



**INTERMEDIA**

The Business Cloud™

# DEATH BY 1000 CLOUD APPS

The 2014 Intermedia SMB Cloud Landscape Report: A comprehensive guide

---

# TABLE OF CONTENTS



---

VMblog Q&A with Michael Gold, President of Intermedia	4
Death by 1000 Cloud Apps	8
Is there such thing as too many cloud apps?	8
Too many choices!	10
Interview with Michael Osterman	12
Too much to manage!	16
Interview with Brandon Ingram	18
Too many logins!	22
Too much risk!	24
Solution #1: Manage less. Look for a “one-stop shop” for cloud IT	26
Solution #2: Login once. Deploy a single sign-on portal.	27
Appendix: A deeper look at the management headache	28

---

## VM BLOG Q&A WITH MICHAEL GOLD, PRESIDENT OF INTERMEDIA

This interview recently appeared in VMblog, and is reprinted here with their permission. It provides a great introduction to our “Death by 1000 Cloud Apps” report and the benefit of consolidating IT services under one vendor.

Intermedia—the world’s leading one-stop shop for cloud IT—recently reached a growth milestone: one million paid users. I caught up with Michael Gold, President of Intermedia, to learn more about the company’s business model and latest product updates.

---

**FOR THOSE READERS WHO MIGHT NOT BE FAMILIAR WITH YOUR COMPANY, CAN YOU GIVE US SOME BACKGROUND ON INTERMEDIA AND EXPLAIN WHAT YOUR SOLUTIONS ACCOMPLISH?**

I'll tell you a quick story. An old friend of mine in Denver is a CPA and CFO. He a finance expert—cash flow, specifically. So a few years ago, he started consulting to help businesses manage cash flow.

In the last four years, he's hired people for sales, marketing, HR and operations. But he hasn't hired a single IT person. Why? Because he figured he could get everything he needed from the cloud.

And he was right. He got email from one provider, phones from another company, Dropbox, WebEx, Basecamp, you name it. As his business grew, he kept on adding new people and new services. And then, one day, his lawyer advised him that he needed compliant email archiving to take on clients in healthcare or any other regulated industry. He started counting all the control panels he was logging in to manage his systems and dozen-or-so people. And he thought, "That's it. I have to hire an IT guy. So much for the promise of the cloud."

That's what he actually told me! "So much for the promise of the cloud." He thought that because he didn't have a server closet—and because his team could manage their own hardware—that IT complexity was a thing of the past. And this is why customers come to Intermedia. Three reasons, in fact. First, they need certain fundamental business apps. Email, phones, file sync and share, security, mobility, etc. Every business needs these tools.

Second—and this is what went wrong in my friend's case—they want to deal with as few control panels as possible. They don't want to worry about integration or mobility or security. They want someone to make it enterprise-grade IT simple and affordable.

And third, they don't want to provide internal support for an outsourced app. A provider should do more than just host software—it should provide the support that you'd get if it were managed in-house.

---

**WHY IS THE ONE-STOP SHOP MODEL ATTRACTIVE TO SMBS?**

Because it eliminates complexity. There's just one control panel for a dozen different services. Because there's just one bill to pay. And one phone number to call if something goes wrong. And because security and integration are the provider's responsibility—and they have experts who are trained and certified far beyond the ability of any IT person my friend in Denver could hire, for example. Oh, and there are cost benefits. The more services you buy from a single provider, the more of a discount you get – as much as 60%. Plus, when you hire someone, you don't have to log into a dozen different services to get them accounts. You do it once. This saves time.

According to Osterman Research, 83% of SMBs find it desirable to get as many services as possible from a single provider. We wrote about this in our 2014 SMB Cloud Landscape Report. And Microsoft's research also supports this: they found that 62% of businesses prefer to get their email and phone service from the same vendor.

By the way—the one-stop shop model is hugely attractive to our channel partners as well. We actively partner with over 5,000 businesses that provide IT services to other small businesses. These guys are in the business of IT—and if these guys turn to us to reduce IT complexity, you know that this is something. So we support them with a Partner Program that gives them the option of branding, full control over billing and pricing and maintaining complete ownership over their customer relationship. It's a win for them, for us, and of course for their customers.

---

**YOU MENTION INTERMEDIA'S 2014 SMB CLOUD LANDSCAPE REPORT, CAN YOU TELL US WHAT INFORMATION IS PROVIDED IN THE REPORT?**

We call it "Death by 1,000 Cloud Apps." The name's dramatic, but it's true. We found that the average SMB is juggling 14 cloud apps, with 5.5 apps per user. The overhead of choosing and managing all these apps is approaching a tipping point. In fact, the report explores four main problems from this glut of apps. First is too much choice. From sales demos to negotiation to procurement, choosing a new app is now a months-long process. And second, once the app is in place, there are far too many headaches around integration, security, mobility, billing, support and so on.

Third, for users, they have too many passwords to remember. Besides the productivity hit this causes, this creates a massive security risk, which is the fourth big problem: the more passwords you have, the more likely you are to choose weak passwords or take other security shortcuts. I guarantee you that if you walk around your office looking at the sticky notes pasted to people's monitors; you'll find someone's passwords in five minutes. Verizon found that 76% of network intrusions exploit weak or stolen passwords.

---

**INTERMEDIA RECENTLY ANNOUNCED NEW PRICING PLANS, CAN YOU SHARE DETAILS AND BENEFITS OF THESE PLANS?**

What we've learned from our million paying users is that there's an incredible spectrum of IT needs. Some businesses need nothing more than a simple mailbox. Other businesses have power users who need practically unlimited storage across a dozen different services.

Our new plans span the spectrum. There's something for everyone, from 1,000-person law firms to five-person bakeries. The plans range four dollars to 100 dollars per user—but most businesses will get everything they need with a \$15 plan. Which, of course, includes discounts for buying multiple services. Plus the kind of reliability and support you need to truly offload the burden of IT.

By the way—we include a huge range of services with every single plan. This is another benefit of a one-stop shop. Every plan includes SecuriSync for file sync and share, Intermedia AppID for single sign-on, and even conference calling.

And all our plans include a 99.999% uptime guarantee as well as expert email migration from our Cloud Concierge team at no additional cost. And they all offer 24/7 phone support. We answer our phones in 60 seconds.

---

**IN THE CLOUD  
SECTOR,  
WE SEE MANY  
COMPANIES THAT ARE  
NOT PROFITABLE,  
AS A PROFITABLE  
COMPANY, WHAT DO  
YOU DO DIFFERENTLY?**

Here's the thing about providing email and phones: these are the foundational services that any business needs to do business. Customers rely on us. They depend on us.

So we see it as our duty to run profitably. Profitability means we're fundamentally sound and in it for the long haul. This may be anomaly in today's cloud world, but we think long term. Just like our customers. This means balancing revenue growth, profit, and investment for future success. Finding this balance is hard. That's why so many businesses are unprofitable. But it's the right thing for us, which is why we have upwards of \$150 million in revenues with significant profitability. Our partners see it too, which is why they now contribute over 2/3 of our new sales. But most important is how our customers feel. We measure their approval in our industry-leading churn rates—which are much less than 1%.

---

**GREAT, IS THERE  
ANYTHING ELSE YOU'D  
LIKE TO ADD THAT WE  
HAVEN'T COVERED?**

I'll tell you what I told my friend in Denver: we keep adding new services and enhancing our existing ones. This is yet another benefit of a one-stop shop. We keep our customers ahead of the technology curve.

Our motto is that we provide a "worry-free experience." This is more than just great support and incredibly high reliability. This is about IT that grows with your business long into the future.

# DEATH BY 1000 CLOUD APPS

The 2014 Intermedia SMB Cloud Landscape Report

---

## IS THERE SUCH THING AS TOO MANY CLOUD APPS?

At first, every new cloud app means one less server to manage. Everyone high-fives as the server racks are emptied out and replaced with a foosball table. But then, one day, there are just too many apps. Finance starts complaining about managing all the vendors. Users tire of remembering complex passwords and take insecure shortcuts. IT plays endless whack-a-mole with integration issues. The IT guys feel like crying, but they no longer have a server room to cry in.

## GOOD NEWS: YOU'RE NOT ALONE.

Intermedia's 2014 SMB Cloud Landscape Report explores the four main problems that SMBs experience with a sprawling cloud. And—thankfully—it presents two broad strategies for avoiding death by 1000 cloud apps.

If you're being crushed by the weight of the SMB cloud, you're not alone. This report looks at the challenges that come with embracing the cloud. And it offers the solutions you need to avoid "Death by 1000 Cloud Apps".

---

**14.3**

**THE AVERAGE NUMBER  
OF APPS PER SMB**



**5.5**

**THE AVERAGE NUMBER  
OF APPS PER EMPLOYEE**



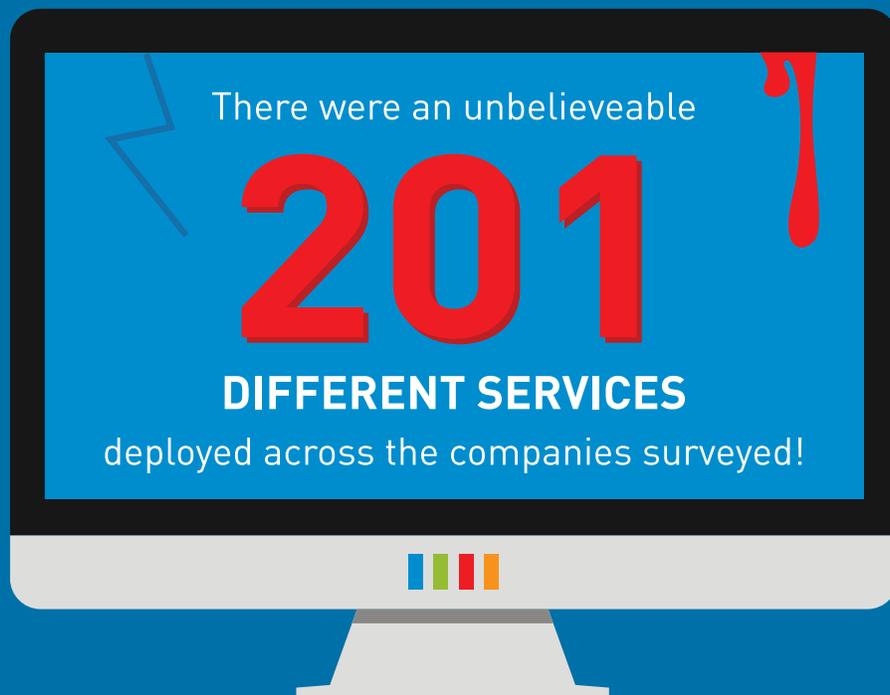
**\$15**

**THE AVERAGE DRAG ON  
EACH EMPLOYEE'S  
PRODUCTIVITY, MONTHLY**



WHEN THERE ARE TOO MANY APPS, THERE ARE...

**TOO MANY CHOICES!**



The pain of a new cloud app begins even before you deploy it. In fact, it begins even before you know the app exists. That's because there are so many apps to choose from that your productivity practically grinds to a halt. Here's what you face.

---

“While virtually every decision to implement a new tool, storage solution or other capability makes sense at a micro level, this creates the macro problem of managing all of these tools.”

—OSTERMAN RESEARCH

### **RESEARCHING VENDORS TAKES FOREVER.**

To choose the right provider, you first research the category. Then you identify the vendors. Then you fall in love with specific features. Then you start comparing plans and, inevitably, sacrificing features. Then it's time for RFPs. Suddenly weeks have passed, and critical projects are piling up in your inbox.

### **THE SALES PROCESS IS PRACTICALLY ENDLESS.**

You've narrowed it down to a couple of vendors. Great! Now you have to deal with the sales process: attending demos, posing questions, waiting for answers, negotiating discounts, looping in decision makers, posing THEIR questions, and on and on. You spend more time talking to sales reps than you do your own family.

### **DON'T FORGET THE INTERNAL DUE DILIGENCE.**

It's not just about dealing with the vendors. You also have to make sure that this new cloud app will play nicely with your other IT services. This means involving IT to model the setup process, create a plan for provisioning, prepare for integrations with your other apps, and more.

### **OH, GOOD. INTERNAL RED TAPE.**

You've finally found the right app at the right price. Now begins the procurement process: getting higher-ups to sign-off, creating a PO, reviewing the contract, talking with lawyers, going through negotiations, working with accounting to establish a relationship with the vendor, figuring out the billing, etc. This is a lot more complicated than buying staplers and paperclips!

### **THEN YOU'VE GOT TO ACTUALLY DEPLOY THE APP.**

The contract is signed. Now it's time for IT to get busy. That means configuring the app, massaging the firewall, provisioning users, setting up cross-service integrations, and—most painful of all—corralling all your users into training sessions.

### **ALL THIS TIME ADDS UP.**

You could have been writing code, or designing a building, or catering a lunch, or doing whatever it is you do to actually make money. Instead, you've just devoted weeks or months just to buy some software. If you run a smaller company with limited IT resources, that loss in productivity can be particularly painful. And all this just for ONE APP.

---

## INTERVIEW WITH MICHAEL OSTERMAN

Michael Osterman, leading analyst of SMB communication and collaboration technology, conducted the research that is central to our “Death by 1000 Cloud Apps” report. In this interview from June 10, 2014, we asked him about the challenges experienced by SMBs when moving to the cloud and his recommendations for alleviating the pain.

---

**HOW WOULD YOU DESCRIBE THE CLOUD LANDSCAPE FOR SMBS?**

Well, I think it's still very much in a state of flux. People are starting to understand the cloud. But the upper end of the SMBs – the 100, 200, 500 seat companies are really at a crossroads. They are still trying to determine what the appropriate mix is between cloud and on-premises.

---

**YOU FIND AN AVERAGE OF 14.3 APPS PER COMPANY. DO YOU EXPECT THAT NUMBER TO INCREASE?**

Yes, very definitely. There are just a huge number of applications out there. I would expect 14 applications to end up being 18-20 on average in the next couple of years.

---

**WHAT ARE THE PAINS SMBS FEEL WHEN IT COMES TO MANAGING THEIR APPLICATIONS?**

Well I think that SMBs are really caught between a rock and a hard place. If you're an SMB, you have to do much of the same things that an enterprise does. But you have fewer users over which to spread the cost of infrastructure and staff.

SMBs have to look for lower-cost ways of doing things or just don't do them at all. They allow more BYOD, or allow users to do whatever they want because they can't afford the same solutions that protect enterprises against potential threats.

We find that the office manager is the part-time IT person at a lot of SMBs. They're sort of a generalist. They can't deal with the minutiae that come up, so maybe the company experiences higher downtime. They might not be able to do the monitoring, archiving and encryption work that a large enterprise could because they can't dedicate the time.

---

## HOW CAN SMBs MAXIMIZE THE IT RESOURCES THEY DO HAVE?

The key is to prioritize everything that IT is doing and look at the stuff that's going to provide a competitive advantage to the company. List everything—even the really mundane stuff like updating spam filters or installing new anti-virus software on laptops. Offload the items that don't provide a competitive advantage to the cloud—keep your IT staff, if you even have any, for really high value stuff that grows your business.

---

## WHAT CAN COMPANIES DO TO MANAGE THE PROLIFERATION OF CLOUD APPS?

We recommend having policies about what's allowed and what's not allowed. But don't implement draconian controls that say users cannot use X app at work, because people will just bring their smart phone and use it anyway. Instead, tell people that they have to be careful. Then implement technology that will defend against any threats.

And offer substitutes. So if someone wants to use Dropbox, there's a substitute that has better security controls that IT can manage. The fundamental problem is that IT has simply lost control. If you have 100 users, each with their own Dropbox repositories, what happens if you have to do eDiscovery across all of your content? You have to go through the corporate systems AND gain access to 100 different Dropbox accounts.

---

## HOW DOES A SSO PORTAL HELP SOLVE USER PROBLEMS?

Single Sign-On is essential. It has two primary benefits. One, with SSO you sign in once and you have access to all your apps. So you save time. And not just by having one login—you save time on password resets, too.

The second benefit is the increased security of having really robust passwords for all your applications, instead of having easy ones, or reusing passwords. In surveys, we've asked people if they use the same passwords for multiple applications, and upwards of 70-80% do.

---

## HOW DOES AN SSO PORTAL BENEFIT IT?

Certainly it makes life easier for IT because it's a much more secure environment for accessing applications. Also, IT won't be fielding requests for password resets. And you can do things like risk-based authentication so that the highest value assets require the most stringent security, authentication and so forth.

---

## HOW CAN BUSINESSES MEASURE AND COMPARE TCO (TOTAL COST OF OWNERSHIP) FOR THEIR APPS?

It's not that easy an exercise because you have to do some pretty detailed analysis to see how much time people are spending on accessing applications, translating data from one app to the other, trying to find data, etc. Then you have to come up with predictions on the time savings if employees had a smaller set of apps that shared data more readily.

And doing that TCO analysis is complicated by the fact that not all managers believe that productivity loss is a real cost, because they don't write a check for it. A lot of managers assume that if someone is spends an extra 30 minutes looking for content they can't find, they can spend an extra 30 minutes at work to make that up, which isn't realistic.

---

## HOW CAN COMPANIES EVALUATE SPECIFIC VENDORS?

I'd look at a variety of things: their customer base, the length of time they've been in business, their financials, the security model they employ, etc. How many data centers do they have? Do they have geo-redundancy in case a hurricane or tornado flattens one of the datacenters? How quickly can they be back online with my data?

We don't recommend going after the lowest cost vendor, because they may not be around long term. Doing your due diligence about the financials of the company and the long-term health is important.

WHEN THERE ARE TOO MANY APPS, THERE IS...

**TOO MUCH TO MANAGE!**



You thought the pain was over? It's just beginning. Now you have to juggle licenses, manage devices, provide support and generally try to wrangle the madness. The more employees you have, the crazier it gets. Here's what you're up against.

---

"[Multiple apps require] more IT effort because there are more interfaces and management consoles at which to become proficient, more time spent in training, more applications on which to provision new users, and less integration between solutions."

—OSTERMAN RESEARCH

---

"Another problem with a highly heterogeneous environment is that the complexity of billing increases, as does the management of the relationships with the various vendors."

—OSTERMAN RESEARCH

### **ONGOING MANAGEMENT IS REPETITIVE—AND NEVER ENDING.**

Someone's hired. Someone's fired. Someone's promoted. Whenever this happens, you need to log into all your apps and make the change, over and over again. If you're lucky, some of the apps will integrate with your directory server. For the rest—well, you may want to get some coffee before you start.

### **DATA STARTS TO SLIP THROUGH THE CRACKS.**

When company data is stored across 14.3 cloud apps, security holes inevitably appear. Especially when people start accessing services from multiple devices. And what about the day when you forget to fully deprovision a departing employee? They could still have access to confidential company data. Just hope they aren't careless. Or bitter. Or angry...

### **YOU SPEND HALF YOUR DAY ON HOLD WITH SUPPORT.**

It's bad enough that you have a unique support number to call for each app. What happens when an integration fails? Each vendor will point fingers at the other, which means you'll have to work with dueling support teams to get anything resolved.

### **INTEGRATION IS UP TO YOU.**

Some of your apps might integrate with others out of the box. Some systems might provide you with APIs. But because every cloud environment is unique, you're still going to end up doing most of the work yourself.

### **MANAGING MOBILITY IS MESSY.**

In today's BYOD world, you need to make sure devices are secure when they access corporate data. This means policing every device owned by every user. And helping configure VPNs. And tweaking settings on individual apps. And performing remote wipes when devices are lost. And on. And on. And on...

### **AND THEN YOU'VE GOT TO PAY THE BILLS.**

Your finance teams are going to examine every single bill from every single vendor. And their reconciliation process is going to be tedious. "Did you add this new user?" "Did you authorize this overage?" "Did you use your full allotment of support?" Next month: more of the same.



---

## INTERVIEW WITH BRANDON INGRAM, SALES AND OPERATIONS MANAGER AT ENVIRONMENT CONTROL

Environment Control is a current Intermedia customer. We spoke with Mr. Ingram recently to get a first-hand view of the struggles faced by IT admins at SMBs when it comes to cloud apps and how consolidating services under fewer vendors has helped alleviate some of the pain.

---

## HOW MANY USERS IN YOUR ORGANIZATION?

We have 170 full and part time employees in the field, but not everyone has access to every app. We also have 20 to 25 people within the office who have computers, iPads, and an iPhone that they are responsible for. So I am managing the IT for them plus people in the field.

---

## DO YOU HAVE A DEDICATED IT TEAM?

I am the sole IT admin, but that's along with the other things that I do. It's a part-time role.

---

## HOW MANY APPLICATIONS DO YOU CURRENTLY MANAGE?

We probably have between 3 and 5 apps that our employees use.

---

## WHAT TYPES OF APPLICATIONS ARE YOU UTILIZING?

One of them is Salesforce. Another is a customer QC metrics tracking program that we use for inspections on our properties. Our phone system is hosted in the cloud, so we're able to track all our voicemails. And we have email and SecuriSync from Intermedia.

---

## WHAT APPLICATION SERVICES DO YOU CURRENTLY USE?

For the mobile devices, we use an MDM product. In terms of file sharing, we use SecuriSync, which has been a huge benefit for us. And being able to manage it in HostPilot along with our email has been really great.

---

## HOW MUCH TIME DO YOU SPEND MANAGING THE MULTIPLE APPLICATIONS THAT ARE IN USE?

When everything runs as it should, it doesn't take any time. But when an issue comes up, I have to track down at least 2 devices per individual and go through the reset process on each device. That takes up a lot of my time, as well as the time that the employees are not able to access the app while in the field.

It really ties up my day. Instead of doing other things, I've got to wait around for someone to bring me their devices. And it's cumbersome for them because they have to come in from the field and find me.

---

## WHAT CHALLENGES, IF ANY, DO YOU FACE IN MANAGING THESE APPLICATIONS?

Well, the biggest challenge that I have right now is that I haven't handed out individual passwords because it's easier for me to keep track of all of them myself. I make everyone with a device come to me, and I put in the password. So it's labor-intensive for me.

And a lot of times, I have one password that I use for everyone. I've made it easier for myself that way, but, unfortunately, it's not a very secure system.

---

## WHAT ARE THE CORE IT CHALLENGES YOU FACE IN YOUR ORGANIZATION?

There's only me, so I try to keep everything pretty well guarded so that no one can get in and muck with the system. Also, my whole day isn't IT. I have other responsibilities beyond that. We've tried to manage IT in house without a full-time admin.

And really, Intermedia has made that possible, because before, it was a much more tedious task. Now I have one place where I can put everything, where I can press a button, and each of the services gets deployed to these individuals. When it comes to new services, the first thing I do is make sure that everything integrates with Intermedia.

---

## HOW HAS INTERMEDIA HELPED ALLEVIATE SOME OF YOUR IT PAIN POINTS?

In terms of working with Intermedia, it's always been a great experience. When you say you'll do something, you do it. It's always been easy to deploy the service and get it working. Even 4-5 years ago

---

## WHAT ARE YOUR KEY CONSIDERATIONS FOR EMPLOYING A CLOUD SOLUTION?

when we did the email migration. It was really easy. You know, looking back, I don't think support and migration were as high on the list as they should have been. When it comes to support, there are a lot of providers out there who will send you to the forum. And the forum is great if you can find your answers there. But if you can't find it in a forum or on the wiki, then it's nice to have someone answer the phone and get your problems solved promptly.

So I use the phone support service at Intermedia quite a bit, because it's nice to get the answer right way and not have to sort through a bunch of pages of information. So now when I look at providers, I look at support, and that's a factor in my decision. So you guys met the challenge even though I didn't know the challenge needed to be met.

---

## WHAT DO YOU LOOK FOR WHEN SELECTING AN IT VENDOR?

I look for ease-of-use and how easy it would be to deploy to my people. We're in the janitorial and landscape industry. And I have a lot of good people who are really great at their jobs, but the cloud and mobile devices talking to each other are out of the norm for them. I need something that is easy to explain to them and easy to manage.

The file level security that I was able to deploy with SecuriSync was far greater than competitors like Dropbox. And of course, there was the fact that it was already integrated with my email. And being easy to manage with HostPilot was great.

---

## HOW DESIRABLE IS IT TO CONSOLIDATE MULTIPLE SYSTEMS/ TECHNOLOGIES TO A SINGLE VENDOR?

I try and put as much through Intermedia as possible because it saves time on my end. I have fewer things to log into to set people up. I can set it all up in one place and be done with it.

---

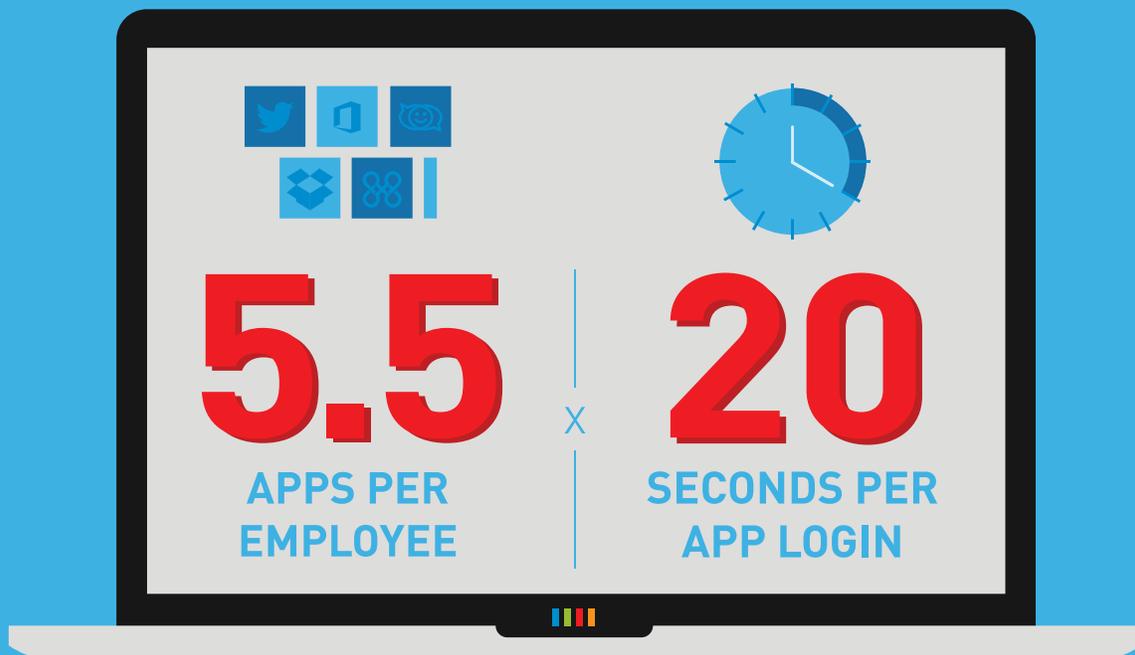
## ARE YOU CURRENTLY CONSIDERING OTHER SERVICES FROM INTERMEDIA? IF SO, WHICH ONES?

We are looking at putting our phone service through you as well. Trying to put as much under one house as possible makes it much more efficient.

I just saw the single sign-on product and I'm looking at how that can benefit us. And you have the mobile app for that as well, which is great. Especially because I can be more secure and give everyone their own passwords. And the reset process would be more secure because I could reset it from one place, too.

WHEN THERE ARE TOO MANY APPS, THERE ARE...

**TOO MANY LOGINS!**



It isn't just IT and Finance who suffer the effects of a runaway cloud landscape. Employees suffer, too. That's because they're the ones who suddenly have to track ever-increasing numbers of login URLs and passwords. This has massive security implications, which we'll discuss in a moment. But even before we consider security, we have to contend with the loss of productivity. Here's what we mean.

---

“The need to employ a number of different applications means many difficulties for users: there are more interfaces to learn, more applications to sign into, a reduced ability to share data between applications, and a longer learning curve that ultimately reduces user productivity.”

—OSTERMAN RESEARCH

### **LOGIN TIME IS WASTED MONEY.**

It takes an average of 20 seconds to load a login page, find your login name, remember your password, and access a cloud app. That doesn't sound like much. But when you put a dollar amount to the time spent staring at a login screen, it gets really ugly. For every login your user is faced with, you're losing money. The bigger you are—and the more you embrace the cloud—the higher the your productivity costs rise.

### **LOGIN FAILURES CONSUME EVEN MORE TIME.**

Mistyped passwords. Misremembered passwords. Hunting through your mailbox to find the password clue you sent yourself. Requesting password resets and then waiting for the reply email. Realizing you had the correct password but the wrong login name. And then, finally, login success—only to realize that you forgot why you were logging in the first place.

### **EVERY APP HAS A LEARNING CURVE.**

The best cloud apps are often the hardest to learn. So users are spending more time attending training webinars or watching how-to videos. There's obviously a value to any new application—but there's always a cost to unlocking that value.

WHEN THERE ARE TOO MANY APPS, THERE IS...

**TOO MUCH TO RISK!**



Most users are perfectly capable of creating and remembering unique strong passwords for every one of their apps. But not all users are willing to do so. And that's the problem: when users are forced to remember a bunch of passwords, they get sloppy. And hackers LOVE sloppy passwords: 76% of network intrusions exploit weak or stolen passwords. Here's what creates your risk.

---

“Users that employ a variety of applications will employ easy-to-remember—and often insecure—passwords or employ the same password across multiple systems in order to remember them more easily. Worse, employees will often write down passwords on sticky notes or in other insecure places.”

—OSTERMAN RESEARCH

### **USERS ARE THE WEAKEST LINK.**

Faced with the task of remembering multiple passwords, users take shortcuts: reusing passwords, creating weak passwords, storing passwords in email, even writing down passwords and pasting them to their monitors. And hackers know this. Why attack a firewall secured by a world-class team when users present a far easier target?

### **MOBILE DEVICES COMPOUND THE PROBLEM.**

Your data is only as secure as your users’ phones and tablets. Are they all password locked? Is the data encrypted? If a device is lost or stolen, what kind of access do the bad guys have? Also—many mobile apps automatically remember user logins. So a thief only has to tap an icon to get to your data. If you can’t remotely wipe that device or shut it down, you’re in trouble.

### **AND WHAT ABOUT ROGUE ACCOUNTS?**

All the facts and figures in this report leave out one thing: many users are using apps that IT doesn’t even know about. How can IT maintain security on rogue accounts deployed by teams or individuals without IT’s knowledge or consent?

---

“An environment with a large number of applications and different vendors in use will allow IT to have less insight into the overall IT footprint.”

—OSTERMAN RESEARCH

---

## BUT ALL IS NOT LOST!

You can have your apps  
and keep your sanity.

### SOLUTION #1: MANAGE LESS. LOOK FOR A “ONE-STOP SHOP” FOR CLOUD IT.

Too much choice? Too much to manage? Too many logins? Too much risk? There’s an easy way to slash all four of these problems: get your fundamental IT services from a single provider. Email, telephony, file sharing, collaboration, security, archiving, mobility, and so on: a one-stop shop for these apps offers far less pain for your business. Here’s why:

#### **You only have one vendor to manage.**

Finance only has to pay one monthly bill and manage one vendor relationship. IT only has to work with one company for orders, questions and customer service.

#### **IT only has one support phone number to call.**

Instead of wasting time trying to figure out whom to call and how to get help, IT can just call one support number for any issue.

#### **Everyone has only one password to remember.**

This applies to both IT and employees. One password makes life easier for everyone and drastically lowers security risks.

#### **IT gets one control panel for users, services and devices.**

One control panel with shared settings: this integration is the ultimate time-saver for IT. And it’s the best reason to get your IT services from one vendor.

#### **You get one location for all your critical data.**

You know exactly where your data is stored and how it’s being protected. IT gets more control over who sees what, full integration across all apps, and fewer helpdesk calls about version-control issues.

#### **You get package discounts with one bundle.**

A single vendor will offer you discounts to buy multiple services. Why pay a premium for individual services, when you can get the cost benefit of bundling?

---

“[You should] identify the solutions running today that can be consolidated to a single vendor. Email, voice and collaboration solutions are often the most likely candidates, although there are many other tools that can be consolidated to a single solution and vendor, as well.”

—OSTERMAN RESEARCH

## **SOLUTION #2: LOGIN ONCE. DEPLOY A SINGLE SIGN-ON PORTAL.**

But what about all your other apps? The ones you can't get from a single provider? You still face weak passwords, lost productivity during logins, and security issues on multiple devices.

The solution is to give users a Single Sign-On (SSO) portal. This offers one-click access to ALL their cloud apps, with just one strong password to remember. From the user standpoint, an SSO portal makes IT simple again.

Remember the days when everything you needed was accessed through the Start menu? For users, an SSO portal makes things just that easy again. Better still, an SSO portal pays for itself.



**INTERMEDIA** The Business Cloud™

---

# **DEATH** BY **1000** CLOUD APPS

The 2014 Intermedia SMB Cloud Landscape Report

---

# INTERMEDIA CAN HELP

## GET YOUR ESSENTIAL APPS FROM ONE VENDOR.

Intermedia is the world's largest one-stop shop for cloud IT services and business applications—including email, phones, file sync and share, single sign-on, security, mobility, archiving and more. All our services are integrated, secure and mobile—and they're all managed through our central HostPilot control panel. Intermedia's Office in the Cloud™ suite integrates all of the essential IT services that SMBs need to do business. This includes email, voice, file sync and share, single sign-on, security, mobility, archiving and more.

Learn more about Office in the Cloud:

[www.intermedia.net/why-intermedia/office-in-the-cloud](http://www.intermedia.net/why-intermedia/office-in-the-cloud)

## DEPLOY A SINGLE SIGN-ON PORTAL

Office in the Cloud's newest service is Intermedia AppID. AppID provides a single sign-on portal that gives your employees one-click access to all their cloud apps, with just one password to remember.

Learn more about Intermedia AppID:

[www.intermedia.net/products/appid](http://www.intermedia.net/products/appid)

---

## APPENDIX: A DEEPER LOOK AT THE MANAGEMENT HEADACHE

Osterman Research's survey took a deeper look into the cloud apps companies deployed across 8 categories of essential IT services, including email, telephony, communication and collaboration, mobility management, file sync and share, and archiving and compliance. In many cases, IT was managing more than one cloud app in each category.

---

**EMAIL: MICROSOFT  
EXCHANGE STILL RULES  
THE EMAIL WORLD**

Osterman Research's survey results show the percentage of SMBs using each type of cloud app. According to Osterman Research, "Microsoft Exchange dominates the on-premises email landscape, while Google Apps is more widely deployed as a cloud solution. This indicates that Google has done a good job at penetrating the small organization market. That said, Osterman Research believes that smaller organizations using on-premises email will be a more receptive market for cloud-based email solutions in the future."

 Microsoft	<b>75.2%</b>
 Office 365	<b>15.7%</b>
Google	<b>9.1%</b>
 IBM®	<b>13.2%</b>
GroupWise®	<b>14%</b>
<b>OTHER</b>	<b>9.1%</b>

---

**TELEPHONE SERVICES:  
VOIP BEATS OUT  
TRADITIONAL LANDLINE**

Slightly more respondents were using traditional landlines than VoIP, but VoIP service is clearly popular among small businesses. And many companies were supporting both landline and VoIP technology.

<b>LANDLINE</b>	<b>59.5%</b>
<b>VOIP PROVIDER (NOT THE SAME AS EMAIL)</b>	<b>51.2%</b>
<b>VOIP PROVIDER (SAME AS EMAIL)</b>	<b>14.9%</b>
<b>OTHER</b>	<b>3.3%</b>

**COMMUNICATION AND  
COLLABORATION: A  
VALUABLE PRODUCTIVITY  
TOOL FOR SMBS**

When analyzing SMB usage of communication and collaboration cloud apps, Osterman Research found that: “There is a significant number of real-time communications solutions in use at smaller organizations: 1.76 per organization. We also found that while WebEx is widely deployed, Citrix GoToMeeting is also very popular among smaller firms.”

	<b>57.8%</b>
	<b>44%</b>
	<b>33%</b>
	<b>15.6%</b>
	<b>9.2%</b>
<b>OTHER</b>	<b>16.5%</b>

---

**SECURITY: VERY  
IMPORTANT, AND VERY  
FRAGMENTED**

Security solutions are vital to all businesses, and the choices are vast. The Osterman Research results showed a lot of fragmentation with 18 different solutions in use by survey participants.

In analyzing the choices made by SMBs, Osterman Research discovered that: “There is a mean of 1.61 different security solutions in place among smaller organizations. While Symantec is the market leader among smaller firms, we found that McAfee and Barracuda are also widely deployed.”

 Symantec™	<b>50.4%</b>
 McAfee®	<b>35.5%</b>
 BARRACUDA NETWORKS	<b>21.5%</b>
 TREND MICRO	<b>20.7%</b>
 Microsoft	<b>10.7%</b>
<b>OTHER</b>	<b>35.5%</b>

---

**FILE SYNC AND SHARE:  
MOST SMBs SUPPORT  
MORE THAN ONE SOLUTION**

A big surprise came when we analyzed the survey results for file sync and share solutions. 63.4% of survey respondents supported more than one app with 2 respondents supporting 6 different file sync and share solutions!

According to Osterman Research, “Not surprisingly, Dropbox is the leading FSS solution, but there is significant fragmentation in this market with vendors like Google Apps and Apple iCloud finding significant penetration. The fact that there is a mean of 2.43 FSS solutions in place per organization indicates that consolidation on fewer solutions is necessary. This is particularly important to maintain data security.”

 <b>Dropbox</b>	<b>66.1%</b>
<b>Google</b>	<b>43.8%</b>
 <b>Microsoft</b>	<b>33.9%</b>
<b>box</b>	<b>18.8%</b>
	<b>33.9%</b>
<b>OTHER</b>	<b>52.9%</b>

---

**MOBILITY MANAGEMENT:  
BLACKBERRY STILL  
DOMINATES.**

Mobility management was a category with a few surprises. Osterman Research found that: “In 30% of smaller organizations there are no mobility solutions in place – many smaller firms simply deploy and/or allow the use of individual mobile phones without any sort of MDM or MAM system to manage them. Those organizations that do deploy a mobility solution are using BlackBerry over 2:1 to any other brand.”

The lack of a solution in 30% of survey respondents could indicate that either IT admins at those SMBs have no real BYOD policy, or they are managing employee devices manually, which involves a significant amount of work. Both of these scenarios put company data at severe risk.

	<b>35.5%</b>
	<b>21.5%</b>
	<b>20.7%</b>
<b>OTHER</b>	<b>10.7%</b>

**ARCHIVING AND COMPLIANCE: IMPORTANT FOR COMPANIES OF ALL SIZES**

With the growing costliness of eDiscovery and the broadening definition of companies required to maintain regulatory compliance, email archiving and compliance solutions are becoming necessary rather than optional. Those SMBs without a solution of this type in place will need to rethink that decision in the future.

Given the negative impacts that can come from not having an archiving and compliance solution, we were surprised to note that 28% of Osterman Research survey respondents currently had not such solution in place. Those that did preferred Microsoft Exchange Online Archiving at a rate of 31% and Google at a rate of almost 28%. Symantec LiveOffice was the third-place favorite at roughly 14%.

 <b>Microsoft</b>	<b>66.1%</b>
<b>Google</b>	<b>43.8%</b>
 <b>Symantec™</b> LiveOffice	<b>33.9%</b>
 <b>Symantec™</b> Enterprise Vault	<b>18.8%</b>
<b>OTHER</b>	<b>52.9%</b>

**IDENTITY AND ACCESS  
MANAGEMENT: MICROSOFT  
PRODUCTS ARE THE TOP  
CHOICE**

Identity and Access Management (IAM) is category that has emerged with the increased move from on-premises IT solutions to cloud-based ones. These solutions provide IT with the ability to manage employee access to cloud apps while providing employees with an easier, more secure login experience. The best IAM solutions support 2-factor authentication for optimal security.

When looking at the answers of survey respondents, Osterman Research found that: "Microsoft's identity and access management (IAM) solutions dominate in smaller organizations, although a significant portion of respondents had no identity and access management solution in place. This puts those companies at a greater risk for regulatory non-compliance and unauthorized access to company data."

 <b>Microsoft</b> Active Directory Federation Services	<b>56.4%</b>
 <b>Microsoft</b> United Access Gateway	<b>11.7%</b>
 <b>McAfee®</b>	<b>10.6%</b>
	<b>10.6%</b>
 <b>Microsoft</b> Virtual Identity Server	<b>9.6%</b>
<b>OTHER</b>	<b>9.1%</b>

**OTHER CLOUD APPS: SMBS  
USE AN AVERAGE OF 3.29  
SPECIALIZED CLOUD APPS**

All the businesses surveyed by Osterman Research used several other cloud apps, including social media, CRM, accounting, payment systems, marketing management and documentation management apps. On average, each SMB deployed 3.41 of these apps across their workforce.

The “Other” category of cloud apps represents the broadest variety of specialized apps that tend to be used only by segments of a company’s workforce. This requires IT to more purposefully manage access to these apps and more carefully track how company data is being used. For example, company financial data is highly confidential, so IT needs to make sure that only the appropriate members of the company’s finance team have access to the cloud app where this data is stored.

	<b>62%</b>
	<b>42.6%</b>
	<b>28.7%</b>
	<b>27.8%</b>
	<b>23.1%</b>
	<b>21.3%</b>



**INTERMEDIA** The Business Cloud™

Sources: Osterman Research, The Benefits of Vendor Consolidation and Centralized IT Management, June 2014; Bureau of Labor Statistics, Table B 2014; 2013 Data Breach Investigation Report, Verizon, 2013

Copyright © Intermedia.net, Inc. 1995 - 2014. All Rights Reserved.