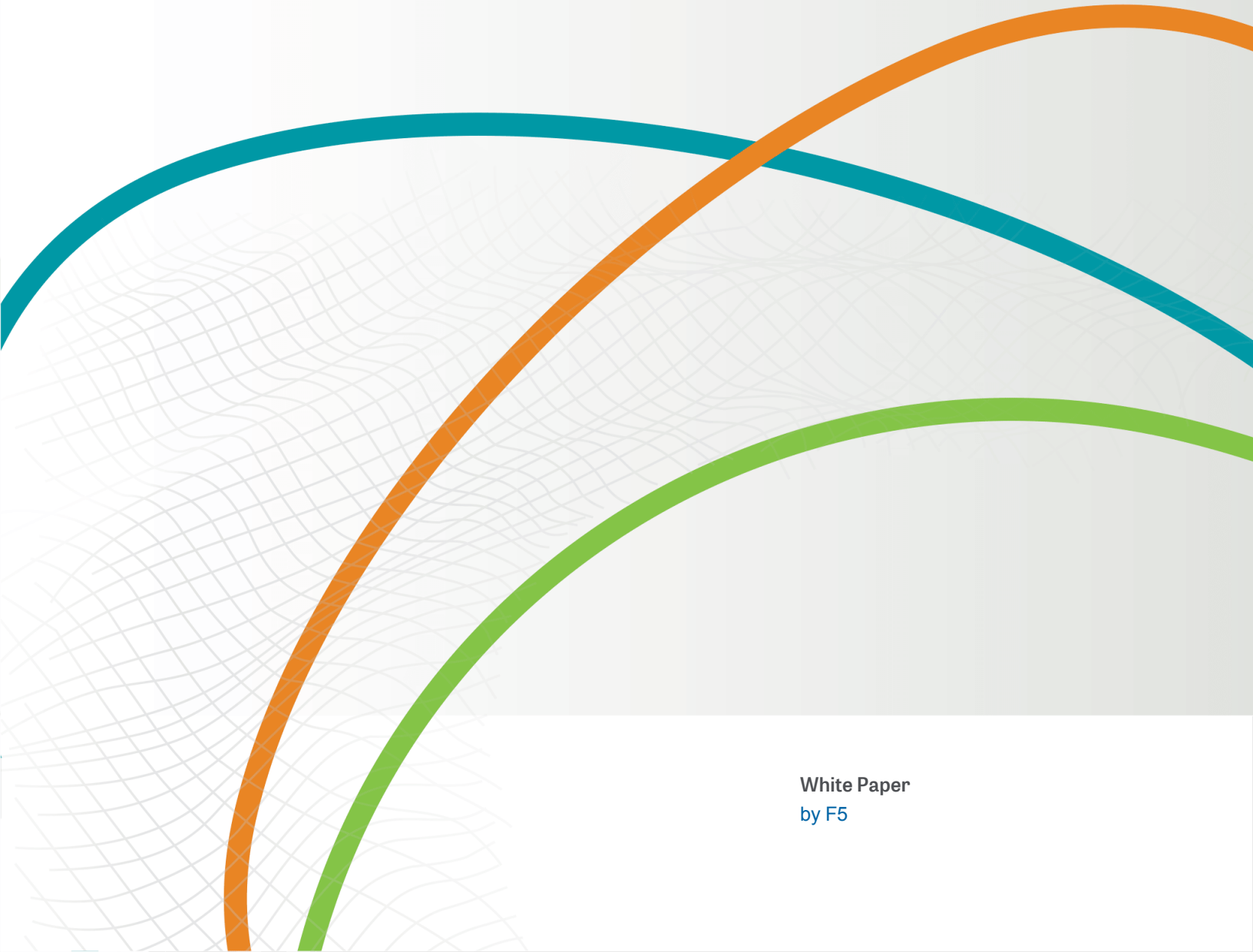
Deploying an Enterprise Mobility Gateway

More enterprises are granting greater access to corporate resources—wherever they may be located—for authorized users through an ever-increasing number of mobile devices. An Enterprise Mobility Gateway helps organizations scale, manage, secure, optimize, and control today's required anytime, anywhere network, cloud, and application access.



White Paper

by F5

Introduction

Enterprises 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.

With the proliferation of users employing a growing number of devices—remote desktops, laptops, smartphones, phablets, tablets, and even wearables—to access corporate resources and be productive, an organization's enterprise access management solution must deliver comprehensive security, contextual management, granular control, and extensible scalability. It doesn't matter whether the enterprise applications and resources are located on the network, in the cloud, or on the web—or whether the users requesting access are employees, contractors, partners, or guests. Organizations must deliver anytime, anywhere application and resource access to authenticated, authorized users— and, even at times, unauthenticated and unauthorized users, such as guests—that is fast, simple, secure, and differentiated.

The F5® Enterprise Mobility Gateway (EMG) solution gives organizations visibility into access by all users and empowers organizations to take control of and manage seamless, anytime, anywhere, any device access for all users. In addition, the solution allows organizations to safeguard sensitive corporate data and personal information; protect their networks, applications, and resources; ensure security compliance; and predict and mitigate threats.

Managing Workforce Mobility

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 eliminate potential security issues before they compromise the integrity of the network, its applications, and data, as well as the enterprise and even its reputation.

Mobility means more than "mobile devices"

Until recently, when enterprises addressed "mobility," they were mostly concerned with the exploding number of mobile devices—corporate-owned and personal—requesting access, attempting to access, and even accessing (many times without appropriate permissions) corporate networks, clouds, and resources. They needed to manage their employees' devices and their access to corporate resources from these smartphones and tablets. Now, however, enterprise mobility is truly multifaceted, with even more types of devices, more varied categories of users demanding access, more networks and methods of access, and more diverse locations of apps and network resources.

In other words, mobility is no longer just about managing an employee's smartphone or tablet and how it accesses an in-house network. Instead, mobility entails securing, managing, and controlling the fast access to and flow of corporate data to and from multiple authorized (and, sometimes, unauthorized) users. And these users are connecting via multiple types of devices, over multiple access networks, to and from enterprise applications and resources, scattered throughout multiple environments, all over the world. It's a daunting task.

Enterprise mobility is much more than BYOD. Mobile devices have been designed for use anywhere, and at any time—in the corporate offices tethered wired or wirelessly to the network, or on the road, over any Wi-Fi network, from any location, worldwide. This brings an increasing number of challenges for enterprises supporting a seemingly ever-expanding number of mobile, remote, and local access use cases.

Overburdening the IT department

Responding to the evolving requirements of controlling and managing mobility and mobile access is not the only challenge confronting organizations. The size, complexity, and cost of network infrastructure are also growing at an 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 management and maintenance, and 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 security.

Organizations need a new, robust, flexible, and scalable way to effectively secure, manage, and control data and information flow between their corporate resources and their mobile workforce. They need to provide for application and resource access, in addition to securing and managing devices, apps, and data. This complex issue requires more than mobile device management (MDM), mobile application management (MAM), or even enterprise mobility management (EMM). What today's enterprises need is a comprehensive, mobile security and access platform.

Simplifying and Securing Mobility

An enterprise mobility gateway (EMG) solution combines the core components of existing mobile management—MDM, MAM, mobile content management, and more—and mobile security, with granular, secure, contextual identity and access management at the network level. An EMG solution enables organizations to understand critical data, such as who the user is, what groups they belong to, how they authenticate, and what resources they are authorized to access. It understands and incorporates the type and security status of their device, and takes into account their location and environment at the time of access, as well as their method of access. Finally, an EMG solution develops and enforces specific policies for network, application, and data access and security—based on the information gathered.

F5 delivers a full-featured, comprehensive, integrated EMG solution in an easy-to-manage gateway, with a seamless, simplified user and administrator experience, helping organizations secure today's perimeter-less network.

Contextual access control

The F5 EMG solution makes it faster and easier for organizations to achieve granular control over user access and connectivity, based on the context of the user and their device. By integrating the mobile device attributes captured by EMM applications with contextual information—such as user identity, group, role, device type and security posture, user and/or device location, and much more—organizations can deliver comprehensive, flexible, and secure access control at the device, network, application, and data levels.

In addition, enterprises can assess contextual policies on a session-by-session basis—not just at the inception of the connection—improving data security and helping prevent malicious attacks. Since devices and their users are mobile, context—and therefore, access to networks, applications, and data— can change due to location, time, and other factors. F5 partners closely with leading EMM vendors so they can leverage its full-featured gateway. F5 also integrates user and device data collected by the EMM products to enable seamless, secure access, differentiated by very granular context, to any corporate resource, wherever it resides.

Better performance, stronger security

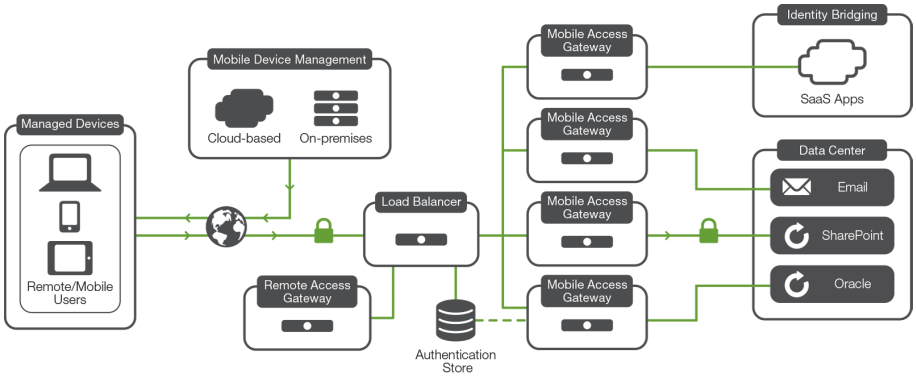
Mobile devices are just that: mobile. So, mobile users need to be able to connect effectively and quickly from anywhere, anytime. The F5 EMG solution is an L3–L7 VPN termination point, delivering full device VPN access. However, it also supports many different mobile and desktop access use cases, including complete VPN access, per-app VPN access, virtual desktop interface (VDI) access, or simple Internet access. This flexibility helps organizations differentiate access based on granular context, further protecting corporate data and applications, as well as personal user information.

This full-featured EMG solution helps enterprises ensure the security of their applications and sensitive data, no matter where they reside—on a network, in the cloud, or on the web. And, unlike traditional mobile gateway technologies, the F5 EMG solution scales quickly and seamlessly—delivering the performance that organizations require, even in the face of ever-increasing demand.

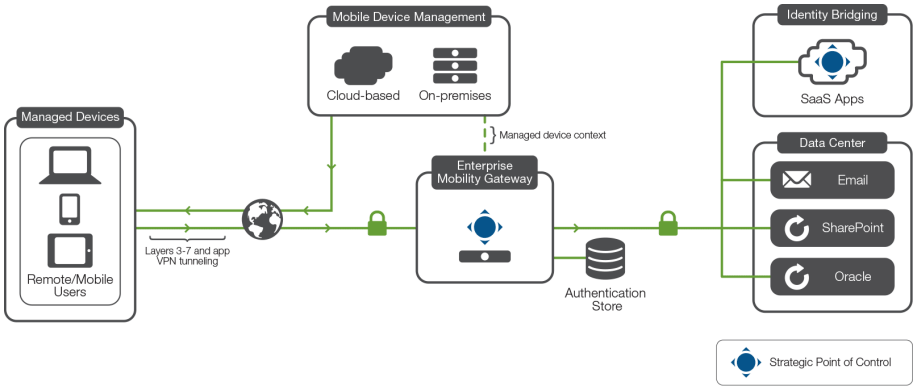
Advanced authentication bridging

However, the F5 EMG solution is more than just a traditional mobile access gateway. Today's organizations need advanced authentication, federated identity, and single sign-on (SSO), and the F5 EMG solution works effortlessly and securely with most authentication means and methods. The F5 EMG solution builds an identity bridge, enabling users to securely leverage their authentication across an array of applications, on premises, in the cloud, or on the web, simplifying and enhancing their user experience.

At the same time, it supports and enables the use of various forms and strengths of authentication based on the granular context of the user, their device, and the data they wish to access. With a robust set of application management and security tools—integrated with mobile applications, organizations can deliver authenticated, authorized application access for all users, wherever corporate resources are located.



The growing size and complexity of network infrastructure.



Integrate and optimize your enterprise applications with the F5 EMG solution.

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

- Deliver secure, seamless user access to all web-based resources.
- Speed deployment with no-touch VPN configuration and per-app VPN.
- Scale anytime, anywhere access control quickly, simply, and exponentially, while supporting 2–5x more devices than mobile and traditional access gateways.
- Centralize visibility and control in one place, 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.
- Effectively manage email, web and mobile apps, and ERP access.
- Easily support and integrate with other mobile or desktop access capabilities, such as VDI.
- Simplify and speed integration of mobile VDI.

- Reduce costs by leveraging existing authentication, LDAP, and critical application systems.
- Reduce support calls for enterprise IT and help-desk teams.

Conclusion

A robust Enterprise Mobility Gateway solution empowers organizations to grant the controlled anytime, anywhere access their users and business demand, while continuing to ensure corporate compliance and the security of their network. The F5 EMG solution delivers a platform that allows enterprises to have broad visibility across and manage access to corporate resources wherever they reside; heighten security for sensitive corporate and personal data; enable differentiated, granular access based on context, including user, device, location, use case and more. In addition, the F5 EMG solution allows an organization to optimize the performance of, while protecting, controlling, and managing access to its network, its cloud, and its applications—and particularly its data—for all devices, from any location, at anytime, and over any network.

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