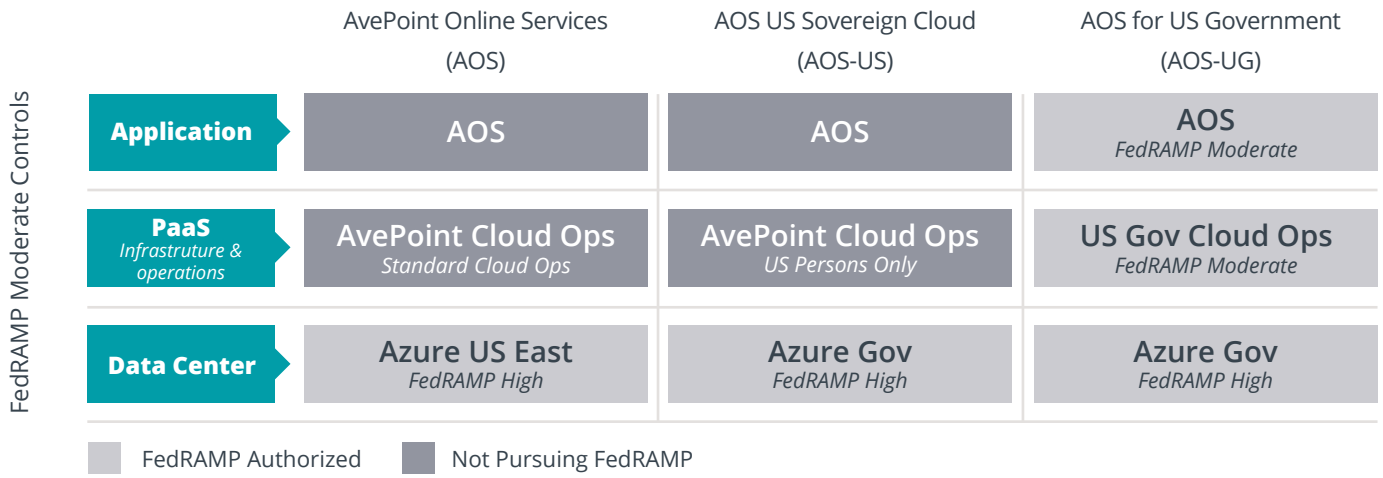
AvePoint

The Security of the AvePoint Cloud

More than 9 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 100 petabytes of data and is offered across three different security levels: AOS-UG (FedRAMP (moderate) Authorized), AOS-US, and AOS.

Understanding AvePoint Options for US Government Customers



AOS

AvePoint SaaS solutions are available in 14 Azure instances across the world. All US Azure data centers are FedRAMP (High) 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.

AOS-US

This application is for organizations that require a US sovereign cloud service. It is managed by a US personnel-only operations team and is hosted in an Azure Government Data Center, which is FedRAMP (High) Authorized and DOD IL5. This is NOT a FedRAMP Authorized SaaS application.

AOS-UG

Our cloud services are a FedRAMP (moderate) Authorized SaaS solution for use across all agencies. We renewed our authority to operate January 2022.

Security is Standard at AvePoint

All 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 your 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 engaged 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 polices 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 stands, ensuring that no one with code-level access could insert vulnerabilities or exploits through to our production environment access has any touchpoints with our code to introduce vulnerabilities. This is continually monitors through both white-hat penetration tests as well as automated code scans.

Our Commitment to Cloud Security: AvePoint has also earned the System and Organization Controls (SOC) 2 Type II certification that covers AvePoint Online Services (AOS). AvePoint Migration Platform (AMP), DocAve, Compliance Guardian, Governance Automation, and Records, that collectively migrate, manage, and protect data cross cloud and on-premises collaboration systems. The SOC 2 Type II audit and attestation, conducted by an independent CPA firm, confirms that AvePoint meets the strict information security and privacy standards for the handling of highly sensitive customer data established by the American Institute of Certified Public Accountants (AICPA). Our report is issued by independent third-party auditors and covers the principles of Security, Availability, Confidentiality, and Privacy.

AvePoint has a long-standing commitment to privacy and security. Achieving both the SOC 2 attestation and ISO 27001 certifications provides independent validation of our ability to provide the highest levels of protection for sensitive data. In addition to our formal certifications, AvePoint has also completed the security self-assessments through Cloud Security Alliance. This ensures we comply with broad industry standards to evaluate and document our security controls, and reliability for our valued customers and partners. AvePoint was assessed against official IRAP controls to verify its commitment to, and expertise in, protecting sensitive Australian government data. Sponsored by the Australian Transport Safety Bureau (ATSB), this assessment confirms that AvePoint adheres to the standard of cybersecurity and information security assessments for ICT systems processing or storing government information. Security and compliance, and the ability to adapt to evolving risks and requirements, are disciplines that must be practiced each day to ensure data protection, integrity, availability, and reliability.

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