together, they act as your virtual security team in the cloud, providing 24x365 monitoring, enriched incident reports, remediation advice and live notification within 15 minutes of critical incidents.

## Accelerate application production with API-driven Automation and agility

You can see cloud computing's disruptive effect on traditional enterprise security as application, operations and security teams struggle to reconcile opposing security models. The old world: weeks-long, change-controlled, manual releases into IT-controlled data centers guarded by perimeter firewalls. The new world: minutes-long, developer-controlled, automated releases and continuous delivery into cloud platforms where monolithic security gateways inhibit cloud-scale applications. Alert Logic helps bridge these two worlds with a single workload security solution that uses APIs to integrate into cloud, hosted and on-premises environments. For Azure, Alert Logic has designed security from the ground up for agility and scale. Our virtual appliances are Microsoft Azure Certified for use in Azure deployments, and our Azure Resource Manager (ARM) templates and orchestration tool recipes for Chef, Puppet and Ansible make it easy to blend security seamlessly into your production pipeline and dynamic production environment.

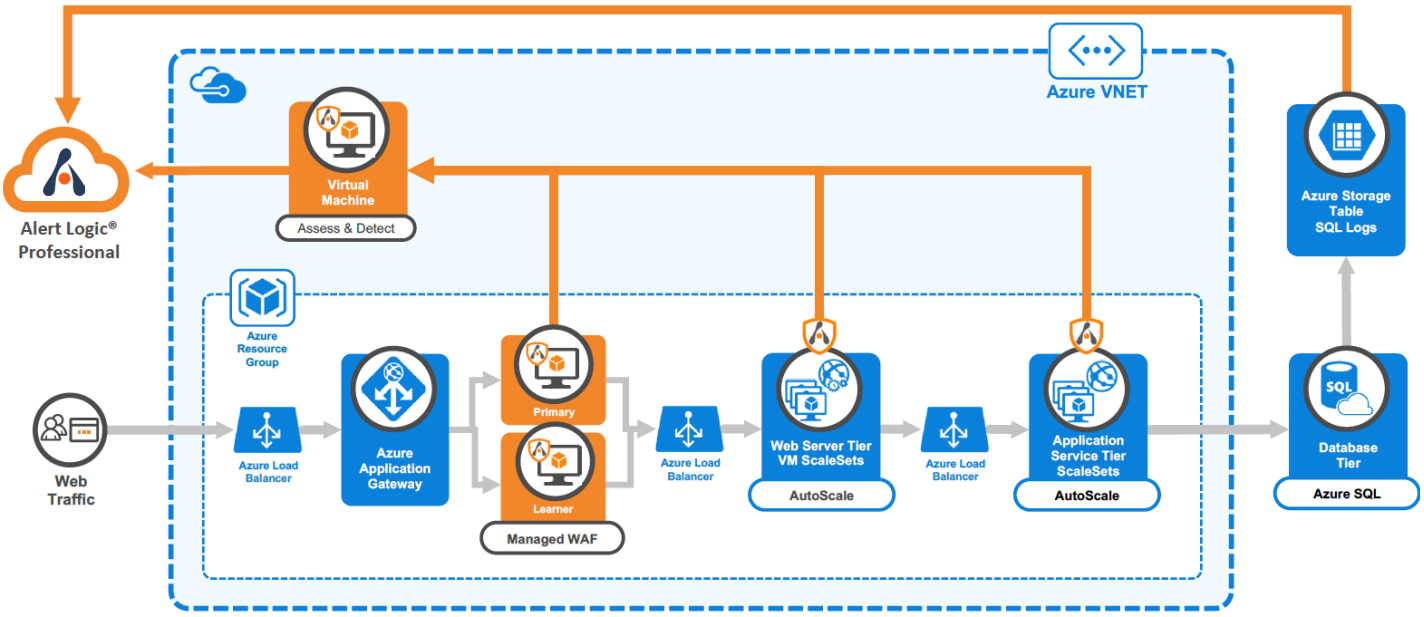
Our integration with Azure makes it easy:

- Deploy directly from Azure Marketplace into your Azure VNets or security workgroups
- Embed security controls into your pipeline automation
- Ensure applications and data are protected as your Azure environment grows and changes dynamically
- Protect against cyberattacks that target your Azure-hosted containers
- Eliminate repetitive manual tasks that can be prone to costly errors



## Agile, cloud-scale security

Deploying Alert Logic® in Microsoft Azure is fast and easy. Our architecture scales to support large migrations and expanding deployments across multiple regions in Microsoft Azure, AWS, Google Cloud Platform, and on-premises environments.




1. **Alert Logic MDR Professional** is a service that delivers 24/7 threat detection and incident management with a 15-minute triage SLA, MDR Concierge support, vulnerability scanning, asset visibility, and endpoint detection and response for Microsoft Azure.

2. **Alert Logic virtual machines** are Microsoft Azure Certified and optimized for Azure to:
   - Detect vulnerabilities and configuration issues in operating systems and applications
   - Provide preliminary detection of intrusions, web application attacks and data exfiltration attempts prior to analysis
   - Consolidate and forward log collection data
   - Deploy quickly and easily from Azure Marketplace or by using our Azure Resource Manager (ARM) templates or orchestration tools like Chef, Puppet and Anisble

3. **Alert Logic data collection agents** extract data from each layer of your Azure workloads and forward to Alert Logic virtual machines and security operations team for further analysis, reporting and alerts. Data collected includes:
   - Distributed network traffic (ingress/egress and lateral “east/west” traffic)
   - Comprehensive logs (syslog, Windows event log, local flat files)
   - Application HTTP session requests and responses

4. **Azure API Integration:** Alert Logic integration with Azure APIs automates the collection of log data from Azure Monitor and Azure Storage Accounts (Blobs or Tables)—such as Azure SQL or IIS logs from AppServices workloads—for custom alerts and reporting.

5. **Fully Managed Web Application Firewall:** Alert Logic offers a managed, in-line, proxy-based Web Application Firewall (WAF) designed to stop web application attacks in real-time. WSMP is built to inspect HTTP traffic on Day 1 using out-of-the-box rules and signatures covering more than 10,000 vulnerabilities. Dedicated experts work directly with customers to integrate, tune and customize each WSMP deployment to optimize detection and blocking protection. Integrated deployment with Azure Load Balancers ensures scalable performance with high availability.

## Right-sized protection for a tailored approach to security

Alert Logic offers comprehensive security coverage in easily consumable packages that can be blended together to provide cost effective security outcomes, to grow and change as your organization does.

**Alert Logic MDR Platform:** Powering all Alert Logic's offerings the MDR Platform provides endpoint, network & application coverage with full hybrid coverage (On-Premises, Cloud & SaaS) and uses machine learning, behavioural, and traditional analysis techniques to uncover exposures and threats to customer's security.

## The Alert Logic MDR platfomr can be leverage in a number of ways:

**Alert Logic MDR Essentials:** For the low risk assets and client systems, Essentials delivers cost effective asset discovery, vulnerability and configuration scanning, and endpoint detection & response.

**Alert Logic MDR Professional:** For mission critical and high-risk assets, MDR Professional delivers 24/7 threat detection and incident management with a 15-minute triage SLA, MDR Concierge support, vulnerability scanning, asset visibility, and endpoint detection and response.

**Alert Logic MDR Enterprise**: An extension of your Staff, the designated security expert provides in depth individualized evaluation, protection & customized response services, leveraging the Alert Logic MDR Professional Service.

**Alert Logic Fully Managed WAF:** For customers running critical or high risk web applications the Alert Logic Web Application Firewall takes the burden off customers of operating a complex technology.

## Learn more by going to alertlogic.com/azure

**Alert Logic Named A Leader**
**The Forrester Wave™: Global Managed Security Services Providers, Q3 2020**

FORRESTER®

ALERT LOGIC™