Deep Analysis

Custom Research

Why On-Premises IT Is Riskier Than the Cloud

By: Alan Pelz-Sharpe

Executive Summary

In the last 30 years, legal documents have moved from being entirely paper-based to mostly digital. Legal firms have invested in hiring, buying, and building their own on-premises IT systems to handle these digital documents; these have worked well and, in many cases, continue to do so.

Many legal IT departments have refrained from leveraging cloud solutions for document sharing and workflow even as this has become the norm in business. Some in the legal sector believe cloud computing is riskier than running technology on their own premises; interestingly, this reluctance comes mainly from partners and management and not from IT departments.

There are good reasons for legal firms to consider moving to cloud-based systems. The pandemic and the associated increased security risks of retaining on-premises IT have led to a dramatic increase in moving to the cloud and in benefits to law firms large and small. The fact is that IT operations continue to expand to meet the needs of an increasingly complex ecosystem, and midsize to large law firms require more than a few back-office servers and one or two IT professionals. In-house IT staff must manage a range of on-premises and cloud applications, ensuring the uptime, security, and availability of structured and unstructured data, and deal with a growing shadow IT situation. Moving to the cloud for these IT professionals is less a threat than it is an opportunity to take control of, and improve, the working environment for all the firm's staff.

Ultimately, managing highly sensitive and confidential legal documents and data within a law firm is inherently risky. Moving to the cloud may come with some risk, but this paper argues that continuing with an on-premises IT system is much riskier.

This report was commissioned by iManage and prepared by Deep Analysis.

 © 2021 | info@deep-analysis.net

A Changed Working Environment

This past year has been one of the most disruptive in living memory. The enforced shift to remote and hybrid working has been hard on everyone, not least the legal sector.

From deal-making through billing to the courtroom, historic working patterns have been upended. Lawyers and legal staff were forced to work from home and set up safe and productive environments in spare bedrooms, basements, and closets. Courtrooms scrambled to continue work online.

Now, as the world slowly returns to normalcy, it is becoming clear that we will be returning to a changed working environment, replete with new expectations, risks, and possibilities. Though many have returned to the office to work daily, the recent upending of working norms will have an enduring impact on the way we structure legal workplaces and practices. And with that change comes a greater reliance on electronic adjudication and interaction, and a resulting increase in exposure to risk in the form of data loss, cyber threats, non-compliance, and the unintended disclosure of confidential client information.

The challenge, then, is to address the need to support remote working practices and access to information while managing the increased inherent risk. Though there may be a desire to return to traditional on-premises working practices, leveraging standard on-premises technology is no longer a realistic or defensible strategy. Conventional working practices are already disrupted, and as such, it's wishful thinking to try to turn back the clock to a pre-COVID era. Moreover, many legal firms that resist moving to the cloud may find that on closer inspection, much of the work their staff undertakes is already running in the cloud.

Though it may seem insensitive to draw positives from the pandemic, the fact is that this period of disruption has triggered explosive change in the technology sector. Legal, healthcare, and government organizations running aging IT systems have been given an opportunity to leapfrog and to drastically modernize IT and working practices. Virtually all the technology vendors in the markets that Deep Analysis researches have reported significant changes in their customer buying patterns. Unsurprisingly, sales of collaboration,

Though there may be a desire to return to traditional on-premises working practices, leveraging standard on-premises technology is no longer a realistic or defensible strategy.

© 2021 | info@deep-analysis.net

video conferencing, and secure messaging systems skyrocketed during the pandemic. But more interestingly, the fairly standard 3-5-year timeline many firms had to digitally transform their IT operations has in many cases been accelerated and restructured to complete the same work within the next 18-24 months.

If your teams are using messaging, file sharing, collaboration, or email services, then they are likely already sharing sensitive information in the cloud. Many of your employees may already be using Box, Dropbox, or Google Drive, for example. But we do not advocate for any law firm to simply lift and shift all their sensitive information and case files to a consumer-oriented cloud-based service. Law firms should take a considered approach to selecting the right services to meet their specific needs. Some of legal firms' past reluctance to move to the cloud is well-grounded. Not all cloud systems and services are equal, and few can meet the precise requirements of legal firms.

What is Cloud Computing?

The term "cloud computing" is a catch-all phrase that covers many different approaches to computing. It is a common term that has no common definition. At Deep Analysis, we define cloud computing as:

"The use of remote servers networked together on the internet to store, process, and manage data."

For a non-technical person, that may not be a helpful definition. But the key is understanding that cloud computing equates to shared services linked together via the internet. You can share multiple data centers, security services, applications, and, by default, large, dedicated, and specialized teams of IT professionals. Those remote IT professionals ensure that systems are running well and that they are secure and maintained 24/7. Cloud services can be global in scale, generic, and publicly accessible; for example, think of Amazon, Google, or Microsoft. On the other hand, they could be small, highly specialized, and private.

The term "cloud" itself is misleading. Clouds are amorphous and easy to penetrate. Cloud computing services, on the other hand, are solid and difficult to penetrate. It's semantic wordplay, but one has to wonder if a different term had been used whether more people would trust the concept.

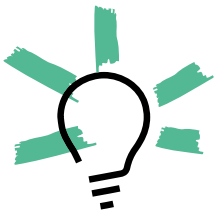
Cloud Computing for Legal – What to Keep in Mind

This section outlines key considerations regarding cloud computing for legal data and files: reducing risk and increasing productivity, keeping control of data and how it is shared, and cost.

Reducing risk and increasing productivity

Law firms often say things like "running on-premises IT is more secure than keeping documents in the cloud." This commonly held belief makes law firms reluctant to move to the cloud. However, though on-premises IT may be made secure, there is nothing to support the view that the cloud is less secure. In fact, there is plenty of available evidence to suggest that the cloud is inherently *more* secure than on-premises IT.

Cloud providers support operational and security certifications like ISO 27001 that go far above and beyond what most on-premises systems possess. Indeed, very few law firms would be able to secure data to the compliance levels required of regulations such as ISO 27001, HIPAA, SAS 70 Type II, or NIST 800-53, whereas it is normal to do so in enterprise cloud computing environments. Few, if any, law firms secure their data to such a high degree (see Figure 1). Furthermore, it is well documented that legal firms' clients highly value such a level of security. According to the ABA, 27% of lawyers see "better security than I can provide in-office" as a benefit of cloud computing.

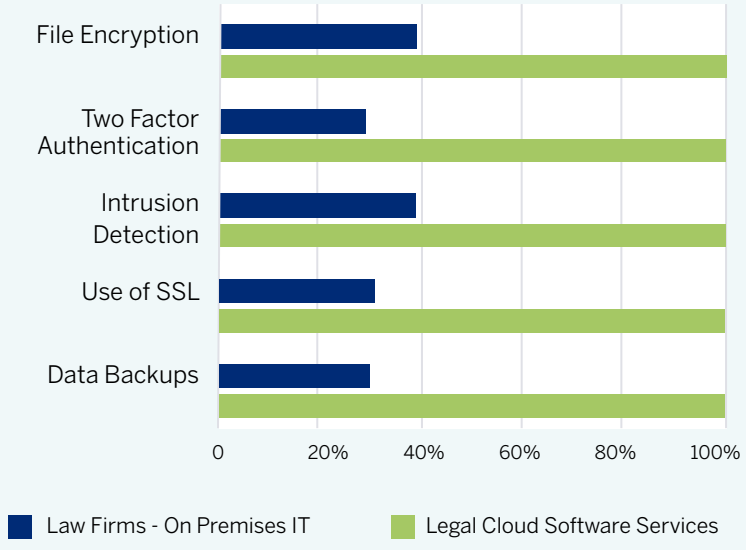


27% of lawyers see "better security than I can provide in-office" as a benefit of cloud computing.

-American Bar Association

Figure 1

Law Firm On-Premises versus Cloud



Source: American Bar Association

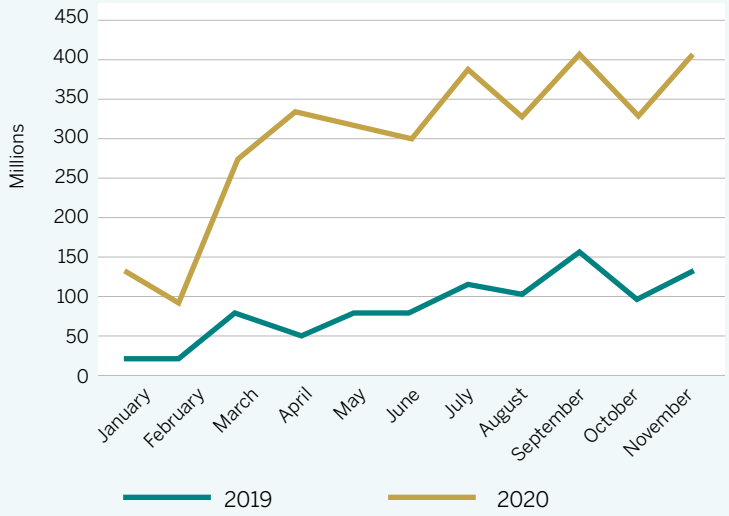
In short, the belief that on-premises systems are more secure is based on perception rather than evidence. The vast majority of law firms apply much weaker and, in some cases, little security to their data and applications. Therefore, the perception that "my" data is inherently more secure if it is situated within "my" building does not stand up to scrutiny. Additionally, we should note a fundamental principle of data security, that the relative "accessibility" of the data, rather than its physical location, has the most significant impact on its actual security.

Of all the objections regarding moving to the cloud, concern about security is, in our analysis, by far the weakest and most difficult to justify. And, in an emerging post-COVID world, the need to move to more secure data and file systems is reaching a critical inflection point. Cyberattacks increased by 60% year over year in 2020, a leap that correlates directly with the increase in employees suddenly working from home. Worse still, cyberattacks are becoming more sophisticated as ransomware attacks are on the rise, with legal firms becoming a particular target for cyber criminals (see Figure 2). In April 2021, the Coveware Quarterly Ransomware Report stated:

> "*The most notable change in industries impacted by ransomware attacks in Q1 was the Professional Services industry, specifically law firms. Small and medium sized law firms continue to succumb to encryption ransomware and data exfiltration extortion attacks. Unfortunately, the economics of many small professional service firms do not encourage or enable adequate cyber security*."
>
> Source: *Slaw* Magazine

Figure 2

Ransomware Attack Growth 2019-2020



Source: Business Wire

To repeat, the security of data and files relates directly to their accessibility, not their location. Newly home-based and remote workers attempting to access on-premises files and data, or just as often attempting to find workarounds, are now the prime threat to your data security. Your staff are not cybersecurity experts, nor should they need to be; rather, they should be given access to highly secure applications to mitigate this risk. Your staff will always be the weakest link in your security chain, and expecting them to operate safely and securely in a remote fashion with on-premises technology that was never designed to support this new work environment is unrealistic.

Cloud service providers engineer every aspect of their services to be highly secure, and their teams work 24/7 to keep them secure. Their systems are designed to meet the most extreme security and compliance needs. Most on-premises IT departments do not, and never will, have the time, skills, or resources to do that. Instead, on-premises teams are limited to focusing on the security basics of managing a firewall and restricting access to information via permission sets.

Most, though not all, cloud service providers encrypt data both in flight and at rest with 2048-bit PKI Certification. In other words, your data is always encrypted, unintelligible, and inaccessible unless you, the customer and sole key-holder, unlock it. Cloud data may well be stored on a third-party cloud storage system, but no third party can unencrypt the data and read it. Only you can do that.

Moving to the cloud will make your data much more secure than it is today. However, as you will have noted, you must undertake due diligence on potential cloud service providers to ensure they truly meet these high security standards: that they fully encrypt the data, cannot access it, and have engineered and certified their system to be fully compliant with the strictest of standards. Some lower-cost or more generic consumer-based cloud services may not want to encrypt your data while at rest, or to meet such high standards. That is the risk you run with lower-cost commodity services; they are cheap for a reason. Specialist enterprise-grade cloud services that sell to regulated and compliant sectors such as legal, healthcare, and government typically do meet these standards. Indeed, as premium services they pride themselves on their security and encryption capabilities.

Today's enterprise-grade cloud solutions are more secure than on-premises systems, and as cyberthreats and ransomware attacks increase rapidly, the need to move to the cloud also increases. *At Deep Analysis, we go further and believe strongly that continuing to store your files and data on-premises is becoming an unacceptable and indefensible risk.*

Today's enterprise-grade cloud solutions are more secure than on-premises systems, and as cyberthreats and ransomware attacks increase rapidly, the need to move to the cloud also increases.

© 2021 | info@deep-analysis.net

Keeping control of data and how it is shared

Closely related to cloud security concerns are concerns regarding the risk associated with entrusting client data to third parties. Again, we hear a common refrain along the following lines: "I cannot trust my clients' confidential data to a third party, nor will I allow my team to access sensitive information outside of our firm's four walls – the risk of something going wrong is too high."

Letting confidential data wander outside the control of your four walls is rightly a major concern, but we need to do a reality check and recognize that this is almost certainly already happening. Your staff members email files and/or save files to zip drives or third-party cloud storage systems like Google, Dropbox, Box, etc. The challenge, then, is not so much in stopping third parties from storing data or allowing remote access to that data, but in controlling how this happens.

There are two concerns to consider here: entrusting data to third-party vendors, and remote access by clients and staff to files and data.

1. **Entrusting your files and data to a third party**

   There is nothing illegal about using a third-party service for storing your files and data. However, you and your third-party vendor do need to follow common sense rules and procedures. In the US, only some states have clear guidelines for the use of cloud services. Those that do not have clear guidelines do not prohibit the use of cloud services. Some jurisdictions in Europe and Asia also have guidelines regarding the use of the cloud.

   But whether guidelines exist or not, in every single case it is a simple matter of following common sense "reasonable care" rules and procedures. For example, you need to know how your cloud service provider handles the storage and security of your data, that they meet acceptable service level agreements (SLAs), and that they follow reasonable and sound security practices. You also need to ensure that your ownership and access to the data cannot be restricted, that the data is backed up and stored in a native format, etc. All of these should be simple checkboxes for an enterprise cloud service provider to mark off except the last one, storing in a native format.

   Legal files and data must be treated as "records" – for certain documents, modifying the format or deleting or changing any associated metadata

is not permitted. This is because any change made to the file by reformatting or deconstructing it for more efficient storage effectively brings its authenticity into question. That is more an issue for legal firms than for many other enterprises using cloud services. Again, you need to check that your cloud service provider has configured its system to meet that specific requirement.

2. **Remote access to files and data**

   Historically, when firms have stored their files and data on-premises, they have provided virtual private networks (VPNs) for the staff to secure remote access. Many law firms believe that by ensuring employees use a VPN they will keep sensitive client data secure. Ten years ago, this was the only effective means of adding some security to remote access, but today internally managed VPNs are often dated, clunky to use, and at worst a security risk. Although they claim to offer full anonymity and encryption, and most VPN systems claim there is no logging of your data, the reality is often quite different. VPN systems cannot work without some data logging; at a minimum it will log your IP address, username, and operating system, along with times of connection and disconnection. Further, when a VPN is used the only encrypted part of the connection is the element that connects you to the VPN provider. From the provider onwards, everything is the same as it would have been without a VPN. To be clear, VPNs do offer some level of on-premises, remote access security, but they also require complex configuration and often end-user training, which is often beyond the scope or skillset of an internal IT department.

   Enterprise cloud services approach the remote access challenge quite differently. All access to a cloud service is, by default, remote. Hence, optimizing the security and accessibility of the service is a priority for these providers. An on-premises system operating a VPN is setting up a private network environment. A cloud system *is already* an optimized private network.

Cost & benefits

Moving to the cloud has many benefits, some of them already addressed in this paper. But one of the thorniest "benefits" relates to hard costs. The advent of cloud computing brought us economies of scale through server farms and aggregated hardware. But over the last 10-15 years the cloud has become much more sophisticated and delivers more value in more ways. Innovative developers have leveraged the core infrastructure and concept of the cloud to create and deliver a vast array of innovative software and services. On-premises systems are less effective and bring less business value today than they did in the past, as both technology itself and legal working environments have evolved.

Moving to the cloud can save you money, but not always. Still, in aggregate the benefits of moving far outweigh any drawbacks.

For years, cloud computing was touted as a move that would automatically save you money versus running IT on-premises. If you doubted those claims at the time, you were right to do so, as nothing is ever that simple. Moving to the cloud can save you money, but not always. Still, in aggregate the benefits of moving far outweigh any drawbacks.

Before exploring the cost aspects, it is important to note that building a business case simply based on potentially spending less by using cloud versus on-premises IT is a bad idea, as you should not be swapping your on-premises system for a like-for-like cloud alternative. You should be looking for a cloud alternative that measurably *improves* your on-premises system, is easier and more intuitive to use, enhances both your employees' and your clients' experience, provides better security and access, and gives you a foundation for future expansion and adaptability. These are not aspirational goals; they are hard and measurable expectations that you should be able to attain when shifting to the cloud.

Pricing a cloud solution and comparing costs with your on-premises system can be complex, as the two have very different pricing models. First, you should recognize that cloud services provide much simpler cost accounting and cost planning, as cloud computing costs are typically more predictable and simultaneously more "elastic" than on-premises IT costs. They are more predictable in that they typically come with a standard yearly, per-user cost structure. You can calculate and negotiate your specific requirements with your cloud provider and then have a regular recurring cost to account for. If your needs grow or contract over time, the costs can be quickly adjusted accordingly.

On-premises systems, on the other hand, require you to calculate the cost of server and storage hardware, software, upgrades, security, in-house staff salaries, outside consulting firm costs, and so on. In contrast, cloud service costs are bundled and relatively fixed, and the only variable will be the cost of making the initial move of migrating to the cloud. The good news is that the cost, complexity, and risk of such migrations have fallen sharply over the past few years. Most migrations are now relatively low-cost, simple, and in fact largely automated. Nevertheless, the cost of this one-time activity does need to be considered and accounted for.

Finally, it's worth noting that pricing actually becomes more predictable in the cloud over time, as there will be no costly future hardware or software upgrades. In short, a full cost/benefit analysis of cloud versus on-premises will almost always land in favor of the cloud. But the biggest benefits to any law firm considering moving to the cloud come in terms of the new system's increased security, flexibility, support, and ease of use for clients and staff alike.

Don't swap your on-premises system for a like-for-like cloud alternative. Look for a cloud alternative that measurably improves your on-premises system.

A Path to the Cloud

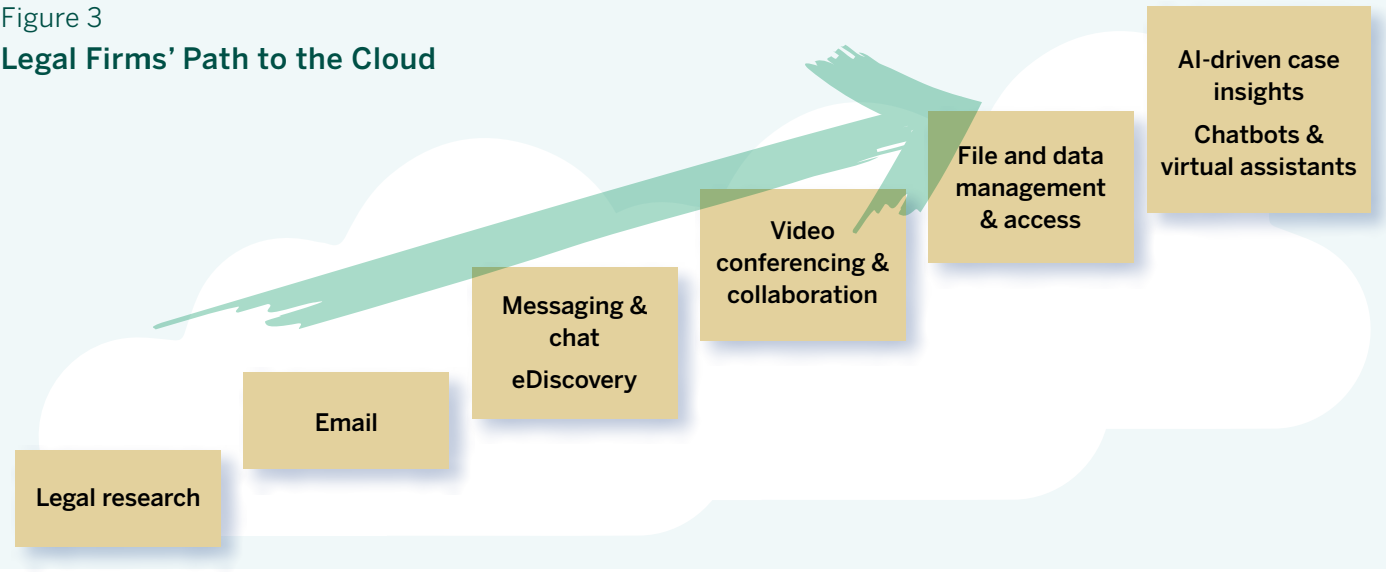
There is merit, tradition, and comfort in maintaining a brick-and-mortar office, and that will be the case for the foreseeable future. Even so, moving forward ever more support staff and lawyers will work remotely, whether 100% of their time or 1-2 days a week.

According to Cushman and Wakefield, 90% of law firm respondents anticipate that 10% of their lawyers will be working remotely at least twice a week within the next two years. In 2019, the ABA published a report stating that 68% of law firms cited "ease of access from any location" as their primary reason for moving to the cloud. That number will likely continue to rise as historic concerns regarding third-party access to data and cloud security become recognized as no longer credible.

It is worth remembering that the idea of renting access to services like Westlaw and Lexis for research once seemed novel, but today law firms have become almost totally dependent on them as core research tools. This was unthinkable 20 years ago, but nevertheless law firms did indeed move to the cloud for research. Companies, employees, and clients alike have shown themselves to be highly adaptable to change over the past 18 months of the pandemic, and more change is likely on the horizon. The legal sector needs to embrace technologies that can adapt to change as well. Moving your firm's files and data to the cloud is simply the next step in this ongoing journey. In fact, many law firms, if not most, are already making extensive use of the cloud whether they know it or not, as the path to the cloud has been underway for decades (see Figure 3).

From its start in the early 00s when cloud-based research services took hold, through the use of email, messaging, and video conferencing, the journey now continues with shifting files, data and associated storage, and management and collaboration services.

Figure 3
Legal Firms' Path to the Cloud



Conclusion & Recommendations

In the world of business process management, there's a general rule that even in the most optimized processes around 10% of activities won't meet the norm; these are classified as "exceptions."

The 10% that are exceptions will take up 80% of your time and resources to resolve. A single lawyer working from home one day a week may seem insignificant, as they will be in the office the other four days. In reality, such hybrid working patterns will require more planning, resources, and adaptation to manage effectively and securely.

Remote and hybrid working is much more than a change of location – it is a transformation in the world of working and corporate culture, and the full ramifications of this shift are yet to be fully understood. Not everyone can or will thrive and succeed in this new environment, and law firms in particular will likely continue to value working together in person to resolve difficult and contentious issues or simply to bond and build a strong working team. But the hybrid work environment is here to stay, and it's up to each law firm to act accordingly. Such hybrid working, accompanied by a shift to cloud computing, should deliver major benefits to any law firm large or small. One example is that smaller firms will be able to compete outside their physical location, helping clients in other cities without the need for travel and while maintaining business continuity.

For the General Counsel, CIO, and CISO, a move to the cloud will immediately deliver vastly improved security and resilience against cyberattacks. It will also deliver more predictable and manageable costs, lower overheads, and less complexity to manage. Alone, these will be reason enough for many to make the move. But just as importantly, the end user – whether a partner, a staff member, or your clients – will find much more adaptability, ease of use, and freedom to work together and access information anywhere, anytime, and on any device. Out of adversity comes opportunity, and sadly it has taken a pandemic to move the tech needle in legal circles. We now have the opportunity to finally make the move to the cloud, transform, stay resilient, and attract and retain the best team.

© 2021 | info@deep-analysis.net

About Deep Analysis

Deep Analysis is an advisory firm that helps organizations understand and address the challenges of innovative and disruptive technologies in the enterprise software marketplace.

Its work is built on decades of experience in advising and consulting to global technology firms large and small, from IBM, Oracle, and HP to countless start-ups.

Led by Alan Pelz-Sharpe, the firm focuses on Information Management and the business application of Cloud, Artificial Intelligence, and Blockchain. Deep Analysis recently published the book "Practical Artificial Intelligence: An Enterprise Playbook," co-authored by Alan and Kashyap Kompella, outlining strategies for organizations to avoid pitfalls and successfully deploy AI.

Deep Analysis works with technology vendors to improve their understanding and provide actionable guidance on current and future market opportunities.

Yet, unlike traditional analyst firms, Deep Analysis takes a buyer-centric approach to its research and understands real-world buyer and market needs versus the "echo chamber" of the technology industry.

About the Author

Alan Pelz-Sharpe is the founder of Deep Analysis. He has over 25 years of experience in the IT industry, working with a wide variety of end-user organizations like FedEx, The Mayo Clinic, and Allstate, and vendors ranging from Oracle and IBM to start-ups around the world. Alan was formerly a Partner at The Real Story Group, Consulting Director at Indian Services firm Wipro, Research Director at 451, and VP for North America at industry analyst firm Ovum. He is regularly quoted in the press, including the *Wall Street Journal* and *The Guardian*, and has appeared on the BBC, CNBC, and ABC as an expert guest.

Contact us:

info@deep-analysis.net
+1 978 877 7915