

Advanced Technology Designed to Grow with You

AirWatch scales to support deployments of hundreds to thousands of devices through a robust architecture that is fully configurable according to your environment and requirements.

AirWatch is built on industry standard technology, making it easy to manage alongside your existing enterprise applications. AirWatch can be deployed in a highly available environment and fully supports disaster recovery configurations to minimize downtime.

Scalability

AirWatch's highly scalable architecture is designed to easily support from 10 to over 100,000 devices. The AirWatch solution consists of three main components: Device Services – used to communicate with your mobile devices, Admin Console – web application for administration and self-service, and the Database – used to store application data and device information. The frontend components of the application can be separated from the database server and deployed behind a network load balancer in an active-active configuration, which easily scales to support additional device capacity.

Multi-tenancy

AirWatch is multi-tenant and allows you to delegate role-based access and capabilities to both user groups and specific device groups. This allows your organization to absorb fragmentation within your corporate infrastructure (e.g. disconnect AD servers, forests, domains, locations) into a single instance of AirWatch. Enterprises can maintain control of all mobile assets at a global level while empowering IT administrators to maintain visibility and control of devices under their particular location or department.

Configurability

AirWatch is architected around the componentization of core functions. This allows you to deploy the software specific to your environment and architecture requirements. You get the option to choose if your end user ports are exposed to the Internet or on a separate server. If you want to scale a single component in the DMZ, AirWatch can be configured to scale only the components you need. If your company is deploying AirWatch on premise on your own hardware, our solution is designed to install on both physical and virtual servers and can be loaded on VMware or Hyper-V instances.

High Availability

AirWatch can be deployed in a highly available environment with all components made to instantly fail over without downtime. AirWatch supports utilizing network load balancers, VM HA technologies, and server clustering to provide a full highly available solution from the application servers to the SQL database.

Disaster Recovery

The AirWatch architecture fully supports Disaster Recovery configurations and the software can be setup in a remote data center and enabled in the event of a data center failure. Since AirWatch synchronizes your data to the remote data center, no information is lost during the failure and your mobile devices continue to function.

Automated Monitoring

You can automate the monitoring of your AirWatch deployment and components through a direct plug in to Microsoft's System Center Operations Manager (SCOM). Automated data retention jobs are available to keep relevant data and purge unneeded data to optimize performance and free up valuable space on your IT infrastructure.

Advanced Integration In the Cloud or On-premise

AirWatch securely integrates with AD/LDAP, Certificate Authorities, Email infrastructures and other enterprise systems both in a cloud and on-premise deployment model. For cloud deployments, the AirWatch Enterprise Integration Service (EIS) server connects your cloud instance to your on-premise services through a secure, self-service process directly from your AirWatch console. For on-premise environments deployed in tiered network models, the EIS server enables AirWatch to communicate to various corporate services across network layers.

Flexible Delivery

AirWatch offers both cloud and on-premise deployment options for our Enterprise Mobility Management (EMM) platform. The same exact solutions and infinite scaling capabilities are delivered with AirWatch Cloud and on-premise deployments, and you have the flexibility to migrate from one deployment to the other if your needs change.



AirWatch Cloud

AirWatch Cloud delivers our Enterprise Mobility Management (EMM) platform in minutes. No infrastructure or staffing investments required.

[Learn more.](#)

AirWatch offers both cloud and on-premise deployment options for our Enterprise Mobility Management (EMM) platform. The same exact solutions and infinite scaling capabilities are delivered with AirWatch Cloud and on-premise deployments, and you have the flexibility to migrate from one deployment to the other if your needs change.



AirWatch Cloud

AirWatch Cloud delivers our Enterprise Mobility Management (EMM) platform in minutes. No infrastructure or staffing investments required.





[Learn more.](#)



AirWatch On-Premise

Customize your Enterprise Mobility Management (EMM) deployment and have total control over your installation in your own environment.

Choose AirWatch Cloud or On-premise

AirWatch Cloud		AirWatch On-premise	
Unlimited scale with no hardware to purchase.	Deployment 	Scale to any number of devices (may require additional hardware).	
Implement in days. Quick Start Configuration Programs and custom programs available.	Implementation 	Implement in days. Quick Start Installation Programs and custom programs available.	
Best-in-class class technology from Cisco, EMC, Dell, F5, VMware and Riverbed.	Hardware 	Choose your own hardware. AirWatch provides a comprehensive installation requirements guide so you'll know what hardware you'll need.	
Configure collected and stored information based on custom privacy policies. Data stored in secure, enterprise-grade AirWatch Cloud.	Security 	Configure collected and stored information based on custom privacy policies. No data stored off-site.	

Best-in-class class technology from Cisco, EMC, Dell, F5, VMware and Riverbed.	Hardware 	Choose your own hardware. AirWatch provides a comprehensive installation requirements guide so you'll know what hardware you'll need.
Configure collected and stored information based on custom privacy policies. Data stored in secure, enterprise-grade AirWatch Cloud.	Security 	Configure collected and stored information based on custom privacy policies. No data stored off-site.
High availability and disaster recovery configurations with additional test environments included.	Architecture 	Develop based on your AirWatch installation requirements and sizing (may require additional hardware).
Preconfigured network seamlessly integrates your network systems.	Network 	Firewall and proxy configuration required for network system setup.
Integrate AirWatch EMM with enterprise systems with AirWatch Cloud Connector.	Integration 	Integrate directly with enterprise systems with APIs and firewall configurations.
Receive software upgrades and maintenance checks automatically.	Upgrades 	Choose when to upgrade based on AirWatch release schedule and OS/manufacturer updates.
Migrate to on-premise deployment at any time.	Migrations 	Migrate to AirWatch Cloud at any time.
Global data center and cloud operations team available 24/7/365; knowledge-base resources including SaaSWatch, ASK AirWatch and announcements; patch, upgrade and test management performed by AirWatch team.	Support 	AirWatch professional services and support teams; ASK AirWatch and health check programs available. Customer IT staff needed to oversee deployment.
Month-to-month subscription includes maintenance, upgrades and support.	Cost 	Annual maintenance fees include access to upgrades and support.

Support Personal Devices in Your Enterprise Deployment

With the consumerization of mobility, many enterprises are turning to Bring Your Own Device (BYOD) programs, or a hybrid approach including deployed corporate-owned devices and a BYOD program. By enabling a BYOD program, or taking a hybrid approach, enterprises allow employees access to corporate resources from anywhere, increasing productivity and driving employee satisfaction. Securing employee-owned devices and supporting different mobile platforms, however, can create complex issues for IT departments.

AirWatch supports Bring Your Own Device (BYOD) programs by enabling unprecedented device choice and supporting the device ownership models you choose without compromising the security and management of your mobile fleet. AirWatch provides a flexible model for asset management, policy enforcement, and distributing profiles, apps and content, based on device ownership type.



Device Choice

AirWatch supports all major mobile platforms, allowing you to implement a flexible BYOD program. Your employees can choose from the latest makes and models for their smartphones, tablets and laptops. Define devices eligible for enrollment with custom device whitelists and blacklists.

Access to Corporate Resources

AirWatch's simple enrollment process provides a consistent agent-based flow for major platforms. Once users are authenticated, profiles, applications and content are configured automatically based on the user and device ownership type. AirWatch enables secure access to enterprise resources from employee-owned devices. Provide employees connections to intranet sites and corporate content, apps, Wi-Fi, VPN networks and more from their mobile devices by pushing profiles automatically or on-demand. AirWatch also empowers your employees and reduces the burden on IT with our self-service portal. From the portal, employees can enroll additional devices, view detailed device information and perform remote actions.



Privacy Concerns

AirWatch enables companies to separate corporate and personal data on devices through customizable privacy policies that can be based on device ownership type. Configure policies to prevent data collection from personal email, content or applications on an employee-owned device. GPS location, personal user information and telecom data can also remain private, and employee-owned devices can be protected from a full device wipe or remote control. AirWatch also allows businesses to mitigate risks that are presented when employee-owned devices are

accessing corporate resources. With custom Terms of Use (TOU) agreements based on user role, organization group and device platform, users can be informed about data that will be captured and what they are allowed to do with the device.

Security and Compliance

Corporations need to enable BYOD without sacrificing the security needs of IT. With [AirWatch Workspace](#), provide enterprise-grade security for corporate resources and applications that are delivered to a device while preserving the separation of corporate and personal data. Create enrollment restrictions to limit the number of specific device types to ensure uniformity. Compartmentalize and manage enterprise applications and data without having to manage the entire device. AirWatch container solutions are designed to work together to deliver a seamless user experience with single sign on capabilities and cross-container integration. Provide enterprise-grade security for your applications with user authentication, data encryption, app-level policies, compliance monitoring and management.



Removing Corporate Resources

Administrators can remove access to corporate email, Wi-Fi and VPN when an end user un-enrolls or leaves the company. Remove internal apps and corporate content from devices upon

end user departure. Finally, perform an enterprise wipe without affecting personal content on the device.