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 HELPSYSTEMS

Written by Steve Brasen

Q3 2018

EMA™

IT & DATA MANAGEMENT RESEARCH • INDUSTRY ANALYSIS • CONSULTING

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

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

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.

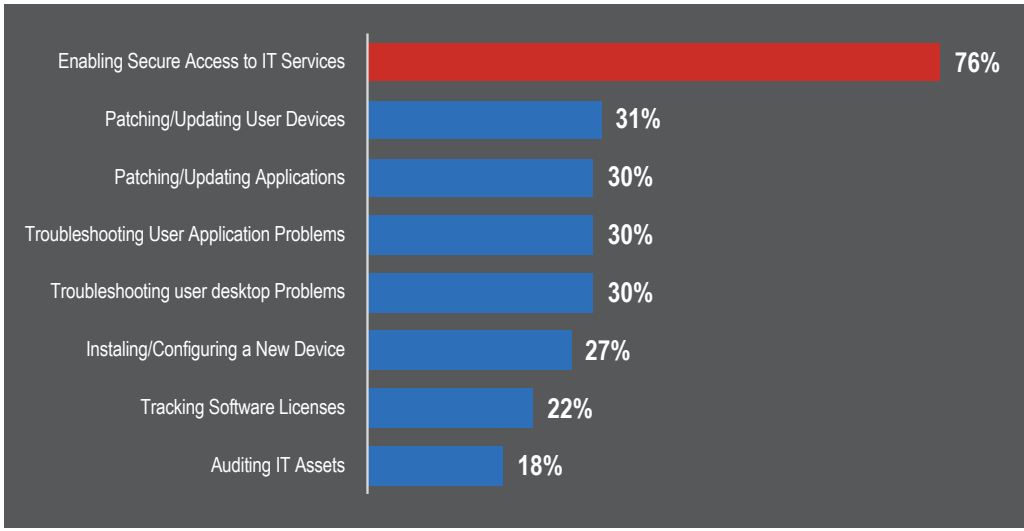

Figure 1: Percent of survey respondents indicating endpoint management processes that are critical to their business

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.

PRIORITY #1—UNIFYING ACCESS CONTROL ACROSS HYBRID IT ECOSYSTEMS

Quick Take

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.

Requirements and Challenges

The introduction of public and private cloud-hosted services marked a radical departure from traditional client/server models of software distribution. Eager to take advantage of the cost-effectiveness, ease of management, and performance improvements inherent in software as a service (SaaS) applications, web services, and virtual applications, organizations rapidly introduced a variety of services without fully considering the access control requirements for the disparate solutions. In fact, in most organizations today, a completely different access process is established as each new service is introduced. As a result, security processes are layered on top of each other in complex and often uncontrolled ways. This complexity substantially reduces the manageability of software ecosystems and obstructs the environment visibility necessary to achieve security and compliance objectives.

Supporting Technologies

Features and integration that enable the unification of access management constitute the core focus of supporting solutions. Centralized solutions must enable consolidated access controls for public and private cloud-hosted applications, web applications, virtual resources, downloadable software, and data shares. While many solutions on the market today support access controls to on-premises software resources, only a few extend these capabilities to also support public cloud and SaaS applications. Additionally, truly hybrid applications (incorporating software components hosted both on-premises and on public clouds) should be supported with a single management interface. Moreover, unified access controls should be provided, ideally governed by multi-factor authentication (MFA) for initial authentication and single sign-on (SSO) access for subsequent friction-less connectivity to all business IT resources. Because the key requirements for this category involve broad control over hybrid and disparate services, supporting solutions typically control access at the network level and must include strong integrations with third-party platforms to enable unified control and holistic visibility.

Key Considerations for Adopting a Solution

- **Console Interface Breadth of Support** – Access to all enterprise-supported software resources should be managed from the unified console to reduce management efforts and ensure consistent policies. Dashboards should be fully customizable, enable access based on user roles, and allow for the creation policies that can be grouped by end-user types, device type, and the hosted IT services being accessed.
- **Endpoint Identity Management Capabilities** – To ensure access to business IT services is limited to only authorized devices, endpoints must be positively "fingerprinted" through a wide variety of unique identifiers, including operating system details, network protocol information, hardware configurations, and data collected though agentless connections (i.e., SNMP and WMI).
- **Hybrid Hosting Environment Support** – To be comprehensive, solutions must be able to control access to all software hosting environments in use by the organization. These may include private business networks, DMZ environments, business-controlled services on public clouds (IaaS or PaaS), public SaaS services, and web hosting environments.
- **Connectivity Governance** – The solution should monitor and manage network connections between the endpoints and the software resources. These may include virtual proprietary networks (VPNs), IPSec connections, tunneling services, and clientless access solutions.
- **IT Service Integrations** – Key points of direct integration with third-party vendors are essential for enabling consolidated management of IT services. In particular, integrations should be established with directory services (i.e., Microsoft Active Directory and LDAP), cloud service providers (AWS, Azure, Google), SAML-based service providers, identify and access management solution providers, and network management platforms. Additionally, robust APIs should be included to enable the creation of custom integrations and extensible automation.

PRIORITY #1—UNIFYING ACCESS CONTROL ACROSS HYBRID IT ECOSYSTEMS

Top 3 Solution Providers

The following solutions have been identified by EMA as providing the leading platforms for unifying access control across hybrid IT ecosystems in 2018.

Note: Solution providers are listed alphabetically. The order presented here is not an indication of EMA preference.

TOP 3 SOLUTION
LUMINATE
PLATFORM: BeyondCorp-as-a-Service
ARCHITECTURE: Cloud-hosed on AWS, Microsoft Azure, or Google Cloud Platform
PULSE SECURE
PLATFORM: Pulse Cloud Secure
ARCHITECTURE: Physical or virtual appliance. May also be cloud-hosed on AWS or Azure.
RSA
PLATFORM: RSA SecurID Access
ARCHITECTURE: Hybrid solution integrating on-premises and cloud-hosted components

PRIORITY #2—PROVIDING SECURE ACCESS TO WEB SERVICES

Quick Take

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.

Requirements and Challenges

According to EMA primary research, 46 percent of organizations today rely on web-hosted services to support business operations, including applications, email services, social media, data shares, and a wide variety of other HTML-based resources that enable workforce productivity. In fact, in many enterprises, users function entirely by performing tasks on web-hosted services. Unfortunately, web browsers have proven to be particularly susceptible to malicious exploitation. Poor user practices for password management, clickbait avoidance, and phishing entrapment all contribute to the exposure of web sessions to malicious exploitation. Compromised and disreputable websites may also modify security settings, alter web links and shortcuts, reset network proxy setting, and change registry keys to alter the behavior of browser activities. Additionally, cross-site scripting attacks can inject malicious instructions into HTML code on a website that would otherwise be considered trusted, and cryptojacking can infect browsers, covertly reducing endpoint performance to support cryptocurrency mining.

Supporting Technologies

To enable trusted use of web services, organizations must proactively prevent the covert downloading of malicious code while also blocking the inappropriate mining of sensitive information from the endpoint. However, this process must not reduce user experiences or the performance of web activities. “Browser isolation” platforms accomplish both requirements by executing the code of a web page inside an isolated container or virtual instance, preventing direct interaction between the website and the endpoint. Since remote browser isolation processes operate invisibly to end users, a familiar user experience is established, allowing them to access the resources they need to perform job tasks in a consistent manner.

Key Considerations for Adopting a Solution

- **Support for Remote Web Access** – Control over web-hosted services accessed to perform business-related tasks must be enabled for endpoints initiating the connection from locations outside the business network to support workforce mobility. End users should be able to access web services in the same consistent manner and with the same security, regardless of where they are physically located at any given time.
- **User-Focused Browser Support** – Ideally, a solution should allow users to access web-hosted services using any browser they prefer (e.g., Chrome, Firefox, Safari, Edge, etc.). If a proprietary, business-dedicated browser must be adopted, it should be intuitive and easy to use.
- **Centralized Control of Web Access** – Role-based user profiles should define the web services that individuals may access by allowing the explicit white-listing and black-listing of websites. Profiles should automatically adjust to contextual situations to add additional layers of security when employed under riskier conditions.
- **Purging of Browser Instances** – Upon completion of a browser session, all elements of the connection (including HTML code, cookies, files, or other remnants of the session) should be automatically purged to eliminate any chance of undetected malware infecting enterprise resources.
- **Blocking of Data Sharing Activities** – Browser use should prevent the unauthorized sharing of business data by blocking activities that may circumvent security policies. These include blocking cutting and pasting, screen grabs (e.g., screenshot capture), direct download of files, duplication of files onto attached media, and the sharing of company files on public email systems.

PRIORITY #2—PROVIDING SECURE ACCESS TO WEB SERVICES

Top 3 Solution Providers

The following solutions have been identified by EMA as offering the leading platforms for providing secure access to web services in 2018.

Note: Solution providers are listed alphabetically. The order presented here is not an indication of EMA preference.

TOP 3 SOLUTION
AUTHENTIC8
PLATFORM: Authentic8 Silo
ARCHITECTURE: Public cloud-hosted solution
ERICOM
PLATFORM: Ericom Shield
ARCHITECTURE: May be deployed in a secure enterprise DMZ, on private/public clouds, or on hybrid environments
NTREPID
PLATFORM: Passages
ARCHITECTURE: Hybrid 'browser as a service' platform with local virtual machine and cloud isolation

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.

PRIORITY #3—ENABLING SECURE REMOTE ACCESS TO BUSINESS NETWORKS

Top 3 Solution Providers

The following solutions have been identified by EMA as providing the leading platforms for enabling secure remote access to business networks in 2018.

Note: Solution providers are listed alphabetically. The order presented here is not an indication of EMA preference.

TOP 3 SOLUTION
F5
PLATFORM: BIG-IP Access Policy Manager
ARCHITECTURE: Physical appliance
PULSESECURE
PLATFORM: Pulse Connect Secure
ARCHITECTURE: Physical or virtual appliance. May also be cloud-hosed on AWS or Azure.
SONICWALL
PLATFORM: SonicWall Secure Mobile Access (SMA)
ARCHITECTURE: Endpoint application. Available as hardware and virtual appliances.

PRIORITY #4—ORCHESTRATING DIGITAL WORKSPACES

Quick Take

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.

Requirements and Challenges

Workforces are increasingly relying on a variety of different devices—including PCs, mobile devices, tablets, and smartphones—to access the business applications, data, and services they need to complete job tasks. In traditional environments, each endpoint device and operating system requires separate access processes and provisioning tools. This creates a complex environment for IT managers to support, requiring excessive time focused on resolving mundane end-user requests and endpoint provisioning tasks. Additionally, end-user productivity is diminished when they need to utilize different access processes depending on their preferred device at any particular moment.

Supporting Technologies

Digital workspace solutions create a common user environment containing all the business IT resources an end user requires to perform job tasks. Unlike traditional desktop approaches, digital workspaces are abstracted from the operating system, allowing users to create custom work environments that operate on any device. Digital workspace solutions are typically cloud-hosted environments that present selectable IT services via an online app store or service catalog. Access, configuration, and security policies are centrally managed for all downloadable, web, and virtual content the platform supports.

It is important to note that a number of vendors offer desktop as a service (DaaS) and HTML desktop platforms that leverage the popular term "workspace." However, EMA does not consider these true digital workspaces because they require persistent connectivity and are not adaptable to unique endpoint requirements.

Key Considerations for Adopting a Solution

- **Breadth of IT Service Supported** – Comprehensive support should be offered for all on-premises and publicly-hosted IT services utilized on endpoints to support business requirements. This includes downloadable applications, web applications, SaaS services, virtual applications, mobile applications, data stores, email services, and any other business-related software resources.
- **Supported Endpoints** – Foundational to orchestrating digital workspace environments is the ability to provide unified endpoint management of IT services. Solutions should broadly enable services to be provisioned on any endpoint device types (PC, desktop, laptop, or smartphone) or operating systems (Windows, macOS, Android, iOS, etc.) in use by supported users.
- **Self-Service Capabilities** – The more control users have in selecting and configuring their preferred and required IT resources, the greater the improvement to their productivity and overall user experiences. Additionally, enabling user self-service reduces the burden on IT support staff for performing mundane provisioning tasks.
- **Context Awareness** – Security policies for enabling access to business services should be conditional based on the context of the intended connection. Risk assessments on access approval is dependent on a number of considerations, including the physical location of the endpoint, the reliability of the network connection, the sensitivity of the resources being accessed, the security of the endpoint device, and other variable states.
- **Adaptability** – End users should only be presented with IT services that they are authorized to use and that can run on their device. When changing devices, the digital workspace platform should dynamically present alternative methods for performing the same tasks (such as by presenting an application in a virtual instance or running a comparable application native to that device).

PRIORITY #4—ORCHESTRATING DIGITAL WORKSPACES

Top 3 Solution Providers

The following solutions have been identified by EMA as providing the leading platforms for orchestrating digital workspaces in 2018.

Note: Solution providers are listed alphabetically. The order presented here is not an indication of EMA preference.

TOP 3 SOLUTION
CITRIX
PLATFORM: Citrix Workspace
ARCHITECTURE: Public cloud-hosted offering with optional integrated software components available for servers, networks, and endpoints
CLOUDJUMPER
PLATFORM: Cloud Workspace
ARCHITECTURE: Public and Private cloud-hosted solution
VMWARE
PLATFORM: Workspace ONE
ARCHITECTURE: Public cloud-hosted solution

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.

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

Top 3 Solution Providers

The following solutions have been identified by EMA as providing the leading platforms for reducing end user friction with single sign-on in 2018.

Note: Solution providers are listed alphabetically. The order presented here is not an indication of EMA preference.

TOP 3 SOLUTION
CA TECHNOLOGIES
PLATFORM: CA Single Sign-On
ARCHITECTURE: Software-based platform that integrates directly with CA's gateway, directory, and authentication solutions
OKTA
PLATFORM: Okta Identity Management
ARCHITECTURE: Software-based, server-hosted platform
RSA
PLATFORM: RSA SecureID Access
ARCHITECTURE: Hybrid solution integrating on-premises and cloud-hosted components

PRIORITY #6—SIMPLIFYING APPLICATION DEPLOYMENT/INSTALLATION

Quick Take

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.

Requirements and Challenges

While application deployments may seem like an outdated IT support requirement to non-administrators, the reality is that managing the secure and reliable packaging, distribution, and installation of software tends to be the task workspace engineers spend the most time addressing. This is principally due to the increased complexities of application ecosystems. Many of today's applications are dependent on access to software subsystems (such as databases, web services, and data repositories) that are hosted across a variety of public and private cloud environments. These hybrid applications require very specialized configurations to guarantee connectivity between services remains secure while still ensuring optimal performance. Additionally, there is a much more diverse range of device architectures (desktops, laptops, tablets, and smartphones) and operating systems (Windows, macOS, Linux, iOS, and Android) that require independent application versions and dependencies. To accommodate these increasing complexities, many organizations resorted to over-scripting their deployment processes. Since scripts are not officially supported software, these became problematic every time there was a radical update to supported applications or endpoint operating systems. Additionally, script-heavy environments are difficult to maintain when the script creators leave the company.

Supporting Technologies

While digital workspaces, enterprise app stores, and service catalogs can provide end users with a consolidated method for accessing software services, the actual installation of downloadable apps or any code that will run locally on endpoint devices is dependent on the automated deployment solution running behind the scenes. Complex application environments must be carefully orchestrated during the packaging process to ensure that applications installed on endpoints are configured appropriately to meet enterprise requirements for security and performance. This includes the execution of pre- and post-installation tasks, and may involve supervising endpoints through one or more reboots. To enable optimal network performance and ensure the security of software elements, application deployment packaging solutions store all software installation components in an on-premises library. This minimizes WAN traffic when hundreds or thousands of endpoints attempt to update or install applications simultaneously. The library also allows versioning support for applications so they can be rolled back, if necessary, to support compatibility or compliance requirements.

Key Considerations for Adopting a Solution

- **Heterogeneous Support** – Automated deployment solutions should be able to manage application installations for all endpoint devices and operating system versions used to perform business tasks.
- **System Configuration and Dependency Validation** – To ensure applications can be installed on endpoints, any specific system requirements or software dependencies should be automatically identified before the execution of installation processes. These include checking for available disk space, sufficient system resources (CPU, memory, etc.), a compatible operating system and patch versions, the existence of previous software versions, and the availability of dependent software subsystems and executables.
- **Identify Security Vulnerabilities** – Before the execution of business application installations, devices should be scanned to ensure they have not been bypassed at the OS level (e.g., rooted or jailbroken), do not contain malware, and conform to any other business requirements for security and compliance.
- **Integration with User Self-Service Portals** – To minimize user requests to IT administrators and improve end-user experiences, automated software deployment solutions should integrate directly with enterprise app stores, service catalogs, and digital workspace environments, allowing end users to select and download the applications they prefer, on the devices they use, and at a time that is most convenient for them.
- **License Management** – The availability or integration with software license management and tracking capabilities will help ensure businesses are not over-paying for software purchases. For instance, the identification of unused software licenses will allow them to be reclaimed or repurposed. Additionally, software metering features will allow organizations to restrict the number of software deployments or allow users to install/access software for only a limited period of time.
- **Migration Support** – As users update their devices or transition to new devices, application deployment solutions should be able to map their previous software installations and configurations to compatible editions on the new environment.

PRIORITY #6—SIMPLIFYING APPLICATION DEPLOYMENT/INSTALLATION

Top 3 Solution Providers

The following solutions have been identified by EMA as providing the leading platforms for simplifying application distribution/installation in 2018.

Note: Solution providers are listed alphabetically. The order presented here is not an indication of EMA preference.

TOP 3 SOLUTION
IVANTI
PLATFORM: Ivanti Endpoint Manager
ARCHITECTURE: Software-based platform
QUEST
PLATFORM: KACE Systems Deployment Appliance
ARCHITECTURE: Physical or virtual appliance
SYMANTEC
PLATFORM: Symantec Client Management Suite
ARCHITECTURE: Software-based platform. May also be hosted as an AWS cloud service.

PRIORITY #7—FACILITATING SECURE DATA SHARING

Quick Take

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.

Requirements and Challenges

While access to applications is most frequently targeted with security protection solutions, it is really the enterprise data that comprises the greatest potential risks to businesses. Data has never been more distributed than it is today—it is stored on user devices, on servers, on public and private clouds, inside applications, in emails, on websites, and on social media outlets. Further, with content continually being created using a variety of different mobile and PC endpoints, it is simply impossible for organizations to maintain control over the location and distribution of sensitive business information using purely manual processes. Unfortunately, organizations do not have the luxury of restricting data storage and sharing capabilities to just approved resources, since this would impact workforce productivity and their ability to functionally collaborate. In fact, EMA primary research indicates attempts to try and impose restrictions are most likely doomed to fail. Forty percent of business professionals surveyed indicated they regularly used unsecure methods for data sharing, even though 81 percent of those same respondents admitted to having access to more secure solutions through their employer. Put simply, users will often opt to circumvent security practices in favor of convenience because, at the end of the day, they just want to get their job done.

Supporting Technologies

To be effective, data sharing solutions must ensure the security of business content in a way that incorporates how users prefer to access, edit, and distribute digital information. Enterprise file sync and share (EFSS) solutions allow users to securely share documents and other data with anyone inside or outside the organization in accordance with business requirements for security and compliance. Additionally, EFSS platforms enable users to synchronize their files across all of their device types (desktops, laptops, tablets, and smartphones), establishing consistent data storage environments and allowing users to seamlessly switch between devices while continuing to perform job tasks. Typically, EFSS solutions store data on cloud-hosted environments and grant users direct access to files when they are on-premises in the business facilities or operating remotely. It is essential for all EFSS solutions to incorporate stringent security protections for files, including authentication processes, encryption, antivirus scanning, and DLP processes.

Key Considerations for Adopting a Solution

- **Heterogeneous Support** – The platform should support storage and sharing of all content created on all endpoint device types (desktops, laptops, tablets, and smartphones), operating systems (Windows, macOS, Linux, iOS, and Android), and applications (installed apps, virtual apps, cloud apps, web apps, and hybrid apps) in use in the organization.
- **Data Governance** – Organizations most frequently adopt EFSS platforms to ensure achievement of regulatory compliance (e.g., HIPAA, SOX, PCI, GDPR, etc.), security assurance, or other governance agendas. To support this, EFSS platforms must enable granular audits and report for "proof of compliance," as well as process workflows that ensure business policies are followed in a consistent manner.
- **Collaboration Tools** – Multiple users should have the ability to edit the same file at the same time to support collaboration scenarios. To prevent conflicts, users should have the option to lock the file while they are making changes. In the event conflicting changes are made to an unlocked document, a reconciliation process should be available to merge the discrepancies into a clean version.
- **Integration with Third-Party Software Providers** – Since many email, SaaS, web, cloud, and installed applications directly create, edit, and distribute business content, direct integration should be established that ensures relevant files are consistently governed by the security protocols of the EFSS platform.
- **Business Continuity** – EFSS platforms must ensure the continuous and reliable integrity of stored data by incorporating disaster recovery and failover capabilities.

PRIORITY #7—FACILITATING SECURE DATA SHARING

Top 3 Solution Providers

The following solutions have been identified by EMA as providing the leading platforms for simplifying application distribution/installation in 2018.

Note: Solution providers are listed alphabetically. The order presented here is not an indication of EMA preference.

TOP 3 SOLUTION
BOX
PLATFORM: Box for Business
ARCHITECTURE: Public cloud-hosted platform
CITRIX
PLATFORM: Citrix Content Collaboration (ShareFile Integration)
ARCHITECTURE: Public cloud-hosted platform
EGNYTE
PLATFORM: Egnyte Connect
ARCHITECTURE: Public cloud-hosted, on-premises, or hybrid deployments available

PRIORITY #8—NETWORK ACCESS CONTROL WITH IOT ENABLEMENT

Quick Take

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.

Requirements and Challenges

The past decade saw an exponential increase in the number and types of supported computing endpoints thanks to the influx of new device architectures and mobile devices. This substantially increased the complexity of managing and securing IT systems and services across an enterprise. However, even this plethora of growing requirements for supporting broadly heterogeneous device architectures pales in comparison to the rising wave of IoT devices that organizations have already begun to introduce into their business environments. IoT devices are used for a variety of automation, sensing, and monitoring tasks, and to enhance workforce productivity. In fact, any chip-enabled object that is network-attached is qualified as a "thing" that requires the same level of security assurance as more traditional servers, desktop, laptops, and mobile devices. What makes supporting IoT devices particularly challenging in comparison to computing systems is that IoT devices lack standards. Different chip sets, unique hardware configurations, and custom software code make each IoT device singular in its design. To enable security policies using traditional software and agent-based approaches would require the development of hundreds or even thousands of software versions. Nonetheless, organizations increasingly reliant on IoT device enablement must ensure secure access to and from these resources is continuously maintained.

Supporting Technologies

A basic precept of modern IT is that nearly all connections between computing elements must flow through a network. This reality offers significant opportunities for unifying security and access enablement by managing network traffic, rather than controlling endpoint devices. NAC solutions accomplish this by utilizing established network protocols to dynamically enforce predetermined policies. The key advantage to operating at the network layer is that no software needs to be deployed on the endpoint devices or server hosting environment to enable access control. A NAC can support any device or service that utilizes the supported protocols. This is particularly advantageous when enabling access to IoT devices, since it is not dependent on any particular hardware chip set or software architecture. Similarly, endpoints seeking access to IoT devices are universally supported by a NAC regardless of their form factor or operating system, without the need to install agent-based management software or malware protection packages. NAC solutions allow organizations to define granular policies that can automatically prevent risky connections, intrusive malware, and other vulnerabilities in real time.

Key Considerations for Adopting a Solution

- **Scalability** – The number of endpoint and IoT devices on enterprise IT networks are expected to grow exponentially over the next few years. Adoption of any security and access enablement solution must provide the extensibility to support future growth while still meeting budgetary limitations.
- **IoT Device Authentication** – The identification of approved devices on a supported network should be enabled based on predetermined characteristics, such as the device type, configuration, manufacturer, network address, physical location, or the owner's business role (e.g., title, department, or job function).
- **Contextually-Aware Policy Controls** – Users should be able to establish conditional rules to create business policies based on IoT device attributes. Based on detected conditions, the NAC solutions should be able to limit the devices that are allowed to operate on a supported network and the devices specific users may access. Additionally, dynamic polices should be able to automatically execute the transitioning of devices to alternate networks, the isolation of devices, or actions on third-party security and network management systems based on a detected access or security state deemed to be risky in real time.
- **Inclusion of a RADIUS Server** – Authentication, authorization, and accounted management services supporting user access to network-connected IoT devices are greatly simplified with the integrated availability of a Remote Authentication Dial-In User Service (RADIUS). Ideally, a RADIUS server should be included with a NAC solution to simplify deployment and ensure fully-functional integration that enables faster-performing network processing.
- **Dashboarding, Reporting, and Alerting** – IT managers should have the ability to generate customizable dashboards and ad hoc reports that provide a variety of detailed and easy-to-understand information on IoT devices, the state of the network, and access requests. Examples include reports for device discovery, classification, inventory, compliance, detected anomalies, and change events. Additionally, alerts should be issued upon the detection of a critical state, such as when a device fails to meet an access policy prerequisite or when anomalous activity is detected.
- **Third-Party Integrations** – To enable holistic views of the IT ecosystem that will facilitate context-aware policies and intelligent access connections, NAC solutions should broadly integrate with third-party solutions including directory services, security management platforms, network switch and wireless controllers, endpoint management platforms, and event management systems. The availability of APIs will also assist in establishing custom integrations.

PRIORITY #8—NETWORK ACCESS CONTROL WITH IOT ENABLEMENT

Top 3 Solution Providers

EMA identified the following solutions as providing the leading platforms for network access control with IoT enablement in 2018.

Note: Solution providers are listed alphabetically. The order presented here is not an indication of EMA preference.

TOP 3 SOLUTION
ARUBA
PLATFORM: Aruba ClearPass
ARCHITECTURE: Physical or virtual appliance
FORESCOUT
PLATFORM: ForeScout CounterACT
ARCHITECTURE: Physical or virtual appliance
PULSESECURE
PLATFORM: Pulse Policy Secure
ARCHITECTURE: Physical or virtual appliance

PRIORITY #9—ENABLING PRIVILEGED ACCESS MANAGEMENT

Quick Take

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.

Requirements and Challenges

In order to complete essential job tasks, it is sometimes necessary to grant end users elevated privileges to their endpoint devices, business servers, databases, and critical applications. However, a lack of constraints on the types of tasks users are permitted to perform often leads to unqualified individuals having an inflated sense of expertise and a belief that they can manage systems as well (if not better) than the trained administrators responsible for supporting them. In the interest of self-serving expediency, end users may sometimes use privileged access credentials to bypass security, circumvent business policies, or introduce unapproved changes to production systems. These actions can violate security and regulatory compliance policies, reduce business performance, disable essential services, and/or introduce IT challenges that are costly and time-consuming to remediate. Additionally, a lack of control over privileged access accounts could result in a severe breach of enterprise security if they fall into the hands of a malicious attacker.

Supporting Technologies

To maintain control over business IT resources, organizations must introduce PAM solutions specifically designed to regulate the issuing of elevated privileges, limit their use to just approved activities, and track any privileged tasks performed to ensure accountability. This infers a level of governance that goes beyond just basic identity management or password vaulting. Two key concepts encompass strategic PAM solutions. The first suggests that users should only be provided access to the systems, application, and service they need to perform job functions, but no more than required. This precludes the option of granting blanket administrator or root privileges that allow users to reach beyond their authorized tasks. The second fundamental precept of a strategic PAM solution is that users should only have elevated privileges for the length of time they require them to accomplish specific tasks. Often called "just-in-time access," PAM solutions authorize access only when it is required and automatically disable access when it is no longer needed. Ultimately, the goal of PAM solutions is to empower users with elevated privileges when, where, and how they require them to perform job tasks, while at the same time eliminating risks of abusing privileges or increasing chances of security breaches.

Key Considerations for Adopting a Solution

- **Control Access Across Distributed Environments** – All environments (on-premises, off-premises, public, private, and personal) that host business IT services should be governed to ensure security and compliance requirements are met. Ideally, a PAM solution will centrally monitor and support all IT systems and services from a single centralized console
- **Default to Least Privileges Required** – Solutions should always grant minimal access privileges to IT services and systematically elevate privileges as they are needed until they reach a hierarchical level necessary to perform essential job tasks. Escalations can be an automated processes or require authorizations from a designated authority.
- **Privilege Expiration** – No privileged access should be forever. To ensure privileges are not granted when they are not needed, PAM solutions should automatically revoke credentials after a predetermined period of time or after completion of the tasks that warranted the privilege elevation.
- **Reporting and Alarming** – Even with protections in place, organizations must still contend with individuals who will attempt to circumvent established PAM restrictions. These events should be detected and reported in real time so immediate steps can be taken to block use of the unauthorized access, identify the culprit, and take steps to prevent future occurrences.
- **Support Governance Requirements** – To effectively reduce access privilege abuse and meet regulatory compliance commitments, organizations should establish governance bodies responsible for overseeing the development of privileged access policies. PAM solutions should provide flexible profiles and automation to help governance bodies meet established policies and process workflows.

PRIORITY #9—ENABLING PRIVILEGED ACCESS MANAGEMENT

Top 3 Solution Providers

EMA identified the following solutions as providing the leading platforms for enabling privileged access management in 2018.

Note: Solution providers are listed alphabetically. The order presented here is not an indication of EMA preference.

TOP 3 SOLUTION		
BOMGAR	PLATFORM: Bomgar Privileged Access	ARCHITECTURE: Physical or Virtual Appliance Also offered as a cloud-hosted solution
helpsystems	PLATFORM: BoKS ServerControl	ARCHITECTURE: Software-based platform
	KEY FEATURES: • Transforms multivendor Linux and UNIX server environments into a centrally-managed security domain, simplifying the enforcement of security policies and access controls • Enables centralized management of user profiles and accounts at scale, including rapidly creating, modifying, and/or removing user and group access rights • Centralized SSH key management and SUDO controls ensure local and remote execution of privileged processes do not violate business policies • Automated credentials management and enforcement help organizations meet strict compliance regulation, such as PCI-DSS, HIPAA, and SOX • Integrates with third-party platforms for federated connections with directory and web-based identity services	
	Learn more about BoKS Server Control at: https://www.helpsystems.com/products/privileged-access-management **Contact HelpSystems:** https://www.helpsystems.com/contact-us Email: info@helpsystems.com Toll free: 800-328-1000 Phone: +1 952-933-0609	
REMEDIANT	PLATFORM: SecureONE	ARCHITECTURE: Physical or virtual appliance Public cloud-hosted platform

PRIORITY #10—SUPPORTING "BRING YOUR OWN DEVICE" INITIATIVES

Quick Take

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.

Requirements and Challenges

In traditional enterprise PC environments, organizations purchased all laptop and desktop devices used by their employees. This afforded businesses a great deal of control over which device architectures were adopted and how they were used. However, over the last decade, the consumerization of IT shifted the purchase power of endpoint devices from the business to the end user. EMA survey-based primary research indicates 70 percent of mobile device users and 35 percent of laptop users now personally own the devices they use to regularly perform job tasks. As more and more business workers began bringing their devices into their workplace to perform job tasks, organizations increasingly need to adjust processes for security and access privileges to accommodate non-business-owned endpoints. The principle challenge is that organizations can not tell employees how they can and cannot use their personal devices. All they can do is allow or deny them access to business IT services. To keep their workforces happy and productive, however, most organizations opt to allow employee-owned devices access to business resources. This can place the business at extreme risk as non-business use of devices often results in the inadvertent download of malware, unsecured device configurations, and a lack of control over stored data and sensitive applications.

Supporting Technologies

To ensure users are able to utilize their personal devices to perform personal tasks without compromising the security of business applications, data, and IT services requires a logical separation of the two environments. Resource isolation solutions have evolved as the primary method for supporting BYOD endpoints. As the name implies, resource isolation solutions segment business services so they can be managed independently of any other device uses. Common technologies introduced to support resource isolation include containerization, app wrapping, virtualization, dual persona, browser isolation, and the tagging of apps and data that are governed by a software agent. Common to all of these approaches is the ability of an organization to centrally define policies that govern business resources, but only business resources.

Key Considerations for Adopting a Solution

- **Heterogeneous Endpoint Support** – Since employee-owned devices are user-selected, they encompass a broad range of form factors (laptops, desktop, smartphones, and tablets) and operating systems (Windows, Mac, Linux, iOS, Android, and Chrome OS). Regardless of the approach to resource isolation offered, BYOD solutions should support all user-owned devices that are permitted to access business resources to enable consolidated policy management, security assurance, and reporting.
- **Ease of Deployment** – Most resource isolation approaches require an agent or software application to be installed on the supported endpoints. Simplifying the distribution of this software element requires the ability to remotely push installations across supported endpoint architectures or allow end users to download the software from a public app store or service catalog.
- **User Experiences** – Since BYOD solutions are supporting devices that are not owned by the business, it is essential that they in no way restrict or reduce the performance of any non-business use of the devices. However, at the same time, it is preferable to most users to not be inconvenienced with numerous tasks necessary for accessing business services. Dual persona, for instance, is less favorable to most users because it requires them to not constantly switch between business and personal environments, which can be time-consuming and irritating if both environments are often used.
- **Policy Management** – Policies for enabling access to business IT resources should be centrally established for groups based on user roles, device types, and other unique identifiers. Additionally, dynamic policies should be established based on context-aware information—such as the physical and network location of devices, active processes on endpoint devices, install applications, and compromised device states (i.e., rooted or jailbroken devices, existence of malware, etc.). Endpoint determined not to be in compliance should be automatically blocked from accessing business IT services.
- **Selective Wipe** – When users terminate their employment with an organization, all relevant business data and applications should be automatically removed from their devices. However, the wipe processes must not damage or remove any of the user's personal data or applications.

PRIORITY #10—SUPPORTING "BRING YOUR OWN DEVICE" INITIATIVES

Top 3 Solution Providers

EMA identified the following solutions as providing the leading platforms for supporting "bring your own device" initiatives in 2018.

Note: Solution providers are listed alphabetically. The order presented here is not an indication of EMA preference.

TOP 3 SOLUTION
CITRIX
PLATFORM: Citrix Endpoint Management
ARCHITECTURE: Available as an on-premises software-based solution, physical appliance, virtual appliance, or cloud-hosted service
IBM
PLATFORM: IBM MaaS360
ARCHITECTURE: Public cloud-hosted SaaS solution
VMWARE
PLATFORM: VMware Workspace ONE
ARCHITECTURE: Available as an on-premises software-based solution or cloud-hosted service

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.

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-HelpSystems.082018