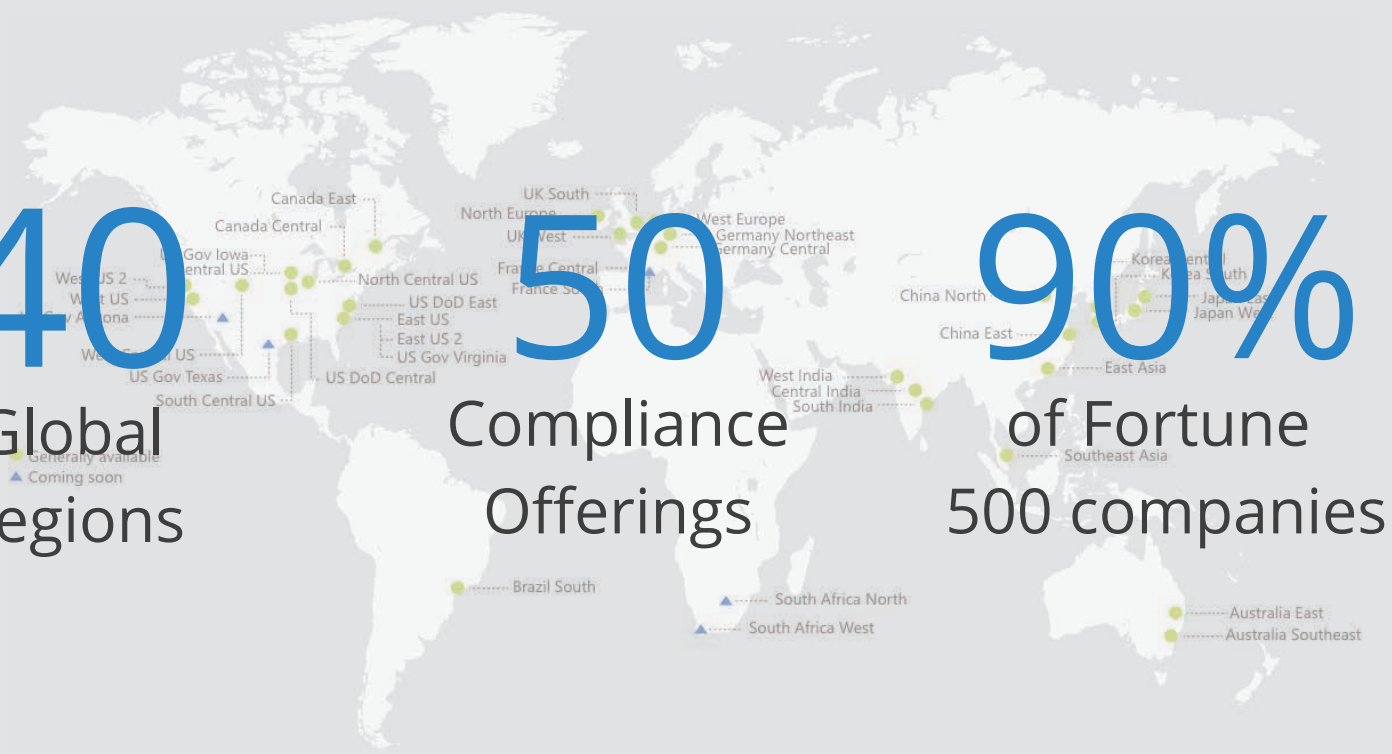
mediavalet™

Gold Microsoft Partner

THE ONLY DAM BUILT ON MICROSOFT AZURE

The Trusted Cloud



40 Global Regions

50 Compliance Offerings

90% of Fortune 500 companies

- Committed to innovation – $15 billion (USD) investment in global datacenter infrastructure
- Largest global reach – data residency enabled through data centres in 40 regions around the world
- Security and privacy are embedded in the Azure platform, using SDL (Security Development Lifecycle)
- The ultimate performance – record-breaking performance and reliability that can handle your largest scale media
- Highest compliance level – the most comprehensive set of certifications and attestations of any cloud service provider (FIPS, HIPAA/HITECH, FERPA, ISO/IEC 27018)

MORE CERTIFICATION THAN ANY OTHER CLOUD PROVIDER

ISO/IEC | CSA/CCM | ITAR | CJIS | HIPAA | IRS 1075

Website: www.mediavalet.com | **Email:** info@mediavalet.com | **Toll Free:** 1 (877) 688 2321 | **Global:** 1 (604) 688 2321

INFORMATION SECURITY AT MEDIAVALET

MediaValet is Software-as-a-Service that was built from the ground-up to maximize the performance, scalability, reliability and security of the Azure Platform-as-a-Service (PaaS) cloud. By using a pure PaaS technology stack, the responsibility of configuration, management and securing of network, system and physical infrastructure is fully covered by Azure, the trusted cloud.

MediaValet proactively shares the responsibility of providing a secure and trustworthy Digital Asset Management platform with Azure and with the customer.

RESPONSIBILITY	AZURE PAAS	MEDIAVALET SAAS	CUSTOMER END USER
DATA CLASSIFICATION & ACCOUNTABILITY	None	Shared	Shared
CLIENT & ENDPOINT PROTECTION	None	Shared	Shared
IDENTITY & ACCESS MANAGEMENT	Shared	Shared	Shared
APPLICATION LEVEL CONTROLS	Shared	Shared	None
NETWORK CONTROLS	Shared	Shared	None
HOST INFRASTRUCTURE	Full	None	None
PHYSICAL SECURITY	Full	None	None

DATA CLASSIFICATION AND ACCOUNTABILITY

Customer data is treated as internal-use only by default. Only authorized users of the customer can access the digital assets in their MediaValet library. In order to ensure that customer data is protected from unauthorized access and minimize the possibility of a breach:

- Data is encrypted in-transit and at-rest. Azure Storage Service Encryption that uses AES-256 is used to secure data-at-rest. TLS 1.2 is used to secure data-in-transit.
- Customer decides the geographic region where it needs its digital assets to be stored at. This allows MediaValet customers to comply with data residency requirements that they may have.
- If MediaValet personnel needs to get access to customer data in order to provide training or support or provide some other type of service, MediaValet will ask the customer for permission to access their library first.
- Audit logs of all operations on digital assets (i.e. view, upload, download, edit, comment, etc.) are available and provides visibility into the custodial chain of ownership.

MediaValet also provides its customers with features such as upload and download policies to help facilitate compliance with data classification and usage requirements that they need to enforce. Customer's users can be required to agree to its own Terms and Conditions prior to an upload and ensure that all the required attributes and licensing requirements are there. They can also be required to fill in asset usage forms and agree to licensing or legal requirements as well before being allowed to download.

CLIENT AND ENDPOINT PROTECTION

MediaValet understands that client and endpoint protection is a shared responsibility between MediaValet and its customers. Hence, MediaValet implements security measures internally such as a next gen firewall, client endpoint protection software etc. to ensure that staff developing, operating and supporting the application are protected.

Although it is the responsibility of MediaValet's customers to secure their computers and devices, MediaValet goes the extra mile of ensuring that a vulnerability scan including the OWASP Top 10 is performed regularly on the MediaValet application. Automated code analysis that includes security rules is also implemented during the development cycle to ensure that code is secure before it gets deployed. This helps ensure that the MediaValet application is not the weak link in the security chain.

IDENTITY AND ACCESS MANAGEMENT

The MediaValet application used by customers follow the OAuth 2.0 standard and customers can optionally use Azure Active Directory as well for sign-on. Each MediaValet customer has their own administrators who manage users, roles and access rights. Role-based Access Control (RBAC) is used to simplify administration of access privileges of users within the system. Access to categories, download or upload permissions, or even asset approval rights are granted based on a user's role.

For the MediaValet operations and support team that deal with development, operations and support, access to the Azure platform is granted using Azure Active Directory (AAD). In fact, all employees of MediaValet are on AAD. For people who have access to production data, multi-factor authentication is enforced as well as an additional layer of security. Role-Based Access Control is also used for internal MediaValet access to the Azure platform for development, operations and support purposes.

APPLICATION LEVEL CONTROLS

The MediaValet portal and platform run on several Azure PaaS services that include the following:

- App Services
- Cloud Services (Classic)
- Service Fabric Clusters
- Storage Services
- Media Services
- Cosmos DB
- SQL DB
- Search Service
- Key Vault
- Service Bus
- Application Insights

The MediaValet portal and API are the only two applications that serve as a gateway to MediaValet platform. Both of these run on App Services and the only endpoints enabled for this are HTTP TCP 80 and HTTPS TCP 443. All HTTP traffic are redirected to HTTPS that uses SSL. Access to the portal and the API require authentication and authorization. Logging is enabled on all web services and it can be used to identify security incidents, audit transactions and monitor performance.

The rest of the MediaValet platform is not exposed to the public. All requests going to the other services needs to get authenticated and authorized by the API. Storage and data services such as Cosmos DB and SQL DB are all partitioned per customer and will only communicate internally via an encrypted channel with other MediaValet service instances. Azure Storage Services Encryption is enabled on the geo-redundant storage accounts used by the platform. Cryptographic keys and secrets are managed and implemented using Azure Key Vault. The entire MediaValet platform is instrumented with Application Insights to provide telemetry and proactive application performance issue detection to the MediaValet operations team.

The product engineering team works on a development platform that is running in its own, separate Azure subscription that is only accessible to the developers. Once code is ready to be tested, an automated deployment pipeline is used to push the same code to another Azure subscription that is dedicated for testing and quality assurance. In that environment, the testers have access to the code. Once it passes quality assurance, then the same code base is deployed using the same templates and pipeline to various Azure subscriptions used for production environments in different regions.

The above-mentioned controls describe how MediaValet implements configurable service-level controls made available by Microsoft Azure. In a similar fashion, MediaValet also provides its customers with tools in which in can implement controls within their own accounts. Upload and download policies, access rights, sharing capabilities are managed by the MediaValet customer.

NETWORK CONTROLS, HOST INFRASTRUCTURE AND PHYSICAL SECURITY

All MediaValet application software is deployed on one or more types of Azure PaaS compute services and these applications leverage the compute capabilities of the services they are deployed on and they may also leverage other Azure services. For example, MediaValet file management services is deployed as an application on service fabric. If a file needs to be stored on an Azure Storage blob container, the file management application running on Service Fabric will receive that request and it will utilize the Azure Storage Service. As far as the MediaValet development and operations team is concerned, it just needs to ensure that the file management application running on Service Fabric communicates in an encrypted manner with the Storage service. The storage service is configured to encrypt the file and provide geo-redundancy. MediaValet communicates at the platform services-level and the development and operations team do not manage the network and host infrastructure. Hence, MediaValet depends on Microsoft Azure's commitment and capabilities for ensuring infrastructure reliability, data privacy and operational security.

As MediaValet is a customer of the Azure PaaS providing SaaS services to its customer and MediaValet recognizes that that security is a supply chain responsibility. So MediaValet has evaluated these dependencies to ensure that the controls and physical security are in place. As noted in Deloitte's SOC 2 AT 101 Type II audit report on Azure, operating systems are hardened and Azure employs mechanisms to re-image production servers with the latest baseline configurations at least once a month or detect and troubleshoot exceptions or deviations from the baseline configuration in the production environment. The Azure OS and component teams review and update configuration settings and baseline configurations at least annually. In addition, there is comprehensive reporting on the physical security controls in place in the same report. Links to the SOC 2 AT 101 Type II report and other SOC audit reports can be found at **https://www.microsoft.com/en-us/TrustCenter/Compliance/SOC.**