TEN PRIORITIES FOR ENABLING SECURE ACCESS TO ENTERPRISE IT SERVICES

EMA Top 3 Report and Decision Guide for Enterprise

ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) REPORT
ABRIDGED VERSION COMPLIMENTS OF F5
Written by Steve Brasen

Q3 2018

CONTENTS

INTRODUCTION

Enterprise productivity, profitability, and success in meeting business objectives are dependent on the ability of workforces to access and utilize the applications, data, email, and other IT services necessary to complete job tasks. However, increased pressure to enable workforce mobility and the distribution of IT services across a variety of public and private hosting environments have challenged organizations to grant secure and reliable access to those resources. This Enterprise Management Associates (EMA) decision guide is intended to provide actionable advice on the best practices and solutions organizations should adopt to empower end-user productivity while minimizing risk profiles.

Why You Should Read This Research Report

IT Managers, Security Officers, and Line of Business Managers will gain key insights into the following areas:

- Understand the end-user computing forces that are shaping today's workforce performance
- Identify the most important considerations for adopting best practices and solutions for enabling secure access to business IT services
- Determine the TOP 3 platforms available today for each recommendation

Research Methodology

All research results in this report are based on EMA's survey of 200 randomly-selected North American enterprises with 100 or more employees across a wide-range of industry verticals. For each of the top ten priorities identified by survey respondents, EMA established evaluation criteria and identified a list of vendors offering viable solutions. The vendors EMA determined to provide outstanding solutions were approached to supply detailed information on solution capabilities. The selection of leading solutions followed a careful examination of how well each solution met the established evaluation criteria and reflects EMA's opinions of what constitutes an innovative and comprehensive approach to secure access enablement.

200 ENTERPRISES SURVEYED

97% ADOPTED MANAGEMENT SOLUTIONS TO ENABLE SECURE ACCESS

10 KEY TRENDS IDENTIFIED

EMA TOP 3:

EMA PRESENTS IT TOP 3 AWARD TO VENDORS THAT ARE BEST ALIGNED WITH TODAY'S CUSTOMER PRIORITIES AND PAIN POINTS

EMA TOP 3

2018 TOP PRIORITIES FOR SECURE ACCESS ENABLEMENT

- Unifying Access Control Across Hybrid IT Ecosystems
- Providing Secure Access to Web Services
- Enabling Secure Remote Access to Business Networks
- Orchestrating Digital Workspaces
- Reducing End-User Friction with Single Sign-On
- Simplifying Application Deployment/Installation
- Facilitating Secure Data Sharing
- Network Access Control with IoT Enablement
- Enabling Privileged Access Management
- Supporting "Bring Your Own Device" Initiatives

EMA

WHAT ARE THE EMA TOP 3 REPORTS?

EMA Top 3 reports identify the leading priorities organizations face with resolving challenges and meeting enterprise requirements in particular IT management focus areas. The intent of this report is to inform and inspire influencers and decision makers in their project planning and vendor selection process.

While EMA internally conducted a detailed analysis of solutions that help support the identified IT management priorities, this report is not designed to provide a feature-by-feature comparison. In certain cases, EMA recognized products for their innovative approach rather than their ability to meet a predetermined checklist of features. Additionally, some popularly adopted approaches may not be represented in this report because EMA's analysis did not indicate that they fully address emerging market requirements. This guide was developed as a resource for organizations to gain insights from EMA's extensive experience conducting hundreds of product briefings, case studies, and demonstrations.

Solution Qualifications

In order for a product to be considered for recognition as an EMA Top 3 secure access enablement solution, all evaluated features and capabilities were required to conform to the following rules:

- Reported features must be generally available on or before May 31, 2018. Features that are in beta testing or are scheduled for inclusion in later releases do not qualify.

- Reported features must be self-contained within the included package sets. Any features that are not natively included in the evaluated package sets, but available separately from the same vendor or a third-party vendor, do not qualify (except where explicitly noted as points of integration).

- Reported features must be clearly documented in publicly-available resources (such as user manuals or technical papers) to confirm their existence and ensure they are officially supported.

> **THE EMA TOP 3 REPORT GETS ITS CREDIBILITY FROM ITS EMPIRICAL FOUNDATION. IT PROVIDES ME WITH INSIGHTS ON WHICH VENDORS I MIGHT WANT TO LOOK AT, WITHOUT CLAIMING TO KNOW WHAT I SHOULD BUY.**
>
> – Director, Application Platforms, Large University

How to Use This Document

It is important to recognize that every organization is different, with a unique set of IT and business requirements. As such, EMA strongly recommends that each organization conduct its own market evaluation to identify solutions that will best match its business needs. This guide will assist with the process by providing information on key considerations to review during the selection process, as well as a short list of vendors that offer solutions to meet particular requirements.

For each priority identified by surveyed organizations, EMA provides the following sections offering insights for use in the platform selection process:

- **Requirements and Challenges** – These are the primary drivers for prioritizing particular IT capabilities. If these resonate with your own organization's needs, then corresponding solutions are recommended for adoption.

- **Supporting Technologies** – This identifies the most common and emerging types of solutions that are designed to address each particular secure access priority. It is important to note that many of these technologies may solve the same problem in radically different ways. However, being aware of the different approaches will help organizations determine the type of solution that will best meet its unique requirements.

- **Key Considerations for Adopting a Solution** – As each organization builds its own list of product evaluation requirements, these lists will provide suggestions for architectures, features, and integrations that should be considered before adopting a solution to meet the targeted priority. These considerations also provide an indication of the requirements EMA utilized in its identification of Top 3 vendors.

- **Top 3 Solution Providers** – By identifying and recognizing the most innovative vendor solutions that address the greatest business priorities for secure access enablement, the table in this section provides a brief overview of each platform and respective capabilities. The solutions are listed alphabetically by vendor, so the order in which they appear is not an indication of EMA's preference. It is highly recommended that organizations seeking to adopt solutions addressing a particular priority investigate each of the corresponding Top 3 vendors to determine which best meet their unique requirements.

UNDERSTANDING SECURE ACCESS

Evolving Challenges for Enabling Secure Access

A decade ago, enabling secure access to enterprise applications, data, and other IT services was relatively uncomplicated. Most business IT services were hosted on enterprise-controlled servers safely located behind secure firewalls that also protected the endpoint devices (principally Windows PCs) accessing them. Two revolutionary technological changes occurred almost simultaneously, however, to dramatically shift how enterprise users access and utilize IT resources. The first was accelerated requirements for supporting workforce mobility. Certainly the rapid adoption and use of mobile devices to perform business tasks was a key driver for this, but equally disruptive was an increase in telecommuting, outsourcing, and other conditions requiring remote access to business services.

The second substantial change in end-user computing emerged from the relatively sudden introduction and rapid adoption of cloud-hosted services. No longer were business applications, data, email, and other IT services securely protected behind a company firewall, but rather have become distributed across private clouds, private servers, platform as a service (PaaS) environments, infrastructure as a service (IaaS) environments, and software as a service (SaaS) resources. In fact, hybrid applications arose that include components (i.e., software subsystems such as a database or data collection service) that are hosted on more than one of these environments. Access must be controlled to all of these environments in order to achieve security and compliance objectives.

TOGETHER, EMERGING REQUIREMENTS FOR WORKFORCE MOBILITY AND DISTRIBUTED IT SERVICES HAVE RESULTED IN SIGNIFICANT CHALLENGES FOR ENABLING SECURE ACCESS.

Reconciling Security and Access Requirements

Together, emerging requirements for workforce mobility and distributed IT services have resulted in significant challenges for enabling secure access. Security and access are actually diametrically opposed forces—the more you enable one, the more you limit the other. However, IT operations and security managers are now constantly pressured to provide both simultaneously. Users require immediate and low-friction access in order to complete the essential job tasks that drive business performance, profitability, and operational goals. Further, users should not have to "jump through hoops" just to access the resources necessary to their function. At the same time, security requirements have never been more paramount. One need only pick up a newspaper (or the digital equivalent) to read about the latest major breach that devastated the reputation of a popular business or institution that would otherwise have been accepted as providing highly secured services. Failure to prevent security breaches can result in identity fraud, a loss of customers and profitability, and an inability to meet regulatory commitments, as well as fines, lawsuit payments, and other compensation to affected customers.

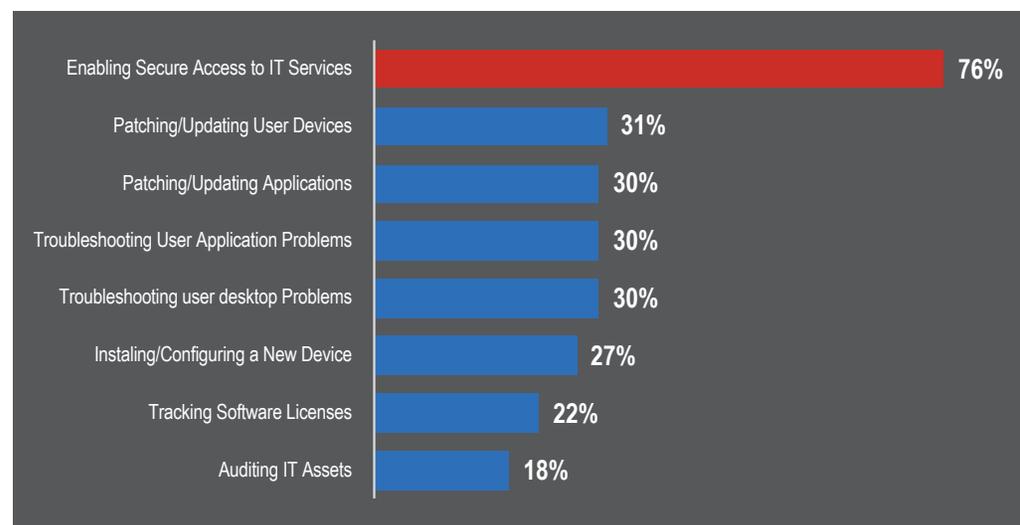| Endpoint management process	Percent
Enabling Secure Access to IT Services	76%
Patching/Updating User Devices	31%
Patching/Updating Applications	30%
Troubleshooting User Application Problems	30%
Troubleshooting user desktop Problems	30%
Instaling/Configuring a New Device	27%
Tracking Software Licenses	22%
Auditing IT Assets	18%

Figure 1: Percent of survey respondents indicating endpoint management processes that are critical to their business

UNDERSTANDING SECURE ACCESS

Key Disrupting Technologies for Enabling Secure Access

Fortunately, it is actually possible to satisfy both security and access requirements simultaneously, but it requires the adoption of innovative solutions that provide user-focused, secure access to distributed IT services. Crucial technologies that were introduced to address both sides of the equation include:

- **Context-Aware Analytics –** The level of risk associated with an access request is dependent on the context of the endpoint and user issuing it. For instance, a user requesting access from a mobile device in use at a public coffee shop would likely be considered a higher risk than a user employing a desktop PC direct connected to a local-area network inside the physical office facilities. Analytics can be utilized to assign risk levels to access authorizations so that predetermined policies can be applied based on the context of the connection request.

- **Digital Workspaces** – Solutions that host applications, data, and other IT resources that are aggregated from a centralized service catalog greatly improve user experiences. In this way, digital workspaces enable access to a consistent set of IT resources available on any user device and configurable to user preferences.

- **Browser Isolation** – To address increasing requirements to support secure access to SaaS and web applications, browser isolation solutions were introduced that essentially sandbox web connections and use virtualization or containerization technology to display browser activities on the endpoints.

- **Identity Management** – Fundamental to enabling secure access to business services is the ability to positively identify the end users and devices that are issuing the requests. Innovative technologies for enabling identity management include physical biometrics, behavioral analysis, hardware and software tokens, and device footprinting.

- **Network Access Control (NAC)** – NAC solutions were designed to support a "comply to connect" policy to assure that only known users and devices would be allowed in a corporate network, both wired and wireless. The technology progressed to also handle guest management and the influx for personal and corporate-issued devices. The most current evolutions addressed the discovery, monitoring and management of unknown and IOT devices as well as offering enhanced interoperability to facilitate the sharing of identity and endpoint configurations and security states to external security systems and to enable other systems to invoke NAC threat response policies for network segmentation and blocking.

- **Secure Remote Access** – While many traditional virtual proprietary network (VPN) solutions proved to exhibit a number of security risks and performance issues, new methods of secure remote access were introduced to resolve these challenges. Some examples of relevant technologies in this category include secure sockets layer (SSL) VPN, Internet Protocol Security (IPSec), layer 2 tunneling protocol (L2TP), secure shell (SSH) tunneling, and STunnel.

- **Unified Endpoint Management** – Combining functionality for client lifecycle management (i.e., PC management) with enterprise mobile management accessible from a single console interface, unified endpoint management solutions simplify processes for application distribution and device configuration across heterogeneous endpoint architectures.

OVERVIEW: TEN PRIORITIES FOR ENABLING SECURE ACCESS IN 2018

Based on responses from 200 enterprises, the following represent the top ten priorities for enabling secure access to enterprise IT resources (including applications, data, email, and other services) in 2018:

1 UNIFYING ACCESS CONTROL ACROSS HYBRID IT ECOSYSTEMS: As organizations increasingly introduce software services across internal and external cloud-, web-, virtual-, and server-hosted environments, the complexity of the access control ecosystem accelerates exponentially. Organizations require consolidated solutions that can manage and secure all of their IT-hosted services from a single interface.

2 PROVIDING SECURE ACCESS TO WEB SERVICES: While the increased adoption of HTML-based SaaS applications has served to reduce the cost and administration required for business productivity software, it has opened the door to new threats to endpoint security. Organizations dependent on web-hosted services to support business operations must ensure there is a logical separation between web browsers and websites to prevent malicious connection activities.

3 ENABLING SECURE REMOTE ACCESS TO BUSINESS NETWORKS: Remote workforces are more frequently requiring access to business applications, data, and services through the Internet and unsecured public networks, increasing business risk exposures. Private network tunneling solutions with hardened security features create intuitive and low-risk connections for workers to access essential IT resources on business networks.

4 ORCHESTRATING DIGITAL WORKSPACES: End-user productivity is greatly enhanced with the availability of a fully automated and centrally managed solution for creating user-defined abstracted workspaces that are accessible from any device at any location. Core to a digital workspace solution is the ability to provision web-hosted, virtual, and downloadable IT resources in a seamless and consistent manner, regardless of the user device employed.

5 REDUCING END-USER FRICTION WITH SINGLE SIGN-ON: As workforces increasingly rely on disparate IT services to perform job tasks, the complexity of initiating and maintaining authentication processes has intensified, reducing overall business productivity. Single sign-on (SSO) solutions minimize the friction of access requirements while enhancing security by establishing a common, hardened authentication process supporting numerous IT services.

6 SIMPLIFYING APPLICATION DISTRIBUTION AND INSTALLATION: Persistent user requests for applications and other software elements to be installed locally on their devices continue to plague IT administrators. Advanced application distribution platforms incorporate intelligent deployment processes that take into consideration device and user contextual information to enable reliable and secure software deployments.

7 FACILITATING SECURE DATA SHARING: As workforces increasingly create, access, and distribute business files and data across a variety of public and private IT services, organizations struggle to prevent the loss of sensitive information. Secure, enterprise-class data-loss prevention (DLP) solutions provide the centralized environment necessary to maintain control over the access and distribution of critical business data.

8 NETWORK ACCESS CONTROL WITH IOT ENABLEMENT: The growing diversity of network-attached devices is straining the ability of organizations to secure access to the breadth of resources on the Internet of Things (IoT). To enforce authentication and security policies to and from non-standard devices, network access control solutions have been introduced that operate at the network level, preventing system-level processes from being compromised.

9 ENABLING PRIVILEGED ACCESS MANAGEMENT: Although users sometimes require elevated access privileges to servers, applications, and their own endpoint device, organizations often fail to adequately govern those authorizations and how they are being used. Privileged Access Management (PAM) solutions provide features for authorizing, tracking, and automatically revoking administrator-level access privileges.

10 SUPPORTING BRING YOUR OWN DEVICE INITIATIVES: The consumerization of IT has resulted in the instruction of employee-owned devices that are now being used to perform business tasks. "Bring your own device" (BYOD) management solutions enable organizations to isolate and secure business resources on the endpoints without limiting a user's non-business use of the devices.

EMA

FOCUS ON:
PRIORITY #3—ENABLING SECURE REMOTE ACCESS TO BUSINESS NETWORKS

Quick Take

Remote workforces are more frequently requiring access to business applications, data, and services through the Internet and unsecured public networks, increasing business risk exposures. Private network tunneling solutions with hardened security features create intuitive and low-risk connections for workers to access essential IT resources on business networks.

Requirements and Challenges

There are two key aspects to supporting increasingly mobile workforces. The first (and most obvious) is extending access support to a variety of portable devices, including laptops, tablets, and smartphones. However, just as important is enabling the portability of the IT services themselves. For instance, telecommuters using a home desktop to perform job tasks require the same level of access as if they were at their desk in the office. Supporting workforce mobility is, therefore, principally about enabling secure access to business resources from any device at any location. In addition to supporting workforce mobility, organizations often must also enable remote access to branch offices, outsourced organizations, and service providers. Each of these types of access requirements proportionally increases the level of risk of a security breach. Malicious attackers do not even need to hack into vulnerable servers to compromise business security. They can just "sniff" the traffic off the public networks hosting the endpoints. Empowering mobile and remote workers with the ability to access the business resources necessary to perform job tasks requires network connections that operate over public networks, but are also ensured to be private and secure. However, any technology introduced to secure network connections must not impede service performance or substantially diminish user experiences.

Supporting Technologies

Enabling secure network access requires the introduction of a private network tunneling (or "port-forward") solution. Put simply, tunneling protocols encapsulate packet data and private network information so that they can be transmitted over a public network while covertly enabling access to a firm's local network. From an end-user's perspective, tunneling solutions provide the impression that their devices are connected directly to their company's local network, even though it is actually connected to remote networks, wireless networks, cellular networks, or the Internet. The most popular type of tunneling is a virtual private network (VPN). While all VPNs and other tunneling solutions are designed to enable access to business networks, only some types of solutions include layers of security to ensure connections remain private. One popular method employed to achieve this is to add a secure socket layer (SSL), which encrypts the data being transmitted so it is unreadable by anything other than the business network and the endpoints. Other types of secure network access solutions include IPSec, SSH tunneling, STunnel, and the Layer 2 Tunneling Protocol (L2TP).

Key Considerations for Adopting a Solution

- **Persistence of Secure Network Connections** – Depending on the use case, secure network connections are required to be always on (persistent) to enable high performance or established on-demand to enhance security. Additionally, secure connections may be enabled for all network activity from a device, or just network activity from specific applications. An ideal solution will have the flexibility to enable a variety of connections so they can be applied based on individual use cases, including supporting smooth roaming from remote access to local LAN access.

- **Context Awareness** – When initiating a remote connection, an enterprise-grade secure access solution should evaluate the risk of any device prior to and during a session, reducing the possibility of malware infiltration and increasing overall security and compliance. Endpoint device conditions such as physical and network location, running processes, installed applications, operating system version, patch levels, browser type, and any risky device states (e.g., the existence of malware or if the device has been rooted or jailbroken). Moreover, connection policies should automatically initiate the appropriate level of security required when establishing a remote connection.

- **Breadth of Supported Endpoints** – While most secure network solutions support Windows devices, the increased heterogeneity of enterprise endpoints now requires broader platform support in most organizations. This includes support for macOS, Linux, iOS, Android, and Chrome OS. Any adopted solution should support all devices used in an organization to prevent the need to adopt multiple secure network solutions. A single, unified client that supports common operating systems can further streamline deployments.

- **Onboarding Process** – All secure network approaches require the installation of software elements on the endpoints. Automated features to distribute this software can greatly simplify onboarding processes, especially if the organization needs to support a large number of endpoints. Alternatively, direct integration with third-party endpoint management platforms, application distribution solutions, and service catalogs can also simplify deployment processes.

- **Third-Party Integrations** – Direct integrations with third-party platforms simplifies management, enhances security, and improves connection performance. For instance, integrations with directory and authentication services (such as Active Directory, LDAP, SAML IdPs, Radius, etc.) can assist with identifying users and endpoints, authorizing connections, and establishing group policies. Integrations with third-party security and endpoint management platforms can help in enabling holistic reporting and consolidated policies that are context-aware. Additionally, direct integrations with specific applications allows secure connections to be established directly within the software. The availability of APIs are also essential to enable custom integrations with third-party solutions.

EMA™

FOCUS ON:
PRIORITY #3—ENABLING SECURE REMOTE ACCESS TO BUSINESS NETWORKS

EMA HAS IDENTIFIED F5 AS A TOP 3 SOLUTION PROVIDER FOR ENABLING SECURE REMOTE ACCESS TO BUSINESS NETWORKS IN 2018

PLATFORM: BIG-IP Access Policy Manager	**ARCHITECTURE:** Physical appliance

KEY FEATURES:

- F5's VPN client is offered for both desktop and mobile endpoints, and utilizes transport layer security (TLS) and datagram TLS to enable secure connections
- F5 supports the IPsec VPN, which is ideal for establishing connections between two fixed endpoints, such as two offices
- Provides native VDI proxy support for Citrix, Microsoft, and VMware on both desktop and mobile devices
- Access policy creation is simplified with the included graphical interface, Visual Policy Editor (VPE)

For more information, visit:

https://www.f5.com/

To contact F5:

Web: https://www.f5.com/products/get-f5

Email: info@f5.com

For access to the full version of this report, visit:

http://www.enterprisemanagement.com/research/asset.php/3642/EMA-Top-3-Report:-Ten-Priorities-for-Enabling-Secure-Access-to-Enterprise-IT-Services