TEN PRIORITIES FOR ENDPOINT MANAGEMENT IN 2019

EMA Top 3 Report and Decision Guide for Enterprise

Vendor Focus: Remediant

ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) REPORT
WRITTEN BY STEVE BRASEN

Q4 2019

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

CONTENTS

INTRODUCTION

Business performance and success are dependent on the ability of a company's workforce to effectively and efficiently perform job tasks. Workforce agility and productivity accelerates when the endpoint devices they rely on—including desktops, laptops, smartphones, and tablets—operate reliabely and ituitively. Endpoint management practices and solutions are designed to ensure user devices operatate optimally and provide users with seamless access to enterprise applications, data, and IT servers from any device at any location at any time. This Enterprise Management Associates (EMA) decision guide is intended to provide actional advice on the best practices and solutions organizations should adopt for addressing today's most pressing challenges to enabling effective endpoint management.

EMA PRESENTS ITS TOP 3 AWARDS TO VENDORS THAT ARE BEST ALIGNED TO ADDRESS TODAY'S ENTERPRISE 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:

- Understanding the end-user computing forces that are shaping today's workforce performance
- Identifying the most important considerations for adopting best practices and solutions for managing endpoint devices
- Determining the Top 3 platforms available today for each recommendation

Research Methodology

All research results in this report are based on EMA's survey of 100 randomly selected North American enterprises. For each of the top ten priorities identified by survey respondents, EMA established evaluation criteria and identified a list of vendors offering viable solutions. Vendors EMA determined to provide outstanding solutions were carefully reviewed and vetted to ensure appropriate qualifications. 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 endpoint management.

2019 Top Priorities for Endpoint Management

1. End-User File Sharing
2. Endpoint Backup and Recovery
3. Identity and Access Management
4. Patch Management
5. Administrator Account Management
6. Asset and Inventory Management
7. Email and Messaging Management
8. Remote Access and Control
9. Orchestrating Digital Workspaces
10. Endpoint Detection and Response

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 has 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 they are fully addressing 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 endpoint management solution, all evaluated features and capabilities were required to conform to the following rules:

- Reported features must be generally available on or before August 31, 2019. 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 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.

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 ENDPOINT MANAGEMENT

Evolving Challenges for Endpoint Management

The average enterprise worker regularly employs more than two different devices to perform job tasks. On average, half of all business tasks are performed when workers are physically off-premises from the business, and 93% of businesses are reliant on IT services hosted on environments not controlled by the business, such as public clouds. Collectively, these converging issues are creating very complex management requirements that are taxing traditional end-to-end device management practices and, in many cases, rendering them ineffective.

Further challenging the sustainability of long-accepted endpoint management processes are accelerating requirements for security assurance and increased expectations of a more demanding workforce. Today's workers broadly expect to be able to use the devices they wish to use in the way they wish to use them while achieving instant, on-demand access to all the IT resources they require. However, satisfying these demands often introduces security vulnerabilities while increasing management efforts and related costs. In order to effectively adapt to increased requirements and environment complexes, modern businesses must adopt more dynamic and intelligent management processes and automated solutions.

Historical Context

Traditional methods of endpoint management evolved from client lifecycle management processes initially developed to support desktop PCs. These approaches principally offered device-centric functionality for operating system deployment, patching, application provisioning, security assurance, and remote access and control. Following the broad adoption of mobile devices, endpoint management solutions expanded to support a variety of different devices (PCs, laptops, desktops, smartphones, tablets, wearables, and IoT devices) and operating systems (Windows, Mac, iOS, Android, Chrome, Linux, etc.). Key vendors in this space developed unified platforms along one of two development paths—they were either PC management platforms that added features to support mobile devices, or mobile device management platforms that expanded to support PCs.

While support for user devices is still a component of endpoint management, more modern approaches focus capabilities on the secure delivery of IT services, including applications, data, email, messaging, and other resources. The primary goal for endpoint management is to ensure consistent and intuitive user experiences for users to complete job tasks from any device at any location at any time.

Addressing Endpoint Security

There can be no doubt that endpoint security is an integral component of the larger topic of endpoint management. However, EMA also recognizes that the scope of endpoint security topics and the vibrant market of supporting solutions warrant an independent evaluation. To that end, EMA prepared a companion report, titled "Ten Priorities for Endpoint Defense in 2019" covering related topics, including:

- Ransomware detection and prevention
- Malicious download detection and blocking
- Multiplatform protection (server, desktop, mobile)
- Malicious network activity detection and blocking
- Advanced persistent threat removal
- Malicious website detection and blocking
- Cloud security analysis
- Post-execution malware detection and prevention
- Full on-system security analysis
- Cloud-based security management console

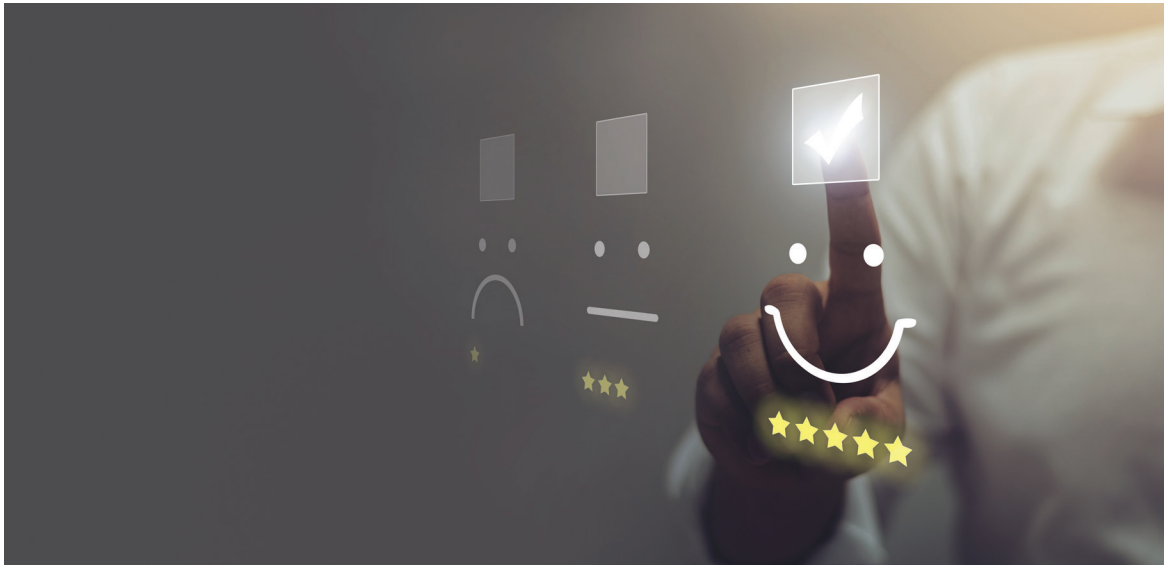
In evaluating requirements and platforms for the broader topic of endpoint management, practices and solution features that are an adjunct to (but not limited to) security practices have been considered and will be discussed in this report. However, solutions that are singularly focused on security functionally will be covered in the companion document.

UNDERSTANDING ENDPOINT MANAGEMENT

Key Disrupting Technologies for Enabling Endpoint Management in 2019

Innovative technologies that have been introduced to address endpoint management include:

- **Unified Endpoint Management** – Solutions in this category provide a single, consolidated platform for managing all enterprise-supported endpoints, including desktops, laptops, tablets, smartphones, wearables, and IoT devices. Applicable platforms also support a variety of operating systems, such as Windows, macOS, Android, iOS, Linux, UNIX, and ChromeOS. Key features of a unified endpoint management platform include a single set of user profiles, a fully integrated management console, a centralized reporting engine, and a consolidated asset management database.
- **Digital Workspaces** – By abstracting a user's work environment from underlying operating systems, digital workspace solutions create common user experiences accessible from any device at any location. Related platforms provide a centralized (typically cloud-hosted) application distribution portal and centralized security enforcement capabilities.
- **User Self-Service** – Recognizing that today's more technology-centric workforces prefer greater flexibility in how they provision and use enterprise IT services, modern endpoint management technologies minimize administrator interactions by providing automated resources for user self-service. Related solutions include web-accessible app stores, service catalogs, and interactive device configuration portals.
- **Intelligence Technologies** – User experiences can be greatly improved with the use of technologies such as analytics, machine learning, cognitive computing, and language processing, which dynamically evaluated information collected by endpoint management platforms and determine optimal responses in real time. These responses can serve to reduce user friction with accessing enterprise resources or to simplify efforts by predicting user needs.
- **Contextual Awareness** – Related solutions manage configurations, security, and service delivery based on the context of a user's activities, such as the type of user, the device in use, the physical location of the device, the conditions of the networks being accessed, and the types of applications and data being remotely served. Contextual awareness can work in conjunction with intelligence technologies or can be based on simple "if/then" automation.



OVERVIEW: TEN PRIORITIES FOR ENDPOINT MANAGEMENT IN 2019

Based on survey responses from 100 organizations, the following represent the top ten priorities for endpoint management in 2019:

1 **End-User File Sharing:**
Increased workforce mobility has accelerated requirements for the security, remote access, and distribution of enterprise files. Modern methods for file sharing must ensure security controls over business data regardless of where the files reside without inhibiting end-user productivity.

2 **Endpoint Backup and Recovery:**
Essential to modern-day disaster recovery and business continuity solutions is the centralized coordination of user data backups across multiple devices and IT services. Solutions must support granular and flexible backup processes while minimizing impacts on end-user productivity and achieving security assurance for stored data.

3 **Identity and Access Management:**
The first line of defense for protecting sensitive business resources from inappropriate use, distribution, loss, and damage is the accurate identification of users and the application of authorization policies. IT operations and security managers are continuously pressured to achieve high levels of security without introducing complex authentication processes that may reduce workforce productivity and/or user experiences.

4 **Patch Management:**
Endpoint device performance and security are dependent on the consistent and prompt distribution of software patches. However, patching processes can often be impactful to business networks and user productivity. Patch management solutions enable centralized, policy-based controls over patch distribution and installation processes.

5 **Administrator Account Management:**
Users are often granted access to privileged accounts on endpoints, introducing risks to the reliability and security of the devices. Elevated permissions should be limited to just those necessary to be performed and only for the time period they are required. Additionally, all privileged activities should be monitored to ensure accountability.

6 **Asset and Inventory Management :**
The increasing number and types of endpoint devices is challenging organizations to track and maintain detailed information on their configurations and status. Automated solutions need to be adopted that discover, record, and report on all managed devices in a support stack.

7 **Email and Messaging Management:**
Modern business communications broadly rely on the dissemination of information and files over email and other digital messaging technologies. Automated support solutions have evolved to assist organizations and their users with searching, administrating, and organizing the massive number of stored messages distributed across business servers, clouds, and endpoint devices.

8 **Remote Access and Control:**
Accelerating requirements to support remote workers on an increasing number of diverse endpoint devices is challenging administrators to consistently and quickly remediate user problems and perform management tasks. Remote access and control solutions must improve support experiences for both administrators and end users.

9 **Orchestrating Digital Workspaces:**
Expanding requirements for workforce mobility, heterogeneous device support, and distributed software ecosystems have challenged organizations to provide secure and reliable IT resources using traditional endpoint management processes. Digital workspace solutions enable consistent access to enterprise applications, data, and IT services from any device at any location.

10 **Endpoint Detection and Response:**
Risks to enterprise security and IT service performance exponentially increase the longer it takes to identify and remediate problems and threats. The rapid detection and response of endpoint issues proactively prevent breach events and impacts to user productivity.

FOCUS ON: PRIORITY #5—ADMINISTRATOR ACCOUNT MANAGEMENT

Quick Take

Users are often granted access to privileged accounts on endpoints, introducing risks to the reliability and security of the devices. Elevated permissions should be limited to just those necessary to be performed and only for the time period they are required. Additionally, all privileged activities should be monitored to ensure accountability.

Requirements and Challenges

It is not uncommon in many organizations for end users to be granted access to the administrator accounts directly on their endpoint devices or as defined in local domain access controls. In fact, EMA primary research indicates that 60% of business PC users retain privileged access to their device's administrator account.[1] Most frequently, this is permitted in order to reduce the day-to-day efforts of IT support staff while empowering workers to complete tasks quickly and independently. Unfortunately, however, users sometimes lack the knowledge to correctly address the problems that require elevated permissions to remediate. Intentional or not, changes to operating environments can significantly degrade the performance of endpoint devices or violate security requirements.

In some instances, users are granted access to administrator accounts to perform a specific set of approved tasks, such as to install authorized applications. Once granted, though, these same privileges may be misused by users to perform unauthorized tasks in order to more quickly complete job responsibilities or even non-business-related tasks. Inadvertently-enabled malware can also hijack administrator accounts, placing the entire business at risk. These occurrences are typically not monitored, providing no accountability for user errors, inappropriate actions, and security breach events. For organizations permitting non-administrators to utilize administrator privileges, it is essential that those permissions be limited to only perform authorized tasks and that all activities are continuously monitored.

Supporting Technologies

The classification of solutions designed to control, limit, and monitor the use of elevated permissions is called privileged access management (PAM). A number of PAM solutions are available that are specifically designed to manage endpoint administrator account access by applying policy-based controls to privileged activities. Users are individually and positively identified during authentication processes, and the tasks they are permitted to perform are limited to very specific activities. Some solutions may also limit the time administrator permissions are available to users. This helps ensure elevated privileges are not abused after they are no longer required. Additionally, PAM solutions that support endpoint administrator accounts will provide continuous monitoring, reporting, and alarming features to identify whether permissions are being abused or harmful tasks are being performed.

Key Considerations for Adopting a Solution

- **Heterogeneous PC support** – Solutions should manage privileged access to all PC operating environments in use in the organization, including Windows, Mac, and Linux endpoints.
- **Least privileged access** – Users should be limited to only perform the privileged activities they are authorized to perform.
- **Enforced time limits** – Access to administrator privileges should be limited to only the time periods necessary to perform approved tasks and then automatically revoked once that time period expires.
- **Session monitoring and recording** – All activities performed with administrator permissions should be meticulously collected and logged to ensure users are held accountable for their actions, any security breaches are immediately detected, and forensic information is easily accessible to speed problem remediation.
- **Third-party integrations** – Direct integrations and/or APIs should be provided to enable the solutions to connect directly with service management platforms, vulnerability scanners, SIEM tools, and endpoint management systems.

1 "Responsible User Empowerment: Enabling Privileged Access Management" 2018

FOCUS ON: PRIORITY #5—ADMINISTRATOR ACCOUNT MANAGEMENT

Remediant

EMA HAS IDENTIFIED REMEDIANT AS A TOP 3 SOLUTION PROVIDER FOR ADMINISTRATOR ACCOUNT MANAGEMENT IN 2019

PLATFORM: SecureONE	**ARCHITECTURE:** Physical or Virtual Appliance

KEY FEATURES:

- Designed to deliver agentless and vaultless PAM support across entire enterprise ecosystems and includes support for Windows, macOS, and Linux endpoints
- Allows authorized users to dynamically grant and revoke their privileged access to specific endpoints, enforcing "Just In Time" and "Just Enough" administrator right principles
- Deploys within minutes and in less than two hours will map the distribution of all privileged access across 100,000+ endpoints
- Provides continuous visibility and on-demand reporting into every administrator account on every managed endpoint

FOR MORE INFORMATION:

Web: https://www.remediant.com/secureone

Phone: 415-848-8771

Email: https://www.remediant.com/about-remediant/get-in-touch

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
Fax: +1 303.543.7687
www.enterprisemanagement.com

3905.102219