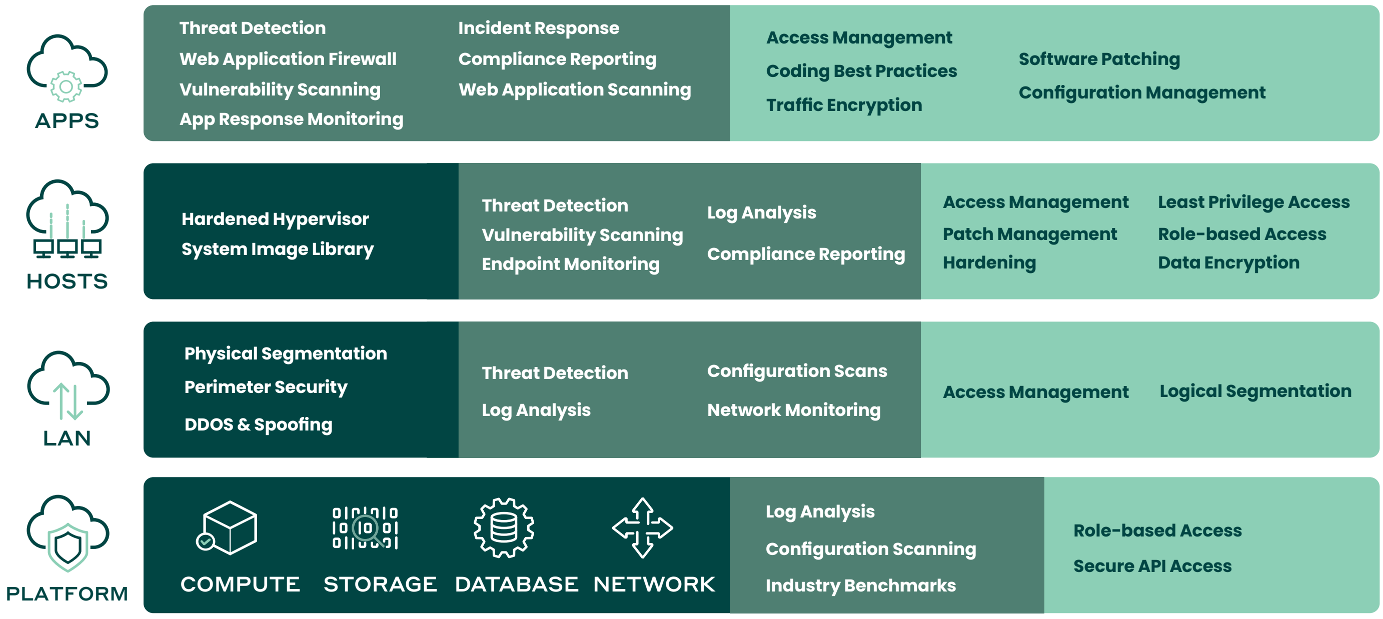
FORTRA

SOLUTION BRIEF (Alert Logic)

Alert Logic MDR for Microsoft Azure

Microsoft Azure cloud services provides organizations with many business and technical benefits. 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 this is a shared responsibility between you and Microsoft.



APPS		Threat Detection Web Application Firewall Vulnerability Scanning App Response Monitoring Incident Response Compliance Reporting Web Application Scanning	Access Management Coding Best Practices Traffic Encryption Software Patching Configuration Management
HOSTS	Hardened Hypervisor System Image Library	Threat Detection Vulnerability Scanning Endpoint Monitoring Log Analysis Compliance Reporting	Access Management Patch Management Hardening Least Privilege Access Role-based Access Data Encryption
LAN	Physical Segmentation Perimeter Security DDOS & Spoofing	Threat Detection Log Analysis Configuration Scans Network Monitoring	Access Management Logical Segmentation
PLATFORM	COMPUTE STORAGE DATABASE NETWORK	Log Analysis Configuration Scanning Industry Benchmarks	Role-based Access Secure API Access

● Microsoft Azure ● Alert Logic & Customer ● Customer

***Diagram 1:** Shared Services Responsibility Model (SSRM)*

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 data within Azure. Things can get a little trickier as you dig into the different services within Azure so it's important to 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, your data on the cloud, network traffic protection, and any incident reporting. The application security components of your site also are 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 Fortra's Alert Logic can help.

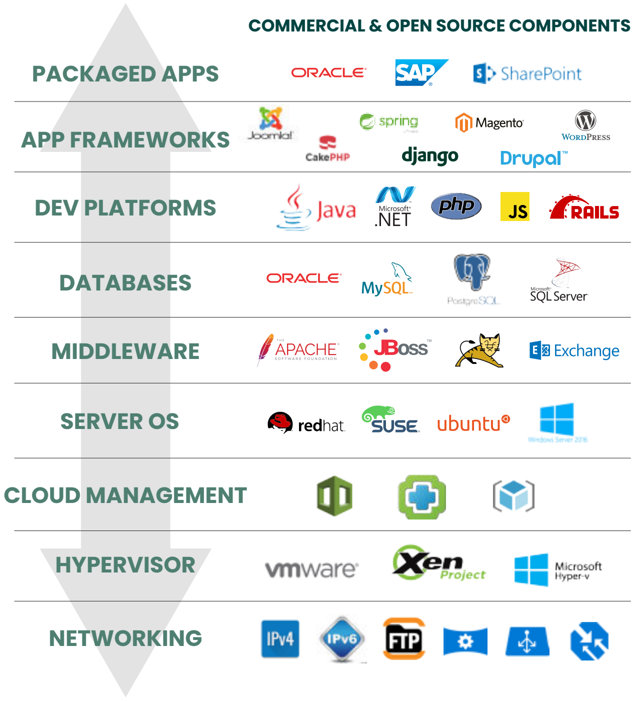
Protecting the Azure Stack

Alert Logic brings together award-winning SaaS delivered security technologies, continuous threat research and analytics, and round-the-clock security experts to address those 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's managed, in-line Web Application Firewall (WAF) targets attacks that follow patterns consistent enough to trigger high-confidence millisecond blocking decisions. Web application security experts in our Security Operations Center (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.

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 working together. Our 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 SOC analysts. Together, they function as your virtual security team in the cloud, providing 24/7 monitoring, enriched incident reports, remediation advice, and live notification within 15 minutes of critical incidents.



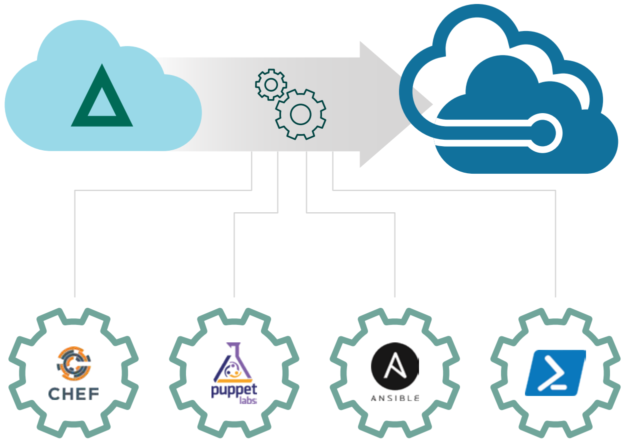
Full-stack security includes continuously updated insights into vulnerabilities of third-party frameworks and libraries

Accelerate Application Production with API-driven Automation & 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, and 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 to ensure 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.

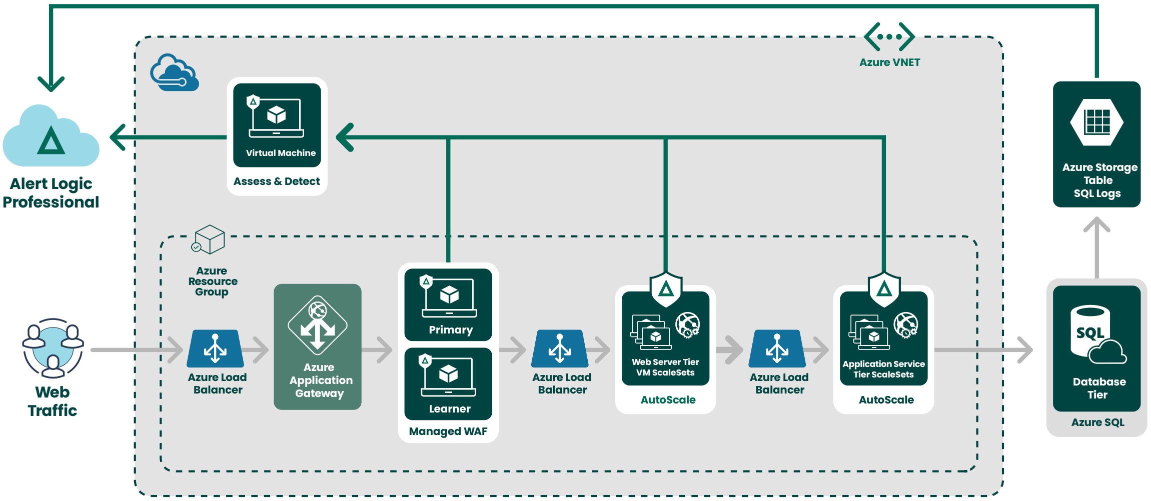
Our integration with Azure makes it easy to:

- 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-scaled Security

Deploying Alert Logic in Microsoft Azure is both 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. Fortra's Alert Logic 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 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 ARM templates or orchestration tools such as 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 our SOC team for further analysis, reporting, and alerts. Data collected includes:

- Distributed network traffic (ingress/egress, lateral east/west traffic)
- Comprehensive logs (syslog, Windows event log, local flat files)
- Application HTTP session requests and responses

4. 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. Our managed, in-line, proxy-based Web Application Firewall (WAF) is 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 Balancer 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 that can grow and change as your organization does.

Powering all Alert Logic's offerings, the Alert Logic MDR platform provides endpoint, network, and application coverage with full hybrid coverage (on-premises, cloud, SaaS) and uses machine learning, behavioral, and traditional analysis techniques to uncover exposures and threats to customer's security.

Leveraging the Alert Logic MDR Platform

Fortra's Alert Logic MDR® Essentials: For low-risk assets and client systems, MDR Essentials delivers cost-effective asset discovery, vulnerability and configuration scanning, and endpoint detection and response.

Fortra's 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.

Fortra's Alert Logic MDR® Enterprise: Working as an extension of your staff, your designated security expert provides in-depth individualized evaluation, protection, and customized response services, leveraging Alert Logic's MDR Professional service.

Fortra's Alert Logic WAF: For customers running critical or high-risk web applications, our Web Application Firewall takes the burden off customers of operating a complex technology.

For more information, please visit **alertlogic.com/azure**

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.