Six Reasons You Must Bring Unapproved SaaS Out of the Shadows

OVERCOMING THE FEAR OF SHADOW IT

CoreView

Six Reasons You Must Bring Unapproved SaaS Out of the Shadows

Overcoming the Fear of Shadow IT

By Doug Barney

The old saying "what you don't know can't hurt you" is turned on its head for IT. Here, what you don't know truly can and indeed does hurt you.

When it comes to end user devices, IT pros can only secure those machines they know about. Likewise, software, especially SaaS solutions, are only safe if they are brought in and managed by IT.

Shadow IT sounds cool on the surface. Tech-savvy end users and departments discover hot cloud apps they love and put to work. However, there are security, cost and even productivity downsides. Cloud apps that are that good should be vetted, and if proven, approved and even made standard. Ones that do not meet this threshold have no place in the enterprise. Finding the right answer means discovering and analyzing these hidden apps.

Shadow IT is inevitable. Sometimes referred to as Rogue or Stealth IT, Shadow IT are those applications, largely SaaS, that employees set up and use without IT permission — and usually without IT knowledge.

Shadow IT is a very big deal. Did you know a Cisco survey of CIOs shows they had 15 times more cloud applications than expected?

The old saying *"what you don't know can't hurt you"* is turned on its head for IT.

Here, what you don't know truly can and indeed does hurt you.

1. Shadow IT Wastes Money

According to Gartner, Shadow IT represents 30 to 40 percent of IT spending in large enterprises. Even more shocking, the Everest Group argues that spending on technology that is outside IT budgets and control is half or more of total spend on IT. Meanwhile, cloud and data center solution provider ServerCentral believes that in 10 years, 90 percent of all IT spending will come from outside the IT organization itself. Sounds like the Shadow IT problem is on its way to becoming far worse.

Cisco research finds the average large enterprise uses over 1,200 cloud services and 98 percent (1,176) of them are in essence Shadow IT. Many of these Shadow apps are a waste of money since there are already corporate standard apps that handle these functions, and in too many cases the Shadow tools are either malicious or present other security vulnerabilities.

Finally, a Logicalis CIO survey found that 90 percent of CIOs are simply bypassed by line-of-business managers in IT purchasing decisions some of the time, and 31 percent if CIO are bypassed on a routine basis.

This all means your IT team is not in charge of what happens to Shadow IT data. Instead, these Shadow apps are left in the hands of non-IT pros who are not experts in software standardization and management practices.

Cisco research finds the average large enterprise uses over 1,200 cloud services and 98 percent (1,176) of them are in essence Shadow IT.

Many of these Shadow apps are a waste of money since there are already corporate standard apps that handle these functions, and in too many cases the Shadow tools are either malicious or present other security vulnerabilities.

2. Shadow IT Insecure

Shadow IT causes all kinds of problems. It is a huge area of attack by hackers, and a vector for malware. Meanwhile, storage, filing sharing and collaboration apps are all key sources of data leakage.

Shadow IT is clearly ripe for attack, as Gartner researchers predict that this year, 2020, one-third of all successful attacks on enterprises will be against Shadow IT resources.

"Many IT decisions are now distributed throughout the organization at the line-of-business level. From a security point of view, it's a nightmare scenario," says Larry Ponemon, founder of the Ponemon Institute, a technology research firm in an IBM sponsored study. "People at the business level may not have any knowledge at all about security, and they may be using these tools in ways that put the organization at great risk." The study, "Perception Gaps in Cyber Resilience: Where Are Your Blind Spots?" argues that some 1 in 5 organizations suffered a cyber-attack due to Shadow IT.

Meanwhile, research from Skyhigh Networks finds that most SaaS providers come up short when it comes to security, and less than 10% of these providers meet the strong security requirements large enterprises need. In fact, just 2.9% of these services require strong passwords, and just 1% encrypt data with data keys controlled by customers.

Shadow IT causes all kinds of problems. It is a huge area of attack by hackers, and a vector for malware.

Meanwhile, storage, filing sharing and collaboration apps are all key sources of data leakage.

3. Top Execs Care About Shadow IT

Information Security (InfoSec) folks are definitely interested in Shadow IT, it is part of overall Governance, Regulation and Compliance (GRC) efforts. Generalist IT managers also want to know what is going on across their organizations.

IT Finance largely worries about Shadow IT apps that are paid for, those that waste money. They should also worry about fast-growing unpaid solutions because those tend to become paid. However, their focus is typically on dollars being spent now.

There is an answer – Alpin technology from CoreView. "It is hugely interesting to have usage monitoring and spending on just one screen. They can get the spending for a specific SaaS tool from a certain date to a following date, as well as other dimensions such as department, teams or location," said Julien Denaes, co-founder of Alpin and now vice president of CoreView which recently acquired Alpin. "Slicing and dicing cost and usage data has many uses in analyzing performance and projecting future spend. This is also crucial when there are mergers or acquisitions."

IT Finance largely worries about Shadow IT apps that are paid for, those that waste money.

They should also worry about fast-growing unpaid solutions because those tend to become paid.

However, their focus is typically on dollars being spent now.

4. Shadow IT Apps Not Always Well Maintained

IT pros know that Microsoft had long had a disciplined approach to maintaining, updating and patching their on-premises products. Today top SaaS providers maintain and patch their software as part of the subscription, closing vulnerabilities and addressing new cyber threats.

However, not all SaaS providers are created, and IT does not know how well Shadow IT SaaS providers update and secure their software. "One of the biggest problems that emerges from SaaS usage is unpatched or out-of-date software. While many SaaS applications perform automatic updates, some do not. When software is left unpatched, it creates security gaps and opens systems to attacks that have already been rendered useless by new patches," argued an article in Dataconomy. Most importantly, unpatched software has a real cost. Equifax's data breach, itself the product of unpatched vulnerabilities, cost the company an estimated $5 billion in market capitalization.

Today top SaaS providers maintain and patch their software as part of the subscription, closing vulnerabilities and addressing new cyber threats.

5. Blocking SaaS Access Doesn't Always Work

Many companies attempt to block access to cloud services that do not meet their acceptable use policy. Skyhigh points out, however, that there is a vast discrepancy in the intended block rate and the actual block rate. Skyhigh calls this the "cloud enforcement gap." The gap arises when cloud services introduce new URLs that are not blocked, or when access policies are not standardized throughout the enterprise, or when certain groups get an exception to access various services. This cloud enforcement gap represents…You guessed it, Shadow IT.

Many companies attempt to block access to cloud services that do not meet their acceptable use policy.

Skyhigh points out, however, that there is a vast discrepancy in the intended block rate and the actual block rate.

6. SaaS and Shadow IT Discovery is Important to Office 365 Application Optimization

With Alpin, you can identify SaaS solutions that you might want to migrate away from to something else that is already provided as part of Office 365. "Microsoft is really pushing on adoption of Microsoft Teams, pointing out to customers just how much functionality is built into this Office 365 workload. Customers need to understand who is on WebEx, who is on Zoom, and who are their Slack users in order to migrate them to Microsoft Teams. "This discovery is immensely useful for Office 365 shops. They can see that many workers are not using core Office 365 applications, but instead using Shadow IT apps that are not a corporate standard. This wastes money since Office 365 is already paid for, and creates a huge security problem and data leakage vulnerability," said Denaes. "Having a way to discover those users on those applications is a way to help them migrate them – to redirect users to adopt the right tool – which is Microsoft."

With Alpin, you can identify SaaS solutions that you might want to migrate away from to something else that is already provided as part of Office 365.

Shadow IT Damage: Real World Examples

Alpin helps enterprises find thousands of Shadow IT apps, and stop the damage they cause.

Here are some examples:

Security and Compliance: An enterprise was hit by an attack from game company trying to get employees to download a game, which turned out to be an egregious form of Shadow IT. This gaming site subscription had full access to many company email inboxes, including access to CEO and CFO inboxes and all their sensitive contents. "The most famous Shadow IT example is a so-called game developed on Android. The game developer was purportedly based in the Netherlands, but was in fact a Russian company. This game accessed all the emails, not only the headers, but the content of all the people installing that game. CEOs, CFOs, CIOs had all given permission to this game that was really a Russian company reading all your emails," said Julien Denaes, Alpin co-founder and now CoreView vice president.

Solution: Alpin discovered the offending app and permissions that led to the situation, and provided the tools to solve it. "We reported this to our customers, and guided them to blacklist this application. They were extremely thankful of course," Denaes said.

License Compliance and Cost Overruns: Duplicate apps are a waste of money, and having more than one app to solve a problem, say, manage projects, saps productivity and kills collaboration. One Alpin customer had many teams each with their own Slack domain, and were all unaware that a corporate Slack account existed. Costs overlapped and added up to huge waste.

Similarly, another organization found not **one**, but **five** duplicate project management apps outside of IT's purview, spread throughout the company. This created massive cost overlap and security vulnerabilities – how much sensitive data may have been stored in the other apps?

Solution: Alpin's extensive discovery tools identified these otherwise hidden instances, giving IT the data and contact information needed to remedy these issues.

Security and Compliance: File storage SaaS tools such as DropBox are notorious for data leakage and theft, and little is more terrifying than hackers accessing executive files. In this case, a finance director, through a cloud file storage app, was sharing a **root-level** folder with outside parties. That inadvertently provided access to detailed financial statements that would never be released publicly or shared. Salaries, P&L, and more were unintentionally exposed.

A team's files, folders, and discussions were made completely public rather than internal and read-only – this made financial files and other sensitive information **indexable by search engines**.

Solution: Alpin's discovery and cloud Data Loss Prevention (DLP) tools provided the information needed to pinpoint the data leakage and change the relevant settings.

Shadow IT Damage: Real World Examples

Cost Overruns and Worse: Alpin's customers have experienced multiple cases of a scary lack of oversight – and the damage they do. For instance, a large technology company's ex-employees – up to three years gone – had access to multiple cloud apps, including the company's CRM. Not only was this a waste of money, it put years of potentially sensitive information at risk.

In another case, an expense and approval system kept IT and procurement in the dark about cloud software purchases. A manager approved employees' software expenses without intervention or detailed purchase audits.

Solution: Alpin discovered these mystery users and programs with tools previously unavailable to IT leadership. With knowledge in-hand, IT could address or correct these issues.

Compliance and Cost Concerns: Finding Shadow apps is the foundation for discovering if known cloud breaches are cause for alarm.

After a recent data breach from a cloud software provider, multiple companies wanted to know if they were affected. Without Alpin, they had no way to know, for sure, if their users were exposed by the vendor's breach. With Alpin, they got notifications about the affected app, as well as who was using it, so they could lock down their exposure.

Another company found over 3,000 SaaS apps when they expected to find a few hundred.

Solution: Whether it's general discovery or looking for a specific app, Alpin sheds light on cloud software ecosystems. Solving shadow IT problems starts with good discovery.

Unwanted Surprise: In one enterprise, users set up a small trial of a video conferencing app that quickly spread department-wide -- and could easily have spread enterprise-wide. It was an expensive solution not subject to negotiation or cost controls. A department head even committed IT to supporting the new application, taking IT completely by surprise.

Solution: Alpin can track down all instances of the new application to help sort out the prickly situation. In this case and others, knowledge is power. Revealing Shadow IT serves as a powerful tool for IT leadership.

CoreView Bought Alpin to Solve Shadow IT Problem

Last year, CoreView bought Alpin for its broad SaaS management and discovery ability. Alpin tracks more than 40,000 SaaS apps, using 13 discovery methods, giving IT a full picture of their SaaS environment. With Alpin discovery, you will:

- **Gain visibility** - view all SaaS applications in one dashboard, along with all their users.
- **Work with the business** - help business users choose the best solutions and use those apps to their full potential.
- **Spot trends** - see app growth among teams, departments, geographies and across the company.

With the acquisition, CoreView now offers granular user-specific and application-specific controls that identify all SaaS applications in use, monitor activity, and offer additional features such as "Blacklisting" (blocking admin-selected SaaS applications from use), "Lockdown" (blacklisting every existing and/or new SaaS application in emergency situations), highlighting file and email data leakage, showing vendor security certifications, and more.

Five Shadow IT Question to Ask

1. Do you have a detailed and comprehensive list of applications your end users use? What categories do these apps comprise (e.g., collaboration, file storage, CRM, chat, or project management)?

2. Which applications are used the most? Does this speak to an unmet need that should be addressed through adoption and standardization? In contrast, which SaaS tools are redundant, wasting money and causing inefficiencies?

3. Which Shadow IT apps harbor the potential to hold confidential, regulated, sensitive, or proprietary data? Does your IT staff have visibility into how this data is created, transferred, and stored?

4. Does your IT group currently have the ability to identify SaaS applications and create and implement effective SaaS usage policies?

5. Do you have security controls to protect SaaS applications from data breaches?

Issues Created by Shadow IT

Data Security Problems – Data can be accessed from former employees, breaches can occur, permissions attacked because they are not managed by IT.

Regulatory and Compliance Disasters – SOX, GLBA, HIPAA, GDPR and others violated because data and data access is not secured – or understood!

License Compliance Violations – Freemium or shared accounts can put your approved SaaS contracts in jeopardy.

Cost Overruns Out of Control – With Shadow IT, your end users are often paying for applications already served by corporate standard SaaS solutions, wasting money through vast redundancies. Shadow IT gets in the way of good IT software negotiations and proper, efficient provisioning.

Misallocated Costs – Finance and accounting need accuracy, knowing what software is acquired, billed for, and renewed to optimize investment.

Missed Financial Goals or Targets – If procurement misses savings goals due to unforeseen expenses from Shadow IT, it may lead to unintended cost-cutting measures.

Loss of Respect for IT – Shadow IT leads employees to question the judgement of IT (they know better than IT does what software makes sense), and security and productivity problems caused by Shadow IT can be blamed on IT.

Learn more from Alpin's Shadow IT Problems blog.

About the Author

Doug Barney was the founding editor of Redmond Magazine, Redmond Channel Partner, Redmond Developer News and Virtualization Review. Doug also served as Executive Editor of Network World, Editor in Chief of AmigaWorld, and Editor in Chief of Network Computing.

Learn more about the new SaaS Management powerhouse:

Explore the Alpin solution – Alpin Co-Founder's Magical Mystery SaaS Management Tour

Dive into our white paper – 1+1=3: CoreView and Alpin are the New SaaS Management Platform (SMP) Powerhouse

Learn more about Shadow IT and SaaS management with an Alpin demo, or visit the CoreView/Alpin web page.

You can also get a free CoreView Office 365 Health Assessment that details license savings, state of application usage, and pinpoints security problems in your Office 365 environment.