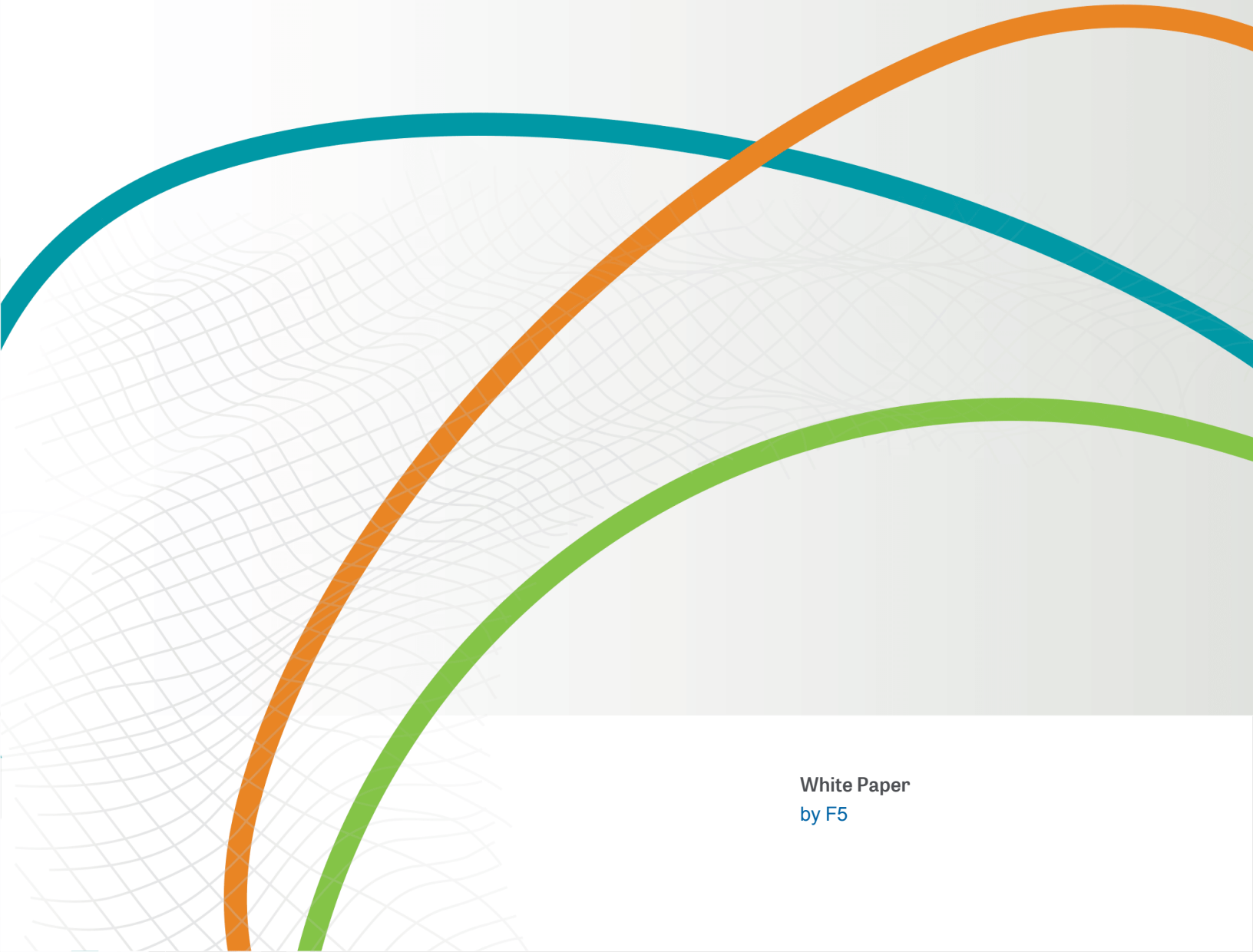
Access Control in a Mobile World

Enterprises are granting expanded access to corporate resources—wherever users are, and whatever the device. With an integrated F5 and VMware solution, you can scale, manage, secure, and optimize anytime, anywhere access to your network, cloud, and applications.



White Paper

by F5

Introduction

Enterprises today need their workforces to be mobile, agile, and flexible—able to work anywhere and at any time. To enhance efficiency, achieve business goals, and remain competitive, organizations are allowing increased access by authorized users to corporate applications and resources, wherever they may reside.

Enterprises deploy AirWatch by VMware enterprise mobility management (EMM) solutions to help them manage their growing number of devices, including remote desktops, laptops, smartphones, tablets, and soon even wearables. Through a simple, centralized administrative console, organizations can authenticate devices and users, configure and update settings, and secure and manage a wide variety of mobile devices. But in this world of anytime, anywhere, any device access, organizations need even more control over the data flowing to and from corporate networks, clouds, and other sources. The F5 Enterprise Mobility Gateway (EMG) solution for AirWatch by VMware offers that control and more through granular, context-aware policies that differentiate access to applications housed on the network, in a cloud, on the web, and in virtualized environments.

The F5 EMG solution for AirWatch by VMware consolidates and manages application access and security through F5® BIG-IP® Access Policy Manager® (APM). BIG-IP APM integrates with AirWatch by VMware to enable flexibility and granularity in the creation and enforcement of corporate access policies for mobile users and their devices, as well as access to and use of mobile and cloud-based applications. Through granular, context-aware policies, the solution enables you to safeguard sensitive corporate data and personal information while providing seamless access for users. You can also protect your networks, cloud, applications, and resources while securing user devices and access; ensure security compliance; and predict and mitigate threats—all while increasing employee usability and productivity, and decreasing cost.

The Challenges of Delivering Comprehensive Application Access

The benefits of enhanced workforce mobility are clear: increased efficiency, productivity, responsiveness, and business agility. However, as organizations expand access, they face serious security and management challenges that must be addressed to ensure continued growth and agility, and eliminate potential security issues before they compromise network, cloud, or application integrity; sensitive corporate or user personal data; and even an enterprise's reputation.

Mobility is more than "mobile devices"

Mobility is no longer just about managing devices like an employee's smartphone and tablet, or how their devices access an in-house network. Mobility now entails securing, managing, and controlling fast access to and flow of corporate data to and from multiple authorized (and, sometimes, unauthorized) users and their devices. And these users are connecting to networks, clouds, applications, and sensitive resources and data from multiple types of devices, over multiple access networks, to and from enterprise applications and resources, scattered throughout multiple environments, all over the world. Delivering a high level of secure, granular access while addressing so many different parameters is a daunting task—and an EMM solution alone is not enough.

Overburdening the IT department

Responding to the evolving requirements of controlling and managing mobility and mobile access is far from the only challenge confronting organizations. The size, complexity, and cost of network infrastructure are also growing at an incredibly accelerated rate. Today, it seems that every new enterprise application requires the deployment of another new access gateway, a costly, time-consuming process that requires ongoing IT attention, and management and maintenance—and that involves the potential for human error. Moreover, security holes can result when different access gateways have conflicting policies—or gaps in security coverage—without the overall visibility necessary to ensure cohesive access control and security.

To keep pace, organizations need new, robust, flexible, and scalable ways to effectively secure, manage, and control data and information flow between their corporate resources and their mobile workforce. They need to ensure fast, secure application and resource access, in addition to protecting and managing devices, apps, and data. What today's organization needs is a comprehensive mobile security and access platform.

Simplifying and Securing Mobility

The F5 Enterprise Mobility Gateway solution for AirWatch by VMware combines the market-leading core components of AirWatch by VMware, EMM, and mobile security with network-level, granular, secure, contextual identity and access management from BIG-IP APM. This combined solution enables organizations to leverage the critical mobile user and device data collected by AirWatch by VMware—such as who users are, what groups they belong to, how they authenticate, and what resources they are authorized to access. It then incorporates the type and security status of user devices, user location, environment at the time of access, and other parameters, as well as their method of access into a context-aware policy that's powered by BIG-IP APM.

BIG-IP APM helps enterprises develop and enforce specific policies for network, cloud, application, and data access and security—based on data gathered by both BIG-IP APM and AirWatch by VMware. This empowers organizations by enabling greater flexibility and granularity in the creation and enforcement of corporate access policies for mobility, while delivering a seamless user experience.

With the integration of F5 and AirWatch by VMware technology, enterprises can deploy a full-featured, comprehensive, integrated EMG solution in an easy-to-manage, highly scalable gateway, with a simplified user and administrator experience—helping them secure today's perimeter-less network.

Contextual access control

The F5 EMG solution for AirWatch by VMware makes it faster and easier for organizations to achieve granular control over mobile user access and connectivity, based on the context of the user and their device, location, access attempt, and what they are trying to access. The advanced Visual Policy Editor (VPE), which is a standard part of BIG-IP APM, simplifies the creation, editing, and management of access policies, and can easily integrate the granular mobile device data gathered by AirWatch by VMware. This data—as well as the data collected by BIG-IP APM—enables specific actions, such as quarantining, based on specific device configuration, for example, enabled passcode, enabled data protection or encryption, required or disallowed apps, or network roaming.

AirWatch by VMware delivers:

- Mobile device management
- Mobile content management
- Mobile application management
- Mobile email management
- Secure mobile browsing
- Workspace containerization

F5 BIG-IP APM delivers:

- Per-app VPN
- Secure remote and mobile access, via SSL VPN
- ActiveSync and other proxy services
- Access policy management and granular access control
    - Contextual policies based on user, device type and posture, location, and more
- Application access management
- Federated identity and single sign-on (SSO)

A vulnerability of traditional EMM solutions is that packet inspection only occurs at the inception of the connection. With the F5 EMG solution for AirWatch by VMware, enterprises can assess contextual security and access policies on a session-by-session basis—not just at the start of a connection—improving data security and helping prevent malicious attacks. Since devices and their users are mobile, context—and therefore, access to networks, clouds, applications, and data—can change due to the user's location, time, and other factors. By incorporating the user and device data collected by AirWatch by VMware, BIG-IP APM enables seamless, secure access, differentiated by very granular context, to any corporate resource or sensitive application and data, wherever it may reside.

And because of the integration of F5 and AirWatch by VMware technology, a user may be provisioned VPN access automatically, differentiated by their identity, device type, device security, location, and more, because of data gathered by BIG-IP APM and AirWatch by VMware, and applied to context-aware policies. The F5 BIG-IP® Edge Client®, which initiates the secure, encrypted VPN tunnel, is automatically deployed to a user's device as part of the AirWatch by VMware provisioning sequence. Once a user attempts to access a network secured by BIG-IP APM as the VPN termination point; or to access a mobile, cloud, or web-based application that has been identified by the enterprise as necessitating per-app VPN access; or policy determines that access to only VDI applications is required, access is seamless, and requires no user intervention. So, there is no need to launch a separate client or app. There is no reason to interrupt or alter the user's experience, which is critical in a mobile environment. Instead, the solution delivers seamless, secure, no-touch VPN access, differentiated by user, application, and access context—automatically.

Better performance, stronger security

Mobile devices are just that: mobile. So, mobile users must be able to connect effectively and quickly from anywhere, at any time. In the F5 EMG solution for AirWatch by VMware, BIG-IP APM delivers a layer 3 to layer 7 VPN termination point, with the BIG-IP Edge Client serving as the starting point. It supports many different mobile and desktop access use cases, including complete device VPN access, per-app VPN access, virtual desktop interface (VDI) access, unified portal access, Microsoft Exchange access, or simple Internet access.

This flexibility helps organizations differentiate access based on the user's identity, device, location, and context, and the applications and data to which they are requesting access—as well as combinations of these variables—further protecting sensitive corporate and personal user information, and critical resources, wherever they reside. And, unlike traditional mobile gateway technologies, the F5 EMG solution for AirWatch by VMware scales exponentially, quickly and seamlessly—delivering the performance that today's organizations require, especially in the face of ever-increasing demand.

Advanced authentication bridging

The F5 EMG solution for AirWatch by VMware is more than just a traditional mobile access gateway. Organizations now require advanced authentication, federated identity, and single sign-on (SSO). Through the integration of F5 and AirWatch by VMware technology, organizations can build an identity bridge, enabling their users to securely leverage their identity and authentication across an array of applications—on premises, in the cloud, or on the web—simplifying and enhancing the user experience and increasing employee satisfaction and usability.

At the same time, the F5 EMG solution for AirWatch by VMware supports and enables the use of various forms and strengths of authentication based on the granular context of the user, their device, location, and the applications and data they wish to access. With a robust set of application management and security tools—integrated with mobile applications—organizations can seamlessly deliver authenticated, authorized application access to all users.

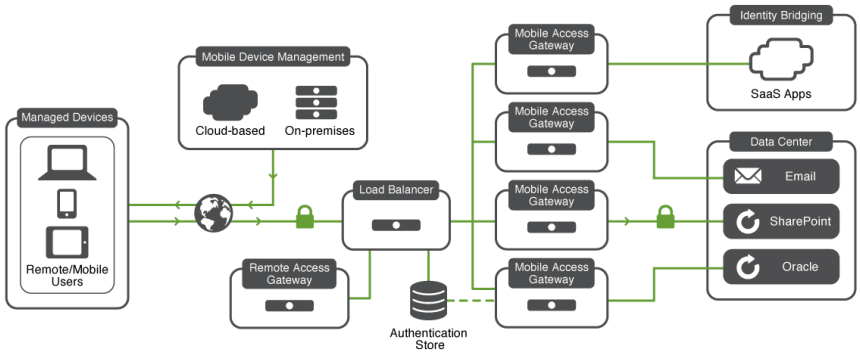


Figure 1: Network infrastructure is growing in size and complexity.

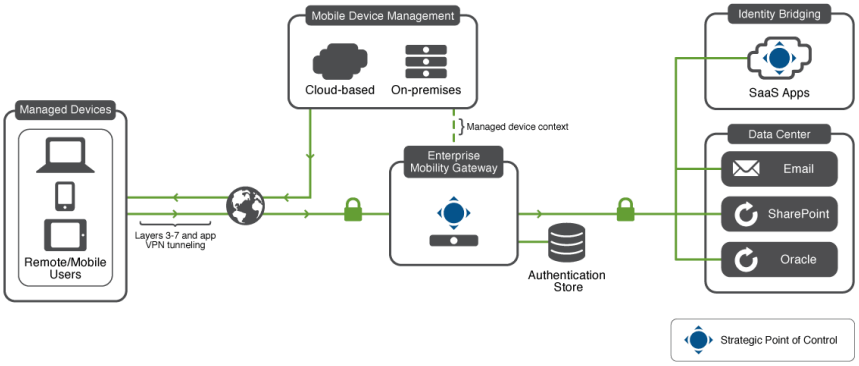


Figure 2: Integrate and optimize your enterprise applications with the F5 EMG solution for AirWatch by VMware.

When organizations deploy the F5 EMG solution for AirWatch by VMware, they will realize the many benefits of simplified access, enhanced security, and consolidated infrastructure. They will:

- Enable secure, seamless user access to all web-based resources.
- Implement comprehensive, layered, end-to-end security, from the mobile device through the network, cloud, and applications.
- Speed deployment and improve usability with no-touch, differentiated VPN configuration, and per-app VPN.
- Scale anytime, anywhere access control quickly, simply, and exponentially, while supporting 2x–5x more device connections than mobile and traditional access gateways.
- Centralize visibility and control, ensuring compliance with secure enterprise network, cloud, application and data access.
- Streamline management and cut costs by decreasing the number of access gateways to be purchased, deployed, managed, and maintained.
- Dramatically reduce CapEx and OpEx, while increasing user productivity and decreasing support calls and costs.
- Enhance and ease the rollout of mobile apps.
- Optimize services, including high-availability, high-performance SSL, complex and legacy authN schema integration, and enhanced Microsoft ActiveSync support.
- Simplify and speed integration of mobile VDI.
- Reduce costs by leveraging existing authentication and critical application systems.
- Reduce support calls for enterprise IT and help desk teams.
- Increase employee satisfaction and productivity with a seamless user experience.

Conclusion

A complete enterprise mobility gateway solution empowers organizations to grant the secure, controlled, anytime, anywhere access their users and business demand, while ensuring corporate compliance and the security and integrity of their network, cloud, applications, and data. The F5 EMG solution for AirWatch by VMware is a platform that provides broad visibility across corporate resources, and allows enterprises to manage access to those resources wherever they reside. In addition, enterprises can heighten security for sensitive corporate and personal data, and enable seamless, granular access based on context. The solution allows organizations to protect, control, and manage access to their network, clouds, applications, and data—for all devices, from any location, over any network, at any time.

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 www.f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com