Alert Logic SIEMless Threat Management solutions provide an award-winning threat management platform, expert intelligence, and an elite team of security professionals for the right coverage at the right time for your Azure-hosted applications. We help our customers comply with mandates like PCI, HIPAA and SOX COBIT. We focus on threats most relevant to cloud-hosted applications by defending each layer of your application and infrastructure stack against hard-to-detect web application attacks such as SQL injection, path traversal and cross-site scripting as well as other server-side threats such as privilege escalation, brute force and advanced malware. Integrated expert services for threat detection, blocking and compliance augment your in-house security while empowering cloud and application professionals to better secure their environments.

- **Reduce your risk** by protecting your full application and infrastructure stack
- **Add security experts** to your team overnight without hiring staff
- **Accelerate secure application deployments** with API-driven automation and elasticity
- **Protect your cloud applications from attacks** with technology that doesn’t impact performance
- **Simplify and save** with one service that works across cloud and on-premises environments

"Alert Logic has a head start in the cloud, and it shows — Alert Logic is an excellent fit for clients looking to secure their current or planned cloud migrations, clients requiring a provider that can span seamlessly between hybrid architectures, and those that demand strong API capabilities for integrations."

– Forrester 2016 MSSP WAVE™ Report
FOCUS ON THE MOST CLOUD-RELEVANT THREATS

Security in Microsoft Azure is a shared responsibility. Microsoft is responsible for security of the Cloud, such as physical security, instance isolation and protection for foundation services. You are responsible for security in the Cloud, meaning you must secure your applications and data within Azure. When moving from your own data center to cloud computing, your list of security responsibilities may actually be shorter. But that doesn’t necessarily make it easier.

Microsoft invests over a billion dollars annually in security, much of which is spent to secure their platforms against attacks at the network, infrastructure, and hypervisor layers. Users can implement automation and continuous patch management, to create “immutable infrastructure” that prevents host-based threats from retaining a foothold. Cloud innovations such as these are making it more difficult and less profitable for adversaries to attack the lower end of your application and infrastructure stack.

While the bottom of the stack is hardening, the top is softening. Businesses are increasingly dependent on inherently vulnerable custom web applications. Accelerated by a potent mix of cloud architectures, DevOps practices, platforms and frameworks such as WordPress, Magento, PHP and ASP.NET, web applications are expanding the enterprise attack surface with more inherited vulnerabilities while inviting attacks that are increasingly difficult to detect.
Alert Logic invests in research and threat intelligence to understand vulnerabilities, exploits, methods and attack behaviors across each layer of your application and infrastructure stack and the open source and commercial components within them.

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.

**REBALANCE YOUR DEFENSES FOR CLOUD THREATS**

**The Challenge**
Web applications have long been under-protected. Enterprise spending on network perimeter security has dwarfed application security 23:1, yet 59% of IT security professionals said traditional tools work somewhat or not at all in hyper scale cloud environments². Forcing cloud traffic to pass through perimeter appliances like next-generation firewalls and intrusion prevention appliances creates performance choke points and single points of failure that disrupt business and slow down production applications.

The reflex to block more and more attacks at the perimeter is also increasingly ineffective. Blocking requires ultrahigh confidence decisions to be made in milliseconds, but a smaller percentage of attacks announce themselves so clearly anymore. Those responsible for the most breaches such as SQL injection and cross-site scripting often hide in plain sight and regularly slip past expensive next-gen firewalls undetected.

**Our Solution**
Alert Logic develops and uses multiple technologies to strike the right balance for cloud and hybrid environments. Alert Logic Enterprise 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.

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 24/7 monitoring, enriched incident reports, remediation advice and live notification within 15 minutes of critical incidents.

"Any company who needs to secure their Azure environment needs Alert Logic. There’s simply nothing else on the market that can cover it effectively." – Jonathan Ranes, CIO at Upsilon Payments

---

**PACKAGED APPS**
- Oracle
- SAP
- SharePoint

**APP FRAMEWORKS**
- Angular
- ASP.NET
- Django
- Java
- Node
- Ruby
- Rails

**DEV PLATFORMS**
- .NET
- Java
- Python
- Ruby

**DATABASES**
- SQL Server
- MySQL
- Oracle

**MIDDLEWARE**
- Apache
- Apache Tomcat
- Chef
- Docker

**SERVER OS**
- Fedora
- SUSE
- Ubuntu
- Windows

**CLOUD MANAGEMENT**
- Azure Monitor
- Azure Active Directory

**HYPERVISOR**
- vSphere
- Xen
- XenServer

**NETWORKING**
- Cisco
- Microsoft
- VMware

Includes continuously updated insights into vulnerabilities of 3rd party frameworks and libraries
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

“Alert Logic has enabled us to protect datacenters in our multi-cloud environment and we appreciate the security continuity we receive from Alert Logic as we move all-in on Azure.”
- Tom Cibelli, Solutions Engineering Manager at Bentley Systems
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. **ActiveWatch™ Professional** is a managed threat detection service that combines anomaly detection and machine learning with 24/7 expert monitoring of Alert Logic deployments within your Microsoft Azure environment. Alert Logic analysts provide live customer notification within 15 minutes of detecting high and critical priority attacks; providing specific and actionable details.

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 Ansible

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. **Elastic Web Application Firewall:** Alert Logic Enterprise includes 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.

---

1. Gartner Research G00269825, Joseph Feiman, 2014

---

### THREE LEVELS OF PROTECTION FOR A TAILORED APPROACH TO SECURITY

Quickly modify your coverage to fit your needs without time-consuming contract negotiations. Get the right level of coverage and the right resources across any environments.
<table>
<thead>
<tr>
<th>SECURITY PLATFORM</th>
<th>ESSENTIALS</th>
<th>PROFESSIONAL</th>
<th>ENTERPRISE</th>
</tr>
</thead>
<tbody>
<tr>
<td>The right combination of assessment, detection, and web security technology</td>
<td>Deployment Automation and Scope Selection</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Continuous Asset Discovery and Visibility</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Vulnerability Scanning - Network Based</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Cloud Configuration Exposure Scanning</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Threat Risk Index Report</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Security Posture Report</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Comprehensive Reporting Portfolio</td>
<td>●</td>
<td>●+</td>
</tr>
<tr>
<td></td>
<td>Log Management and Search</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Network Intrusion Detection</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Log Based Intrusion Detection &amp; Analytics</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Security Analytics: Rules, Machine Learning</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Managed Web Application Firewall</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Web Application Anomaly Detection</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Service Health Monitoring and Support (continuous)</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>PCI ASV Support</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>24/7 Triage, Escalation and Response Support</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Security Posture Reviews</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Designated Security Analyst</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>Threat Hunting</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>THREAT INTELLIGENCE</td>
<td>Vulnerability and Remediation Content</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Cloud Configuration Exposure Content</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Threat Risk Index Content</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Threat Intelligence Feeds</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Intrusion Signature Content</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Log Content</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Rule Based Content</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Network Based Machine Learning Content</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

© 2018 Alert Logic, Inc. All rights reserved. Alert Logic and the Alert Logic logo are trademarks, registered trademarks, or servicemarks of Alert Logic, Inc. All other trademarks listed in this document are the property of their respective owners.