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 PULSE SECURE
WRITTEN BY STEVE BRASEN

Q3 2020

EMA™
IT AND DATA MANAGEMENT
RESEARCH | INDUSTRY ANALYSIS | CONSULTING

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, pressures to give an increasingly mobile workforce access to IT services distributed across a variety of public and private hosting environments have significantly challenged organizations. 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 when enabling secure access to business IT resources.

EMA TOP 3

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

Why You Should Read This Research Report

IT managers, security officers, and line of business managers will gain key insights into the following areas:

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

Research Methodology

All research results in this report are based on EMA's survey of 109 randomly selected North American enterprises across a wide range of industry verticals and horizontals. 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.

109	IT managers surveyed
100%	responsible for enabling secure access in their organization
10	key trends identified

2020 Top Priorities for Secure Access Enablement

- Identifying the Level of Data Sensitivity
- Facilitating Secure Data Sharing
- Group and User Policy Management
- Perform Access Auditing and Reporting
- Risk-Based Access Controls
- Achieving Access Requirements for Regulatory Compliance
- Supporting Single Sign-On (SSO)
- Supporting Secure Access to Web Services
- Vaulting Passwords/Credentials
- Enabling Secure Remote Access Across Hybrid Business Networks

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 1, 2020. 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 are 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 this process by providing information on key considerations to review during the selection process, as well as a shortlist 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 endpoint management 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 – Identifying and recognizing the most innovative vendor solutions that address the greatest business priorities for endpoint management enablement, the table in this section provides a brief overview of each platform and their capabilities. The solutions are listed alphabetically by vendor, so the order in which they appear is not an indication of EMA 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 meets 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. Most recently, requirements for enabling secure remote access have substantially increased as the global response to the COVID-19 pandemic broadly expanded work-from-home policies.

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 they 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.

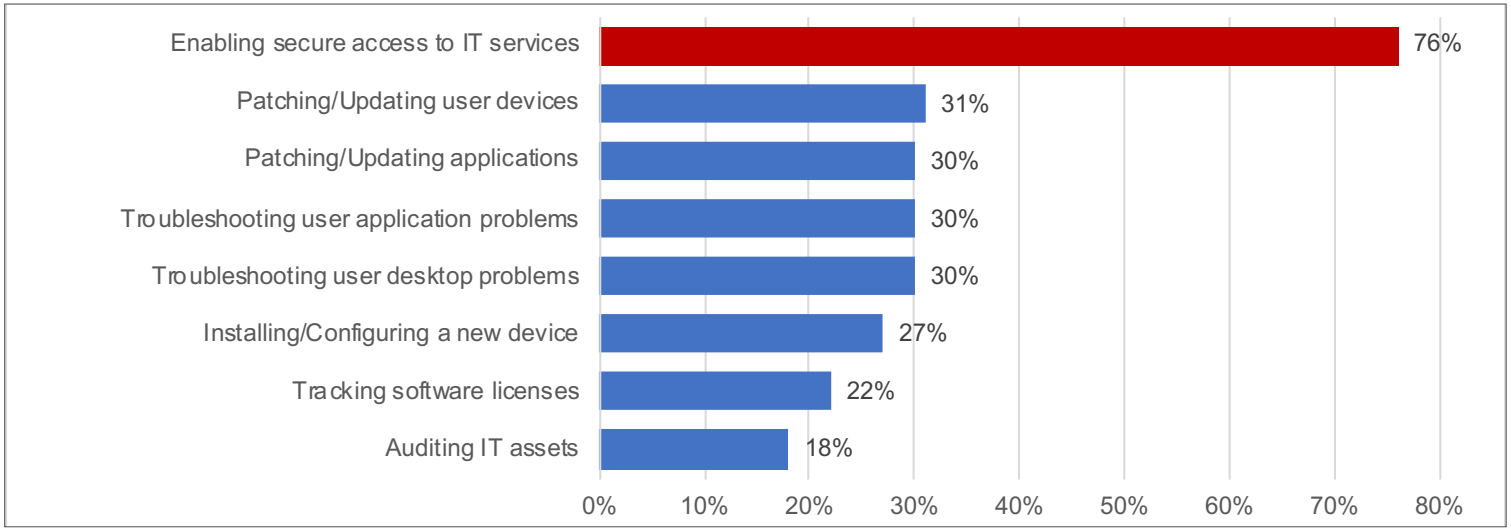

Figure 1: Percentage of survey respondents indicating endpoint management processes that are critical to their business

UNDERSTANDING 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 often considered to be diametrically opposed forces—the more one is enabled, the more limited the other becomes. 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.

EMA primary research strongly indicates that the perception that security and access requirements are opposing forces is not entirely accurate. Overall, organizations that were noted to utilize authentication processes that reduce end-user friction were reported to be 62% less likely to have experienced a security breach in the preceding 12 months than businesses relying on authentication solutions that inhibit end-user productivity. This correlation emphasizes the fact that users are far less likely to bypass enterprise security controls when they are presented with processes that do not disrupt their work performance and are less apt to place the business at risk in order to more quickly perform job tasks. The clear implication is that organizations that responsibly simplify access to IT service simultaneously increase security effectiveness.

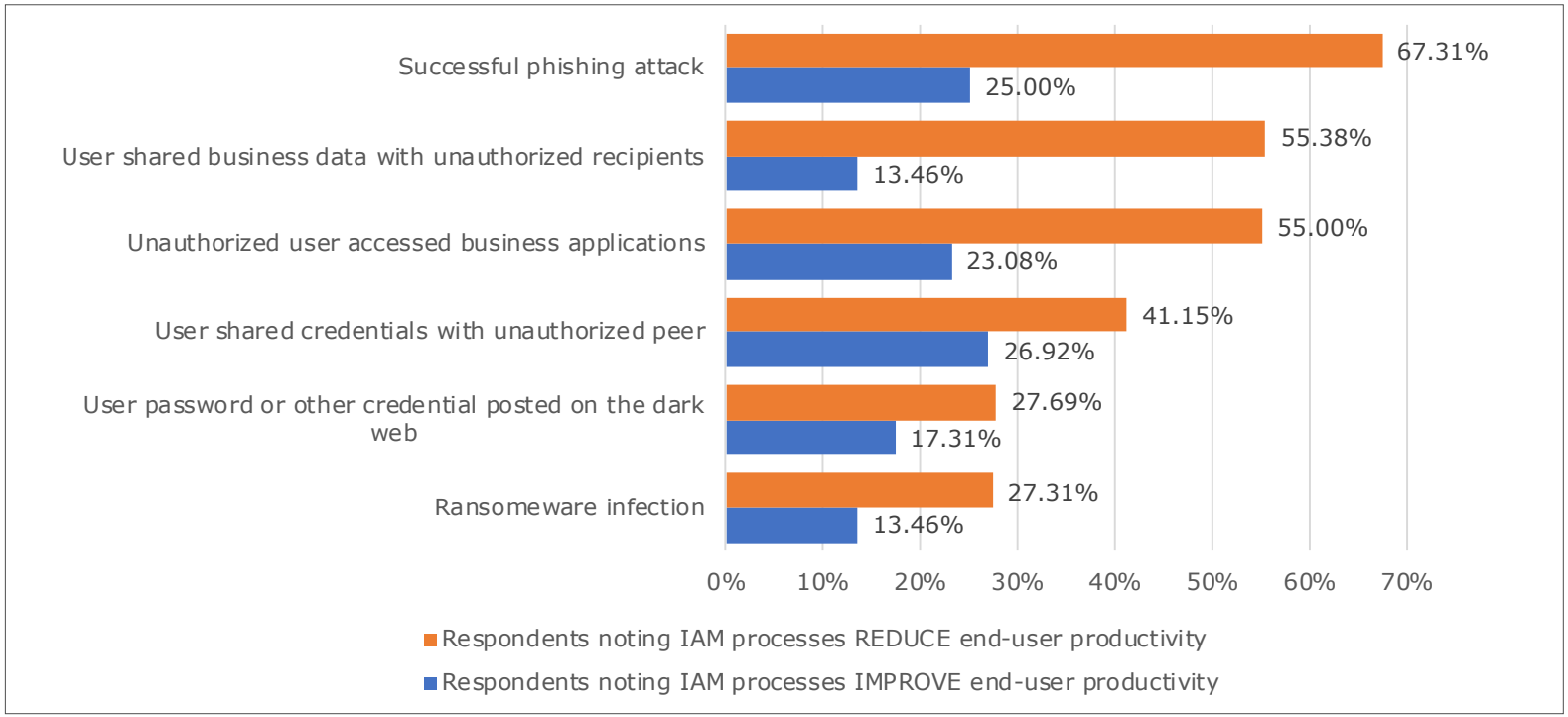

Figure 2: Comparing the percentage of surveyed organizations experiencing security breaches in the previous year between those with high-friction and low-friction authentication processes

UNDERSTANDING SECURE ACCESS

Key Disrupting Technologies for Enabling Secure Access

Satisfying both security and access requirements simultaneously 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:

- **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.
- **Contextual Awareness** – 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 directly connected to a local-area network inside physical office facilities. Policies can be applied to access events to ensure the amount of friction imposed on the end users is appropriate to the contextual conditions.
- **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.
- **Network Access Control (NAC)** – To deal with increasingly complex hybrid IT ecosystems, NAC solutions were developed to dynamically identify, authenticate, and monitor devices accessing networks while extending capabilities that further assess endpoint configurations and security states to determine the extent of authorized access.
- **Secure Remote Access** – As organizations increasingly support mobile workforces, the adoption of technologies designed to securely enable remote access to business IT services has become indispensable. Traditional perimeter-based access solutions—including NGFW, IPSec, and VPN—have been popularly adopted to support these requirements, while new methods and features continue to gain ground that further fortify security, performance, and control. Some examples of advancing technologies in this category include more advanced secure sockets layer VPN (SSL-VPN), internet protocol security (IPSec), layer 2 tunneling protocol (L2TP), secure socket shell (SSH), and STunnel.
- **Risk Intelligence** – Intelligence technologies (including analytics, machine learning, and language processing solutions) can rapidly evaluate large and complex contextual, asset, and security datasets to make a determination on the level of risk posed by authorizing an access request. Typically, related solutions distill results into a single numerical value—a risk score. Policies for accessing business IT services and identifying the tasks that can be formed on them can be specifically limited based on resulting risk scores.
- **Access Governance** – Coordinating the implementation and enforcement of access policies across disparate organizational structures requires a centralized and executive-level governance initiative. Supporting solutions facilitate the orchestration of policy-based access controls, perform periodic access audits, and ensure compliance attainment.

OVERVIEW: TEN PRIORITIES FOR ENABLING SECURE ACCESS IN 2020

Based on responses from 109 enterprises, the following represent the top ten priorities for enabling secure access to enterprise IT resources (including applications, data, email, and other services) in 2020:

1 **IDENTIFYING THE LEVEL OF DATA SENSITIVITY:** 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 **FACILITATING SECURE DATA SHARING:** As workforces increasingly create, access, and distribute business files and data across a wide 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.

3 **GROUP AND USER POLICY:** The creation of comprehensive and effective access policies can be time-consuming and effort-intensive if supported by purely manual processes. Solutions that enable the standardization of policies to align with specific user roles (or other common characteristics) can substantially reduce administration efforts while ensuring consistency in access security enforcement.

4 **PERFORM ACCESS AUDITING AND REPORTING:** Achieving effective access governance requires the periodic examination of user permissions and past access events to identify any violations of established access policies. Comprehensive intelligence on the state of access controls should be collected frequently, cost-effectively, and with minimal administrator effort. The results should be presented in a clear, easily-digestible format to facilitate problem resolution and the determination of policy improvements.

5 **RISK-BASED ACCESS CONTROLS:** The most effective access policies specifically define which IT resources may be accessed and how they may be utilized based on the level of risk posed to the business. This is achieved by collecting a rich set of contextual information on the users, devices, networks, and IT resources involved in the access event. Intelligence technologies analyze this information in real time to determine the level of risk against which access policies can be applied.

6 **ACHIEVING ACCESS REQUIREMENTS FOR REGULATORY COMPLIANCE:** New regional regulations for security and privacy, most notably the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), are challenging businesses to implement more stringent access governance processes and visibility. Supporting solutions simplify efforts for auditing and help attain continuous compliance with secure access processes.

7 **SUPPORTING SINGLE SIGN-ON:** As workforces increasingly rely on disparate IT services to perform job tasks, the complexity of initiating and maintaining authentication processes also accelerates, 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.

8 **PROVIDING SECURE ACCESS TO WEB SERVICES:** While the increased adoption of HTML-based SaaS applications served to reduce the cost and administration required for business productivity software, it also opened the door to new threats to endpoint security. Organizations dependent on web-hosted services to support business operations must ensure fast, easy, and safe connectivity to HTML-based content and services.

9 **VAULTING PASSWORD AND CREDENTIALS:** In order to reduce risks of passwords, personal identification numbers (PINs), and other unique identifiers from being stolen, credentials may be stored in a secure digital (and often encrypted) location called a password vault. Optimal solutions providing these capabilities include elevated protections on credential during use, when in transit, and when stored.

10 **ENABLING SECURE REMOTE ACCESS ACROSS HYBRID BUSINESS NETWORKS:** Remote workforces increasingly require access to business applications, data, and services from a variety of devices through the Internet and unsecured public networks, increasing exposures to attack and risks of compliance failures. Secure access solutions with identity and device security features must create intuitive, compliant, and protected connections for workers to access essential IT resources across business networks, private clouds, and SaaS environments.

FOCUS ON PRIORITY #10: ENABLING SECURE REMOTE ACCESS ACROSS HYBRID BUSINESS NETWORKS

Quick Take

Remote workforces increasingly require access to business applications, data, and services from a variety of devices through the Internet and unsecured public networks, increasing exposures to attack and risks of compliance failures. Secure access solutions with identity and device security features must create intuitive, compliant, and protected connections for workers to access essential IT resources across business networks, private clouds, and SaaS environments.

Requirements and Challenges

In 2020, requirements for enabling secure access from remote workers to hybrid IT business networks accelerated rapidly and substantially. As a result of the COVID-19 pandemic and global stay-at-home orders, workforces in nearly every business sector were suddenly required to enable remote access capabilities in order to continue operations. Solutions enabling employees to work remotely became a critical lifeline during the most challenging days of operational restrictions and trends towards increased workplace flexibility and permanent work from home requirements are expected to define secure remote access capabilities as a key element of IT enablement into the future.

There are two key aspects to supporting remote workforces. The first (and most obvious) is extending access support to a diverse range of users and a variety of portable devices, including laptops, tablets, smartphones, wearables, and IoT devices. The diverse range of end user devices may be managed directly by the business or unmanaged, such as with user-owned devices.

Equally critical to facilitating remote workforces is enabling the portability of the IT services themselves. For instance, telecommuters must be able to perform job tasks require the same level of access as if they were at their desk in the office. In fact, for many companies, enabling remote device use while providing an appropriate level of accompanying security controls is a key requirement for business operations. EMA believes evolving requirement for corporate workstyle and workplace flexibility will drive broader adoption of tighter endpoint security postures. The principle focus for supporting remote workforces is, therefore, enabling secure access to business resources from any device at any location to data centers and cloud-hosted resources.

Beyond supporting workforces accessing business resources from home and abroad, many organizations must also enable remote access to branch offices, outsourced organizations, and service providers. In addition, new digital business services that include web applications, connected businesses, and consumer IoT devices, also add to the scope of secure access requirements, each of which proportionally increases the level of risks of identity theft, outages, unauthorized use, and security breaches. Malicious attackers do not even need to hack into vulnerable servers to compromise business security. They can phish the user, infect the host or 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 policy-based network connections that operate over public networks, but are also ensured to be private and secure. However, any technology introduced to secure sensitive traffic must not impede service performance or substantially diminish user experiences.

Supporting Technologies

Enabling secure access requires ensuring that sensitive traffic is protected end-to-end, regardless of the network path it takes. The most popular method for achieving this is to employ a virtual private network (VPN). While all VPNs (and firewalls that offer VPN services) are designed to enable access to business networks, only some types of solutions include additional security features to ensure identity and host security verification and that connections remain private. One popular method employed to achieve this is to add a secure socket layer (SSL), which encrypts the data being transmitted between the endpoint and the network or cloud resource depending on policy.

An alternative method to ensure confidential network communications is to place a transport layer security (TLS) termination point, such as a reverse proxy, alongside sensitive resources in the same environment. If using a reverse proxy approach, no tunneling is required. Instead, it is installed in the same environment as the application or resource. Additionally, the network path from the requester is irrelevant as all the same encryption and security mechanisms may be applied to the data, ensuring end-to-end security.

Other types of secure network technologies include simultaneous tunneling, split tunneling, SSH tunneling, STunnel, and the Layer 2 Tunneling Protocol (L2TP). The primary goal of each of these approaches is to ensure secure remote access to business IT resources while presenting users with an intuitive experience. In most cases, these types of solutions provide the illusion that user devices are locally connected directly to their company’s IT resources, even though it is actually connecting through remote networks, wireless networks, cellular networks, or the Internet.

FOCUS ON PRIORITY #10: ENABLING SECURE REMOTE ACCESS ACROSS HYBRID BUSINESS NETWORKS

Key Considerations for Adopting a Solution

- **Pearsistence 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 such features as split-tunneling, multi-tunneling, and smooth roaming from remote access to local LAN access.
- **Flexible Access to Internet-Hosted Services** – Many organizations prefer to route traffic through a traditional VPN to business networks and then back to the internet in order to enable access to cloud, SaaS, and web-hosted resources, which may necessitate additional bandwidth and load balancing considerations. Solutions that employ a split- or multi-tunneling approaches will allow devices to send control data through the VPN tunnel while sending data directly to internet resources. To further improve user experiences and resource accessibility, multi-tunneling maintains simultaneous secure connections to multiple distributed VPN gateways and their respective business networks. The ability to provide clientless, browser-based portal access also allows for additional access flexibility to apps and resources.
- **Context Awareness** – When initiating a remote connection, an enterprise-grade secure access solution should evaluate risks to the endpoint 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 locations, running processes, installed applications, operating system version, patch levels, browser type, and any risky device states (e.g., a disabled personal firewall, the existence of malware or if a mobile device has been rooted or jailbroken). Moreover, adaptive access policies will automatically initiate the appropriate level of security required when establishing a remote connection depending on the user, role, device, network and application states. Ideally, access may be terminated if the context violates policy requirements or otherwise indicates an increase in risk.
- **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, Chrome OS, and IoT devices. Any adopted solution should support all devices used in an organization—and for some organization to include personal device control—to prevent the need to adopt multiple secure access solutions. A unified client that supports common operating systems can further streamline deployments.
- **Onboarding Process** – Most 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 integration 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. It is also essential to adopt solutions that support a variety of authentication technologies, including two-factor authentication (2FA), multi-factor authentication, certificates, hardware and software tokens, biometrics, and credential vaults. Integrations with third-party security and endpoint management platforms can help in enabling holistic reporting and coordinated controls that are context-aware. Additionally, direct integrations with specific applications allows secure connections to be established directly within the software. The availability and use of standard protocols and APIs is also essential to enable custom integrations with third-party solutions.

FOCUS ON PRIORITY #10: ENABLING SECURE REMOTE ACCESS ACROSS HYBRID BUSINESS NETWORKS

Pulse Secure®

EMA HAS IDENTIFIED PULSE SECURE AS A TOP 3 SOLUTION PROVIDER FOR ENABLING SECURE REMOTE ACCESS ACROSS HYBRID BUSINESS NETWORKS IN 2020

PLATFORM: Pulse Access Suite Plus/Pulse Connect Secure

ARCHITECTURE:

- Physical, virtual, or cloud appliance with high availability options
- May also be cloud-hosted on AWS, Azure, or Alibaba
- Centralized and scalable: one manager can control up to 100 appliances

KEY FEATURES:

- Extensive Secure VPN connection modes: always-on, on-demand, or only when utilizing specific applications, as well as split tunneling and multi-tunneling. Layer 2, layer 3 and layer 7 access security with broad application support
- Ensures compliance with support for MFA and SSO authenticators (e.g., SAML IdP and SD), and user and device security before and during connections
- Simplifies administration with wizards, granular policy settings, and adaptive access with built-in UEBA
- Pulse One management platform to automate appliance and policy administration while viewing an operational dashboard
- Unified Client, agent and agentless, for VPN, SDP, and NAC, as well as clientless web access portal

FOR MORE INFORMATION: https://www.pulsesecure.net/

Americas:	EMEA:	Asia Pacific / Singapore:	Japan and Korea:
Phone: +1-844-807-8573	Phone: +44-203-026-4485	Phone: +65-6716-9904	Phone: +81-3-6809-6836
Email: info@pulsesecure.net	Email: infoemea@pulsesecure.net	Email: info_apac@pulsesecure.net	Email: info_JPKR@pulsesecure.net

EMA

PULSE SECURE CASE STUDIES

EMA interviewed current Pulse Secure customers in order to gauge real world experiences with adopted technologies. Featured below are summaries of EMA's customer reviews in two relevant use cases. Customer names have been withheld to honor their requests for anonymity.

Case Study #1: An Aerospace Research and Development Laboratory

Prior to adopting Pulse Secure solutions, the organization struggled with enabling VPN capabilities and recognized it as the "number one pain point for the company." Particular challenges the organization was facing involved dealing with overly-complex management tasks, a lack of visibility into user activities, and an inability to create user specific access policies. Supporting workers who frequently travel to locations around the world addressing high-security and highly-regulated topics requires flexible access policies while ensuring elevated levels of network security. Similarly, requirements for enabling telecommuting, which have accelerated over the past few years, are driving increased needs for more dynamic remote access controls.

The company introduced the VPN features of Pulse Connect Secure as its primary remote access solution and saw immediate improvements in manageability and user satisfaction. The consistent and intuitive interface completely eliminated the need to train users and administrators on their use. Additionally, the organization adopted Pulse Policy Secure to define granular controls over which resources a user can and cannot open and utilize. In particular, the company values the role-based access capabilities which enable the development of access policies that are based on end user requirements. Exporting data into third-party platforms without the need to establish custom APIs was also determined to be easy and effective, particularly with ingesting access records into data mining tools that assist with compliance audits. As noted by the organization's principle network technician, "It just works! We just don't have any problems with this project, and if my phone isn't ringing, that's great." Since adopting the Pulse Secure solutions, the company has been able to directly quantify reduced management efforts and related cost-savings. "If we're not contently spending time and money firefighting [remote access] problems, then we can focus our attention on resolving higher priority issues."

Case Study #2: A Large Professional Services Firm

In its support of IT consulting, strategy, digital information, technology, and operations, the organization has adopted and has actively relied on Pulse Secure solutions for the past seven years. Initially, the organization adopted Pulse Connect Secure to provide more than 400,000 remote workers and outsources with secure access to business hosted IT services and resources. Often, these connections were established to enable the delivery of complication data to mobile devices and wearables (i.e., smartwatches) that often contain financially sensitive information. The most valuable features provided by Pulse Connect Secure were the ability to perform a posture check to identify the level of trust that can be placed with the endpoint. The organization was also able to leverage the platform's API to create critical integration points with a third-party multi-factor authentication (MFA) solution.

The company additionally adopted Pulse Policy Secure (Network Access Control) roughly four years ago to facilitate more powerful password checking capabilities. In particular, the business needed to ensure access to enterprise IT services was limited only to devices supported by the company and only those that met a specific security posture. Additionally, Pulse Policy Secure allowed the organization to institute role-based access which provided a much-needed level of standardization for administering user access. In particular, PPS utilizes the same Pulse Client, Pulse Secure Appliance and policy engine – as a result, existing PPS customers can realize more rapid NAC implementation and more simplified management than if they were to have different vendor solutions. Overall, the organization has been impressed with Pulse Policy Secure's reliability, ease of management, and seamless redundancy, which achieves high availability through automatic failovers. As noted by the company's security and compliance lead, "Stability is extremely important to us. If the NAC environment is compromised, we can't support our customers. We cannot afford ANY downtime."

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.

Please follow EMA on:

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

3993.070220