



Research


April 2018

Unified Endpoint Management in the cloud: Why it's critical to the success of your company

A.J. Gold Associates Research Report

"This report will analyze why moving to a holistic UEM approach for enterprises is required if a company wishes to remain competitive longer term. Further, it will examine the cost tradeoffs of deploying a UEM solution in an internal data center versus implementing a cloud-based SaaS solution..."





Unified Endpoint Management in the cloud: Why it's critical to the success of your company

Contents

Introduction.....	2
What is UEM?	3
<i>MDM vs. UEM</i>	<i>4</i>
Table 1: Comparison of features/functions of MDM vs. UEM	4
<i>Why should an enterprise care?.....</i>	<i>5</i>
<i>Creating unified workspaces</i>	<i>5</i>
<i>What should a unified workspace include?.....</i>	<i>6</i>
UEM – protecting against threats.....	6
<i>Enterprise must manage risk and security</i>	<i>6</i>
<i>Optimizing security</i>	<i>7</i>
<i>Is the cloud secure?.....</i>	<i>7</i>
<i>The cost of a data breach.....</i>	<i>7</i>
Think access and productivity – not management and security	8
<i>Future-proofing.....</i>	<i>8</i>
<i>Agility and flexibility.....</i>	<i>8</i>
<i>Selecting a cloud-based UEM – some key attributes</i>	<i>9</i>
The important role of analytics.....	9
Cost and deployment mode	10
Table 2: Cost of on-premises vs. SaaS UEM over 3 years	10
Conclusions.....	11
Recommendations	11
Appendix	12
Table 3: Cost of on-premises UEM per user.....	12



Unified Endpoint Management in the cloud: Why it's critical to the success of your company

Introduction

We are rapidly entering a market phase where users no longer are assigned company-defined standard devices necessary for access to corporate systems. Indeed, it's now been many years since the majority of enterprise employees used only a company-supplied, PC-based solution to meet their computing needs. The advancement of mobile devices over the past decade, with powerful processors, high-speed networks, and intuitive user interfaces, and especially driven by the Bring Your Own Device movement, transformed the way companies enabled access to corporate systems so employees could get their work done in a timely and convenient fashion.

The early stages of this change required that companies put in place infrastructure that could manage these devices, often as a result of reacting to a growing installed base rather than implementation of a strategic plan. Early deployments of basic Mobile Device Management (MDM) enabled limited management of users' smartphones (e.g., asset management, application inventory, device "kill" if lost, etc.). Over time, a more holistic view of mobility brought about the implementation of Enterprise Mobility Management (EMM) with enhanced policy setting and security capabilities, application "hardening" for enterprise use, and user support functions.

However, both MDM and EMM systems were primarily targeted at users of mobile devices, and therefore did not unify the necessary management of all employee access devices. Further, they did not "rationalize" the enablement of universal access to virtually any corporate app from any device. Nor did they provide a unified user workspace that brings together a managed environment for enterprise apps while protecting company data from leaking outside of the corporate boundaries, which is a growing threat. As a result, a complete management solution required multiple applications/infrastructure solutions running simultaneously within the IT infrastructure environment.

Recently, the market has shifted toward a Unified Endpoint Management (UEM) approach that encompasses enhanced services for all devices, not just mobile devices, and includes the ability to uniformly set policies and offer enterprise application access no matter which types of devices are being used by the employee at that particular time.

TREND: *Within 3-4 years, we expect 75%-85% of enterprises to have a majority of workers access corporate systems from at least 3-5 different endpoints, and not just the current traditional ones like PCs, smartphones, and tablets. Indeed, as new Enterprise of Things devices become prevalent (e.g., autonomous vehicles, specialty machines, embedded intelligent systems smart personal devices), many with significant compute and user interface capabilities, enterprise users will demand access from any device, at any time, through multiple interfaces (e.g., voice, video, AR/VR), and over any connection. It will become increasingly impossible to have uniformly consistent management, security, and user profile capability by installing a unique software component on each device. The only way companies can accomplish this will be through cloud-based Unified Endpoint Management. Companies not effectively managing this transition will become noncompetitive through user disenfranchisement, lower employee productivity, and increased infrastructure costs.*

J.Gold Associates LLC.



Unified Endpoint Management in the cloud: Why it's critical to the success of your company

Despite the benefits, it has been a struggle for many companies to move to the more encompassing UEM model, as many early implementers of MDM and EMM solutions chose to install a management solution running on the company's own servers and supported and managed by the IT department. Implementing a UEM solution that is on premises is a costly and often difficult thing to do, and it severely restricts the agility necessary to cope with the rapidly changing landscape of access devices and the new user requirements emerging in the next 2-3 years. Further, since there is often a substantial lag in a company's ability to implement the "latest and greatest" versions of UEM, many on-premises implementations lag significantly behind in features/functions of the latest versions, which can cause management and security challenges

This report will analyze why moving to a holistic UEM approach for enterprises is required if a company wishes to remain competitive longer term. Further, it will examine the cost tradeoffs of deploying a UEM solution in an internal data center versus implementing a cloud-based SaaS solution, including some of the inherent limitations of an on-premises approach. And finally, it will examine some of the "soft costs" associated with not being able to quickly adapt to a changing landscape, which will be dramatically altered by new access points emerging in the next 2-3 years. This change will make the previous wave of web access and mobile access devices look tame by comparison.

What is UEM?

Most companies are rapidly expanding the numbers and types of computing platforms they have installed. Ten years ago, the number of corporate-sponsored endpoints for the majority of users was one – a PC. But currently we estimate that the average corporate user has at least 3 endpoint devices they use on a regular basis – often a company-provided PC, a smartphone, an alternative like a tablet, and/or a privately owned PC or publicly available one. With the plethora of new device types that will need corporate access in the near future, it's imperative that companies are able to control all endpoints — and even servers and cloud-based services — from a single consolidated platform that can set policies and control security access uniformly across all devices, apps, and users. Therefore, the ultimate goal of any UEM deployment should be a single management console that provides uniform command and control of the entire computing infrastructure in the enterprise through a unified directory system and with connections to all existing corporate control mechanisms and apps.

"Ten years ago, the number of corporate-sponsored endpoints for the majority of users was one – a PC. But currently we estimate that the average corporate user has at least 3 endpoint devices they use on a regular basis – often a company-provided PC, a smartphone, an alternative like a tablet, and/or a privately owned PC or publicly available one."

Many current attempts at UEM have resulted in only partial success. Vendor-specific implementations like Microsoft's System Center attempt to extend their "management umbrella" to include a variety of non-Microsoft platforms, like iOS, Android, Chrome, etc. But



**Unified Endpoint Management in the cloud:
Why it's critical to the success of your company**

generally, platform vendors (including Google and Apple) who have a vested interest in providing superior functions on their own platforms fail to fully implement equality of functions across all platforms. In most situations where a variety of diverse platforms need to be managed, third-party solutions do a better job of creating an equal playing field across all platforms (although, it can be argued that since they control their own APIs, OS vendors probably do a better job of management and control within their own ecosystem).

MDM vs. UEM

While many companies have installed an MDM system to manage mobile devices, far fewer have deployed UEM as a necessary component of their management and security infrastructure. Table 1 indicates and values some of the major distinctions between traditional MDM and UEM product capabilities.

Table 1: Comparison of Features/Functions of MDM vs. UEM

Features/Functions	MDM	UEM
Device Asset Management (inventory, configuration, device wipe, password set, OS updates)	+++	+++
Multi device/OS support (unified tools for all smartphones, tablets, PCs, etc., with path to new devices/types)	++	+++
Provisioning/Policy enforcement (configurations, encryption, device components enabled (camera, etc.), enrollment, network access, VPN)	++	+++
Application Management (app deployment and monitoring, containerization, protected space enablement, updates)	++	+++
Security management (data isolation, device encryption, secured browsing, secured email/productivity, Multifactor authentication/Single sign on, LDAP/AD directory interface)	+	+++
Workspace management (file sync and share, VDI, secured email client, secured browser)	-	++
Support services (remote device access, self service portals, dashboards, help desk access)	+	++
Secure Network Access (VPN, enhanced networking access)	+	+++
Workspace Analytics –Performance (monitoring apps/users, identifying bottlenecks, performance alerting)	-	++
Workspace Analytics – Security (monitoring activities for anomalous behaviors, enhanced security enforcement, remediation)	-	++



Unified Endpoint Management in the cloud: Why it's critical to the success of your company

Why should an enterprise care?

It's currently common practice for enterprises to have at least 2 and sometimes as many as 5-6 different management tools deployed in their IT infrastructure. We estimate that most organizations have "siloe" tools for managing either by OS or by device type (e.g., PC vs. mobile). This is a very inefficient method to manage what should be combined into a unified structure. It requires that IT staff have high levels of expertise in more than one system, which is a resource challenge. Further, it requires the company buy licenses from more than one vendor, which means spending more per user on a duplication of products. Finally, it requires that companies rely on multiple vendors to provide updates and support, and as such, they receive varying capabilities on different upgrade cycles with different deployment schedules. As a result, it's not uncommon for companies to have to perform a series of upgrades/maintenance on their incompatible solutions, causing potential management and security "holes" in their systems, and causing a near-continuous upgrade cycle.

"It's currently common practice for enterprises to have at least 2 and sometimes as many as 5-6 different management tools deployed. Indeed, we estimate that most organizations have "siloe" tools for managing either by OS, or by device type (e.g., PC vs. mobile)."

Creating unified workspaces

A key benefit of moving to a UEM model is that users can have personalized profiles, enabling each user to be configured with a unified, enterprise-class, secured workspace to run corporate apps, do secure web browsing, securely communicate and collaborate with colleagues, etc. Each user has a unique profile assigned to him/her that enables complete corporate management and security policy implementation. Further, a unified and secured workspace for employees ensures that universal access from any device is available. With a uniform access interface, companies no longer need to worry about obtaining and employing unique workspaces for individual users and/or platforms.

Including unified workspaces as a key component of UEM provides companies with a way to fully deploy corporate apps to any user on any device without having to define specific apps for specific platforms. As a result, users are more productive because they no longer need to be concerned if they have the right apps installed on their current device of choice. Enterprises have far more flexibility as IT departments no longer need to create unique applications for various device types. This creates a significant cost savings to the organization, as well as preserves scarce IT resources that can be deployed to more strategic initiatives than cross-platform enablement.

TREND *"Follow-me-everywhere productivity requires that users are able to access enterprise assets not only from various locations, but also on various device classes and types. We estimate that the average worker in the next 2-3 years will be spending more than 50% of their time accessing corporate information from non-traditional devices (e.g., PCs, smartphones) and that the companies that can provide access will increase users' productivity from 10% to 25%. UEM will be a required technology to enable this."*

J.Gold Associates LLC.

What should a unified workspace include?

Enterprises need to evaluate user needs and determine what features/functions are most appropriate. But at a minimum, we recommend the following features/functions:

- *A universal policy-setting capability for each user, no matter the device or connection*
- *A secure workspace providing secure access to corporate apps and data*
- *A protected storage area to keep corporate data safe*
- *An ability to modify user access profiles based on specific device capabilities*
- *A protected/secure browsing capability*
- *A secure messaging/collaboration capability*
- *An interface that's familiar to the user based on preferred device*
- *An optimized analytics capability that can monitor and inform the organization of any anomalies and take appropriate actions*
- *Analytics based on user behavior to reduce risk and improve application performance*
- *Secure network access that enables single sign-on (SSO)*

While all of these capabilities should be available in any system that a company selects, it's important to note that not all of the capabilities need to be rolled out at once. The most effective systems provide for an "à la carte" capability that can be tailored to suit the needs of the organization and can easily add or subtract capabilities as needed. This provides companies with the maximum flexibility needed to operate in a rapidly changing environment.

UEM - protecting against threats

UEM not only improves overall user and device management, but it also has a major benefit in enhancing corporate security. We estimate that companies that deploy stronger device management and security oversight through enterprise-class UEM cloud-based services are 25%-35% less likely to have a security breach. According to the Ponemon Institute 2015 Cost of Data Breach Study, the average consolidated total cost of a data breach

"We estimate that companies that deploy stronger device management and security oversight through enterprise-class UEM cloud-based services are 25%-35% less likely to have a security breach."

is \$3.8 million. Verizon's 2015 Data Breach Investigation Report says approximately 45% of threat actions were credential thefts, while Trustwave in its 2015 Global Security Report indicated that in the breaches it investigated, 28% resulted from weak passwords and another 28% from weak remote access security. This data emphasizes the need for enhanced security and why enforced policies and active monitoring and remediation are mission-critical. This is why UEM has placed so much emphasis in these areas.

Enterprise must manage risk and security

With so many ways to have a data breach, companies must focus on better management of risk. Some key questions organizations must ask, especially when evaluating a potential UEM deployment, include:



Unified Endpoint Management in the cloud: Why it's critical to the success of your company

- *What does security mean in a world of multiple access devices?*
- *How can security be equalized across inherently different devices?*
- *Does backend monitoring and intelligence take over from on-device monitors?*
- *How do we best create uniform profiles, compliance, and cross-boundary enforcement?*
- *How do we best enforce universal policies for any-user, any-device, anytime access?*

These high-level concerns should be at the heart of security and risk assessment when looking at potential UEM deployments.

Optimizing security

With so many malware attacks and exploits, and with so many high-profile data breaches exposing hundreds of thousands to millions of records, companies can ill afford to do business as usual. Multifactor authentication, verified single sign-on, analytics, and behavioral analysis all contribute to making companies safer. A well-structured UEM program will dramatically decrease the potential data loss from malware and breaches, and will ultimately save the organization many times the cost of the UEM deployment. However, since most companies are ill equipped to create their own internal bulwark built on UEM, the best way to deploy is in a cloud-based SaaS model where vendors spend much greater resources on security than an individual enterprise could.

Is the cloud secure?

In the recent past, many enterprises viewed cloud-based services' security as questionable when compared to their own controlled data center environment. However, in the majority of cases, we estimate that cloud-based security actually exceeds corporate on-premises solutions by a significant margin. The amount of resources applied by the average organization to secure their internal infrastructure is generally orders of magnitude less than the cloud service providers expend to ensure their safety and security. Further, amortized over many more users, the amount of data gathered and analyzed for actionable intelligence is far more likely to create an effective early barrier to new infections than could an individual company. Finally, while most cloud-based SaaS includes the cost of security in their per-user charges, the average enterprise with on-premises solutions has to expend significant time and cost to make sure all of its infrastructure is secure, which often can be substantially more than the overall SaaS cost per user.

The cost of a data breach

There are various estimates as to what a data breach costs a company. The Ponemon Institute 2015 Cost of Data Breach Study estimates \$142 per exposed record. The Verizon 2015 Data Breach Investigations Report loss per record estimates vary widely based on the number of records lost and size of company, with 1K

"Our research indicates that almost one-third of companies know they have had a data breach, and it's likely an equal number have had a data breach without knowing it."



Unified Endpoint Management in the cloud: Why it's critical to the success of your company

records expected to cost a company \$67,000 (but could be as high as \$1.5M) and a loss of 100K records expected to cost a company \$475K (but could be as high as \$10M).

The loss estimates vary from different sources, but even the conservative estimates are substantial. Our research indicates that almost one-third of companies know they have had a data breach, and it's likely an equal number have had a data breach without knowing it. And the predominant way for hackers to get data is through credential theft. Organizations should look at a high-quality UEM solution as a way to substantially mitigate risk.

Think access and productivity – not management and security

Most management and control systems are designed to limit access so as to minimize exposure to “bad actions.” Indeed, a favorite security control mechanism is to limit the amount of data an employee can access, even if it means getting in the way of that employee being maximally productive. The problem with this approach is that it's self-defeating from two perspectives: first, if users feel hindered in any way in getting their work done, they will find a way to work around it, and second, if you are hampering productivity, you are also costing the company money in terms of reduced employee productivity. So companies looking at implementing a UEM approach should be asking not just how much control the system offers, but how it can ultimately lead to making the organization more productive and making it less restrictive for users to get their jobs done while also protecting the corporate assets.

Future-proofing

Proper workspace designs in a UEM implementation also have the advantage of offering access via next-generation access points and user interfaces. New interfaces like voice and video, AR/VR, and biometrically activated access will have to be individually installed into each corporate app if companies are to keep up with the rapid pace of newer devices. Yet a well-designed UEM workspace approach means that these access methods can become part of the solution much earlier than they could as individual efforts in companies and often don't require a full rework of the apps — instead adding a user interface layer on top of the solutions. This allows the organization to rapidly include new access features while essentially “outsourcing” such feature creation to the UEM/workspace vendor of choice.

Agility and flexibility

We estimate that the time lag to fully implement on-premises upgrades for new UEM system releases and upgrades is 6-12 months at a minimum. During this time, it's likely that the internal components will be substantially behind in capabilities of those available in the cloud as a SaaS offering. Further, the expertise

“We estimate that the time lag to fully implement on-premises upgrades for new UEM system releases and upgrades is 6-12 months at a minimum.”



Unified Endpoint Management in the cloud: Why it's critical to the success of your company

and resources needed to upgrade the internal systems will mean a significant delay in potentially more strategic IT initiatives.

Companies investing in cloud-based UEM solutions are able to rapidly implement new technology capabilities on an as-needed basis without expending substantial amounts of internal resources to install, configure, and manage infrastructure. The savings in manpower and infrastructure costs makes SaaS a very attractive option for most enterprises.

Selecting a cloud-based UEM – some key attributes

We recommend that enterprises evaluating cloud-based UEM solutions look at the following key attributes and assess if products being evaluated will meet the organization's needs.

- Available across a variety of cloud platforms (e.g., AWS, Microsoft Azure, Google Cloud)
- Multi-cloud platform operation (e.g., single view into multiple dispersed/different cloud operations)
- Integration with corporate apps to ensure all management functions available
- Integration with corporate directory services for user profiles, access, etc.
- Common policy enforcement mechanisms across all apps from a single interface
- Unified content storage enablement across multiple repositories (e.g., Box, OneDrive, Dropbox, Google Drive, ShareFile)
- Cross-platform integrated identity and access management (e.g., SAML, SSO, Kerberos)
- Single management view across all platforms/devices/apps/infrastructure assets
- Support enablement through easy-to-navigate analytics
- Ability to easily extend new end user services as they become available/necessary

The important role of analytics

Modern-day UEM systems not only allow administrators to set policies and initiate various device operations, but importantly provide an active monitoring capability that aggregates data from the devices, apps, networks, and potentially additional external data for analysis. While early systems did this primarily for informational purposes, next-generation systems not only gather the data, but analyze it for actionable intelligence that allows the organization to quickly act and take remedial actions as required by real-time events. Such capability can only be made available within the UEM system if there is a fully instrumented capability that monitors and analyzes all of the transactions, user interactions, and external events against established corporate policies. Not only is actionable intelligence through analytics being included in next-generation systems, but within the next 1-2 years, we expect virtually all enterprise-class UEM solutions to include a machine learning/artificial intelligence engine under the covers that will elevate the actionable intelligence level even further. The ability to be proactive rather than reactive is a major advance in limiting security breaches.

“Indeed, not only is actionable intelligence through analytics being included in next generation systems, but within the next 1-2 years, we expect virtually all enterprise-class UEM solutions to include a machine learning/artificial intelligence engine under the covers that will elevate the actionable intelligence level even further.”



Unified Endpoint Management in the cloud: Why it's critical to the success of your company

Cloud-based systems have an advantage by securely and anonymously capturing data from multiple firms. By amplifying the number of users, the level of actionable intelligence will grow dramatically, and this can't be accomplished effectively by employing AI in an on-premises installation. It's therefore important to evaluate any UEM solution not only on how it analyzes local data, but also what capabilities it has to aggregate data from multiple sources to increase the level of security and anomaly detection. Those UEM vendors that do not provide such capability do not offer the most capable systems and will become noncompetitive in the marketplace.

Cost and deployment mode

Some have suggested in the past that having an on-premises solution is more cost effective than paying for a continuous service in a cloud-based SaaS model. But that is not the case. The CapEx vs OpEx argument often is based on old data or "intuition" rather than reality. Our analysis shows that it's less expensive to deploy UEM on a SaaS, per user per year model, when taking into account all the various costs that contribute, but are often hidden, in deploying a product in a corporate data center. Our 3-year analysis shows that for a 2,000-employee organization, companies can save approximately \$98 per user, or \$196,000, in a SaaS deployment. Further, IT resources are extremely scarce in most organizations, and this path frees that resource. Finally, SaaS solutions get updated immediately and eliminate the 6-12 month lag typical for upgrades on premises, thus eliminating potential security risks much more quickly.

"Our 3-year analysis shows that for a 2,000-employee organization, companies can save approximately \$98 per user, or \$196,000, using SaaS."

Table 2: Cost of on premises vs. SaaS UEM over 3 years

	Year 1	Year 2	Year 3
Cost per user, per year on premises	\$240	\$49	\$49
UEM SaaS cost per user, per year	\$80	\$80	\$80
Cost savings	\$160	-\$31	-\$31
3-year SaaS savings per user	\$98		

See appendix for a complete analysis showing assumptions and costs.



Unified Endpoint Management in the cloud: Why it's critical to the success of your company

Conclusions

Our analysis has shown that when done properly, a SaaS-based implementation of UEM and the inherent advantages of well-regulated and secured workspaces is accomplished far more effectively and with less cost than when done internally on premises. Enterprises should be evaluating and/or migrating to a UEM solution that is cloud-based and feature-rich, and avoid the necessary additional cost, resource constraints, and time lag associated with maintaining an on-premises UEM solution.

Recommendations:

We recommend that enterprises take the following actions:

- Look at the total device/access picture, not just current needs. There is no doubt that those needs will expand over the next 2-3 years as new devices/access points emerge. Organizations should choose a solution that can be easily expanded to meet those needs without having to “rip and replace.”
- UEM solutions should be seen as strategic, not just tactical as many MDM solutions were in the past. As a result, enterprise-class solutions should be deployed as part of an overall managed security strategy compatible with corporate goals and not as an independent solution.
- Even if you can't immediately deploy a full workspaces solution, choose a UEM product that can be easily upgraded to future-proof your user and corporate needs.
- Capable UEM solutions are most readily adopted and deployed when they are in a cloud-based SaaS model. This is the way for organizations to maximize limited IT resources, ensure the most up-to-date features/functions, and implement the lowest-cost alternative.
- A UEM cloud-based solution should be part of an entire workspace that can be delivered in the cloud and provide users access to all their corporate applications and data.
- Select a vendor you're confident will be able to continuously improve and expand its UEM products. Further, select a partner, not just a vendor — it's imperative that you can rely on the vendor to improve your overall business and user productivity, and not just offer a product. Strategic vision is critical!

We strongly believe that those companies that do not implement a strategic UEM program over the next 1-2 years will be noncompetitive longer term, as user productivity, IT resources, and business flexibility will all be compromised. Enterprises must act now to implement a UEM capability.

This research report is distributed with permission by Citrix. No other parties are authorized to copy, post and/or redistribute this research in part or in whole without the written permission of the copyright holder, J.Gold Associates, LLC.

Appendix

Table 3: Cost of on-premises UEM per user

On-premises UEM cost (3-year total)			
	Year 1	Year 2	Year 3
General server cost			
Cost of server hardware	\$8,500		
Cost to maintain server (20%)	\$1,700	\$1,700	\$1,700
Cost of OS	\$3,000		
Cost of OS maintenance (15%)	\$450	\$450	\$450
IT labor costs (assume 2 hrs/mo at \$60 per hr)	\$1,440	\$1,440	\$1,440
Electricity - assume 500W, .10/KWH)	\$438	\$438	\$438
Networking costs (assume 15% of HW/SW cost)	\$2,048	\$323	\$323
Storage cost (assume 10TB RAID, \$1/GB)	\$10,000		
Storage maintenance (assume 15%)	\$1,500	\$1,500	\$1,500
UEM software:			
UEM license cost (assume 2K users, \$180/user)	\$360,000		
SW maintenance (assume 25%)	\$90,000	\$90,000	\$90,000
SW upgrades (assume 2 at 8 hrs IT/yr, \$60/hr)	\$960	\$960	\$960
Backups/restores (assume 1hr IT/mo)	\$720	\$720	\$720
Total	\$480,756	\$97,531	\$97,531
Cost per user, per year	\$240	\$49	\$49
Estimated UEM SaaS cost per user, per year	\$80	\$80	\$80
Cost savings	\$160	-\$31	-\$31
3-year SaaS savings per user	\$98		

About J.Gold Associates

J.Gold Associates provides insightful, meaningful and actionable analysis of trends and opportunities in the computer and technology industries. We offer a broad based knowledge of the technology landscape, and bring that expertise to bear in our work. J.Gold Associates provides strategic consulting, syndicated research and advisory services, and in-context analysis to help its clients make important technology choices and to enable improved product deployment decisions and go to market strategies.



J.Gold Associates, LLC
6 Valentine Road
Northborough, MA 01532 USA
+1 508 393 5294
www.jgoldassociates.com