# 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 CA TECHNOLOGIES**

Written by Steve Brasen

Q3 2018

EMA™

*IT & DATA MANAGEMENT RESEARCH • INDUSTRY ANALYSIS • CONSULTING*

# CONTENTS

Introduction ..... 3
What are the EMA Top 3 Reports? ..... 4
Understanding Secure Access ..... 5
Overview: Ten Priorities for Enabling Secure Access in 2018 ..... 7
Focus On: Priority #5—Reducing End-User Friction With Single Sign-On ..... 8


© 2018 Enterprise Management Associates, Inc.

# 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

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


## 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

**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


© 2018 Enterprise Management Associates, Inc.

# 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.


© 2018 Enterprise Management Associates, Inc.

# 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.

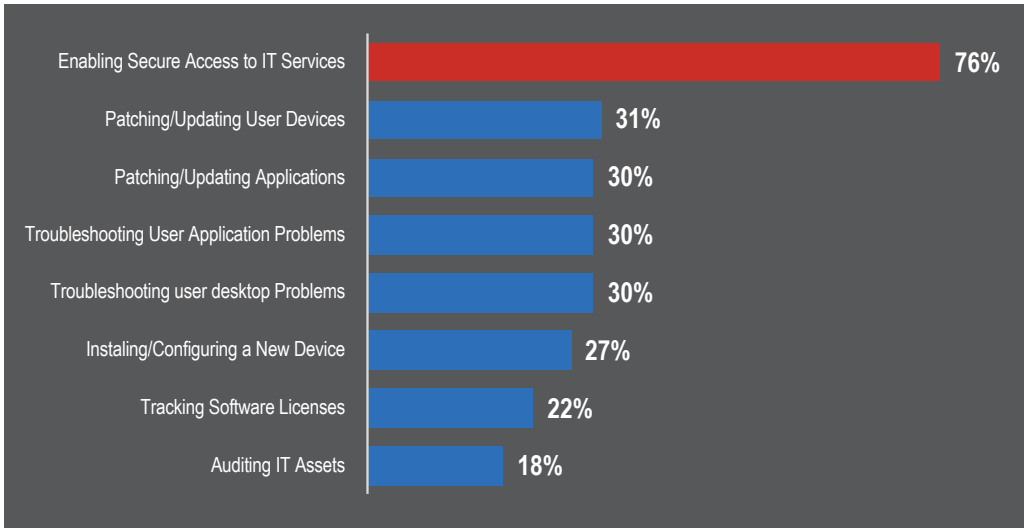


Figure 1: Percent of survey respondents indicating endpoint management processes that are critical to their business


© 2018 Enterprise Management Associates, Inc.

# 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.


© 2018 Enterprise Management Associates, Inc.

# 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.



© 2018 Enterprise Management Associates, Inc.

# FOCUS ON: PRIORITY #5—REDUCING END-USER FRICTION WITH SINGLE SIGN-ON

## Quick Take

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.

## Requirements and Challenges

Business productivity is dependent on the ease in which workers are able to access enterprise applications, data, and other IT services. "Friction" refers to the number of manual steps users must perform to access the resources they need to complete job tasks. In high-friction environments, users are continuously challenged with passwords and other authentication tests that severely diminish their productivity. According to EMA research, every time a user is distracted from completing a task in order to enter information necessary to access essential IT resources, it can take as much as 20 minutes for them to refocus their attention back to activity they needed to complete in the first place. This wasted time can rapidly add up over the course of a day as users require access to a variety of different IT resources (e.g., applications, email systems, and data repositories) distributed across a variety of hosting environment (e.g., private servers, public clouds, web services, and virtual instances). While strong security practices are essential for organizations to meet regulatory and business objectives, users should not have to "jump through hoops" just to access the IT resources they need to do their job.

## Supporting Technologies

The most basic method for reducing end-user friction is the introduction of an SSO solution that allows a single authentication process to be performed to gain access to multiple IT services. The basic philosophy is that once a user and/or device is authenticated to access one business IT service, it should not be necessary for them to immediately authenticate again to access a different IT service. Typically, SSO solutions operate by integrating with directory services (such as Active Directory, LDAP, or RADIUS), which are used to store a common set of credentials. Once authenticated, a token can be sent to relevant systems, applications, and services to authorize access for specific users or devices until the access times out or is otherwise revoked.

Another advantage to employing SSO is that it can actually increase overall security. Most individuals have a difficult time memorizing and maintaining numerous effective passwords necessary for accessing a number of disparate IT services. As a consequence, users often utilize the same password for multiple accounts, fail to use a strong password, rarely change passwords, and often forget passwords (substantially increasing access friction by introducing the password recovery processes). SSO substantially reduces this complexity by reducing access credentials to a single authentication process, which is much easier for fallible humans to maintain effectively. By extension, this also reduces the amount of support requests administrators receive from end users having difficulty performing password and other authentication tasks.

## Key Considerations for Adopting a Solution

- **Breadth of Supported Authentication Protocols** – Different applications and IT services support different authentication mechanisms, so the broader the support offered by an SSO platform, the more resources the solution can support. Types of authentication schemes include OAuth, OpenID, OpenID Connect, and Facebook Connect.
- **Support for Security Assertion Markup Language (SAML)** – In order to extend support to the breadth of web-based applications, SSO solutions must conform to the XML-based SAML 2.0 standards to allow common assertions to be issued across disparate security domains.
- **Key IT Service Support** – To minimize end-user friction with authentication processes, an SSO solution should govern the majority, if not all, of the IT services in use in the organization. These include providing support for specific applications, private and public application hosting environments, and different types of service. It is recommended that organizations create a list of critical IT services to ensure they are supported when potential solutions are being evaluated.
- **Context-Aware Authentications** – The level of security imposed by the SSO solutions should dynamically adjust to the level of risk associated with the conditions of the access request. Risk elements may include a device's physical location, network connection, running processes, installed applications, and device states (e.g., the existence of malware or if the device has been rooted or jailbroken). High-risk scenarios could result in more frequent re-authentication cycles, an increased number of authentication factors, or a restriction of the number of services that can be accessed through SSO.
- **Integration with Identity Management Tools** – SSO typically does not necessarily need to incorporate any native authentication process, but instead can leverage services offered by third-party solutions. Two-factor or multifactor authentication solutions are always preferred, since they provide the most effective methods for confirming user and/or device identities. Direct integration with identity management tools will greatly simplify SSO administration and security effectiveness.


© 2018 Enterprise Management Associates, Inc.

# FOCUS ON: PRIORITY #5—REDUCING END-USER FRICTION WITH SINGLE SIGN-ON


ca technologies

**EMA HAS IDENTIFIED CA TECHNOLOGIES AS A TOP 3 SOLUTION PROVIDER FOR REDUCING END-USER FRICTION WITH SINGLE SIGN-ON IN 2018**

| | |
|---|---|
| **PLATFORM:** CA Single Sign-On | **ARCHITECTURE:** Software-based platform that integrates directly with CA's gateway, directory and authentication solutions |

**KEY FEATURES:**

- Supports SSO access across multiple cloud, mobile, and web applications
- Identity federation is supported over a wide variety of open standard protocols, including OpenID Connect, OAuth, SAML, and WS-Federation
- Social identities can be leveraged for SSO authentication
- Access requests that require additional security can automatically "step up" authentication processes
- JSON web session tokens can be shared with other authorization providers to create a seamless login experience

**To learn more about CA's Identity and Access Management solutions, visit:**

https://www.ca.com/us/products/identity-and-access-management.html

**To learn more about CA Single Sign-On, visit:**

http://www.ca.com/single-sign-on


© 2018 Enterprise Management Associates, Inc.

## About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

---

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "EMA" and "Enterprise Management Associates" are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2018 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

**Corporate Headquarters:**
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3749-CA.091418