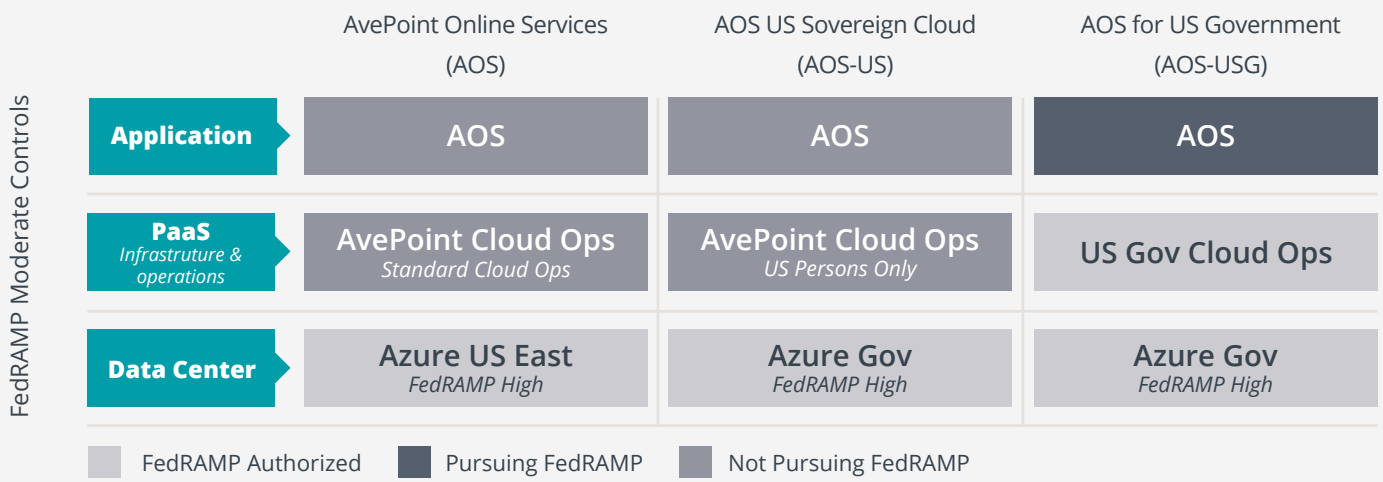
AvePoint

The Security of the AvePoint Cloud

More than 7 million users worldwide trust the AvePoint Cloud to migrate, manage, and protect their Microsoft 365 and other cloud collaboration platforms.

The AvePoint Cloud manages more than 50 petabytes of data and is offered across three different security levels: AOS-USG (*FedRAMP Moderate In-Process*), AOS-US, and AOS.

Understanding AvePoint Options for Government Customers



AOS-US

Our SaaS solutions are currently hosted in the US East Government Azure Data Center.

This is a FedRAMP accredited, GCC High data center that follows the certifications and accreditations for FedRAMP High as well as the Department of Defense Impact Level 5.

The service is not pursuing FedRAMP authorization, but is managed by an operations team consisting only of US persons.

AOS-USG *(FedRAMP Moderate In Process)*

Our cloud services are officially "In-Process" and will be fully authorized as a FedRAMP accredited SaaS solution at the Moderate impact level pending completion of our agency sponsored authority to operate (AT0) expected in early 2021.

AOS

AvePoint SaaS solutions are available in 12 Azure instances across the world. All US Azure datacenters are FedRAMP authorized.

They include everything you would expect from a robust, mature cloud offering including: an insider release program, dynamic resource availability, automated updates, and fixed subscription pricing.

Security is Standard at AvePoint

All of our offerings are backed by AvePoint's commitment to the highest security standards.

Engineering Security into Managing Office 365

- **RBAC to All Environments**
- **Secure Credentials & MFA**
- **Azure-Based Security**
- **Auditing & Alerting**

Security Event Response

- Monitoring/Auditing for all activity
- Alerting for potential risks
- SIEM integration for AOS platform
- 7*24 hour for security event response

Keeping Security in Customer's Hands

BYOK — **Customer-Owned Encryption Keys:** Azure KeyVault ensures unique keys for each tenant, owned and managed by each customer to prevent unauthorized access

BYOS — **Customer-Owned Data Storage:** Data Residency provides hosted options through Azure or through any customer-owned cloud and server storage service

BYOA — **Customer-Owned Authentication:** Single Sign-on with Office 365 Credentials and Azure AD applications ensures customers retain control of authentication and authorization of AOS

Other Key Features

Privileged Access

- AvePoint integrates with Azure AD to allow users to log in with their own Office 365 credentials
- Support for multi-factor authentication (MFA), user monitoring (including impossible traveler scenarios), and logging directly from Microsoft
- Security trim your admin team with role-based-access-controls (RBAC) to individual products
- AvePoint stores and manages no passwords!

Enterprise Monitoring

- AvePoint integrates with Systems Center (SCOM) for logging as well as providing its own independent logs of all administrator activity
- All activities for our application are logged through the customer's Office 365 tenant to ensure all access can be independently verified

Whitelist Known & Trust Contacts Only

- AvePoint publishes known IP ranges for our service to all customers to whitelist our application in their Office 365 environment
- IP whitelists ensure that access to either AvePoint Online Services or you Office 365 tenant come from known access points

Security Standards

AvePoint's Commitment to Information Security

AvePoint builds on the foundation and discipline necessary to develop and support some of the leading privacy and security products in the world. We have implemented a cross functional security and privacy team through which we engage senior management on issues, align policies, procedures and technical controls to demonstrate our process and our commitment to our customers and users, and train each of our employees on all privacy and security expectations.

Secure Development

AvePoint provides penetration testing as part of the platform, ensuring resiliency with certified security professionals (CEH, CCNP, CISSP). Application penetration test is performed in each product release. Software development lifecycle follows industry security standards (NIST 800-64 and OWASP) and verified through automated code quality and vulnerability checks against industry standard CVEs. Executive sign-off is embedded in the release cycle to ensure that security issues are addressed with high visibility and accountability.

Security & Privacy Training

AvePoint ensures its employees and contractors are aware of and fulfill their InfoSec responsibilities in accordance with A7.2.2 of the ISO 27001:2013 standard. AvePoint conducts a variety of mandatory InfoSec training events, including annual Privacy, Security, and Risk training and ad hoc department and role-specific training to ensure colleagues can effectively execute their InfoSec tasks responsibly. We supplement this training throughout the year with a variety of newsletters and social broadcasts to raise awareness throughout the company. Our Training and Awareness plan has been reviewed by an independent ISO 27001:2013 audit.

Secure Operations

AvePoint is ISO 27001:2013 certified. Our ISMS policies and procedures are reviewed least annually. Additionally, internal audits are conducted annually, and AvePoint is subject to annual third party surveillance audits to prove ongoing compliance. AvePoint abides by Segregation of Duties outlined in NIST 800-64 and OWASP development standards, ensuring that no one with code-level access could insert vulnerabilities or exploits through to our production environments, and no one with production environment access has any touchpoints with our code to introduce vulnerabilities. This is continually monitored through both white-hat penetration tests as well as automated code scans.

AvePoint Global Headquarters
525 Washington Blvd, Suite 1400 | Jersey City, NJ 07310
www.avepoint.com | +1 201.793.1111