Kaseya ACCELERATE Online!

EBOOK

HOW TO AVOID BEING SPOOKED BY SHADOW IT

STRATEGIES FOR SHINING A LIGHT ON CLOUD SERVICES IN YOUR ORGANIZATION

Shadow IT: Permanent Nightmare or Fleeting Cloud?

In many ways the rise of Shadow IT was inevitable. Shadow IT, sometimes called stealth IT or rouge IT, refers to the IT applications and infrastructure employees deploy and use without IT department authorization — and often awareness — to accomplish tasks and projects. While Shadow IT can include hardware, it most often is used in reference to software, web services, or cloud applications.

Many factors have contributed to the rise of Shadow IT, but its roots can be traced back to the end of the mainframe era. As employees transitioned to PCs, they slowly gained greater control over their individual computing environments. With IT's control and business unit requirements, users were able to personalize based on roles on preferences. As the trend shifted to the consumerization of IT, employees increasingly expected their workplace tools to be as innovative and sophisticated as their consumer counterparts, and they increasingly found ways to incorporate them.

The rise of cloud services only exacerbated this. As companies across all industries embrace popular enterprise cloud services, such as Office 365, Salesforce and Box, other applications have also found their way into organizations. Along with that has come new questions about how IT can protect data that is now dislocated from storage that is in their direct control.

> ...employees increasingly expected their workplace tools to be as innovative and sophisticated as their consumer counterparts, and they increasingly found ways to incorporate them.

GARTNER studies have found that Shadow IT is 30 percent to 40 percent of IT spending in large enterprises.[1]

30%
40%

EVEREST GROUP found that technology spend external to IT actually comprises 50 percent or more of IT spending.[2]

50%

SERVERCENTRAL projects that within the next 10 years, 90 percent of IT spending will take place outside of the IT organization.[3]

90%

These figures aren't the least bit surprising when you consider the ease of purchase. In most cases, an email or a credit card is all that is needed. The resulting growth rate of Shadow IT is concerning to those tasked with overseeing it.

IT can't manage what IT can't see.

The old adage continues to be true. Shadow IT creates this dilemma. How can an administrator possibly secure the organization from cyber-attacks with such widespread adoption of applications that may have exploitable vulnerabilities?

This rapid adoption brings with it the benefit of increased productivity and agility, but the downside is that IT often has little to no visibility into the full scope of IT services employees are using. Without visibility, it becomes very difficult for IT to manage both cost expenditures and risk in the cloud.

Most organizations have guidelines as to how new software is introduced to the environment. There is a process in place in which comprehensive testing is done in a sandboxed environment before it is introduced into production. Bypassing these procedures enhances the risk of potential threats and attacks to the environment. This increases the risk for data loss and compromise.

Locking down all systems may seem like a good solution, but the reality is that there is no turning back the clock on Shadow IT. Users and lines of business are not going to give up the autonomy and speedy adoption of being able to select the optimal service or application for their use case, and they are quite comfortable bypassing IT to do so.

But the news is not all dark. Organizations that seek to manage Shadow IT rather than expend unnecessary energy fighting it will have a leg up. To succeed, you need an approach that enables you to achieve your security goals without hindering productivity and that allows your business users to access the tools they need without jeopardizing company data.

2

KEY THINGS

to keep in mind...

As you embark on a strategy to manage Shadow IT, there are two key things to consider.

Shadow IT is highly vulnerable.

According to industry analyst firm Gartner, by 2020, one-third of successful attacks enterprises experience will be on their Shadow IT resources. Why is Shadow IT such an easy mark? The answer stems from the implementation of applications outside of IT's realm.[4]

IT organizations have guidelines to how new software is introduced to the environment. There is a process in place where proper testing is done in a sandboxed environment before it is introduced into production. When these procedures are bypassed, the risk of potential threats and attacks to the environment goes up, increasing the potential for data loss and compromise.[5]

In addition, many of the cloud services used are consumer-grade and thus do not meet the strict security and governance needs of an enterprise. This makes understanding the services employees are using, the types of data that are uploaded and shared, and the security capabilities of these services even more critical.

Shadow IT buyers aren't skilled at managing data.

Per a recent Logicalis CIO survey, 90 percent of CIOs worldwide are bypassed by line-of-business leaders in IT purchasing decisions sometimes, and 31 percent are bypassed routinely. Not only does this result in the security problems described above, but it also means that skilled IT resources cannot influence what happens to Shadow IT data. Non-IT pros aren't schooled in software standardization and integration practices; nor do they understand or communicate best practices for introducing new applications to their constituents.[6]

And, contrary to popular belief, malicious cyber-attacks aren't the biggest threat. Logicalis found that while only 7 percent of lost organizational data is actively hacked, 81 percent of lost data is stolen or inadvertently disclosed.

Further, Gartner estimates that by 2020, one-third of successful attacks will be on data located in Shadow IT resources.[7]

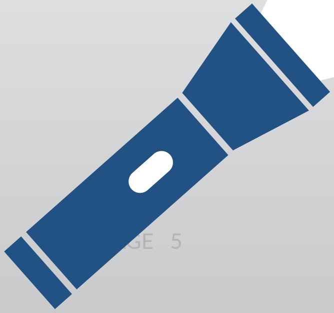
The Hidden Challenge:
Shine a Light on Third-Party Applications

2017 was billed as the worst year on record for cybersecurity. No doubt, the continued rise of modern threat vectors has IT on high alert. In essence, IT professionals view their role as responsible for keeping the door shut. However, even with IT administrators keenly aware that most exploits can be averted simply by keeping the environment current, the task is no small feat and one that often isn't done as well as it needs to be.

Only two-thirds of IT shops spend any time managing third-party applications, according to the **2018 Kaseya MSP Benchmark Survey Results Report**. It is highly unlikely these applications are updated in a thorough manner, as dealing with Mac or third-party software is typically viewed as an afterthought and an annoyance.[8]

THE HIDDEN THREAT in securing your infrastructure from vulnerabilities lies with IT's difficulty in managing third-party software.

However, criminals do not sit still. They know that as the operating system becomes a less-viable means to wreak havoc, they need to shift their focus. And they know that third-party software presents a gaping hole that IT administrators have challenges managing.



The VSA Effect

How Patch Management Ensures a Clear View for Methodist Healthcare Ministries

Methodist Healthcare Ministries (MHM) of San Antonio, Texas relies heavily on VSA by Kaseya. With most breaches impacting unpatched computers, keeping machines up to date is an essential safeguard for the organization. "I use VSA for Windows patch management, instead of having to have three or four different servers just to manage the patches. Everything is agent-driven right now. I have about a 92-percent patch rate within a week of when a new Microsoft patch is released. It is easy to set up. I did not have to tie in with everything else. You set up your policies and automation — and let it go," said Roy Herron, systems analyst for MHM.

Multiplatform capabilities are also essential. "I am excited about the ability to patch Macs. Usually there is no centralized mechanism for that. In the enterprise arena, you usually build your own Mac server to do that. VSA cuts down on the cost of standing up different servers to do different things," Herron said. A broad software reach is more than handy. "It patches third-party software, not just the Microsoft Windows updates. I patch Firefox, Java some Adobe Flash. That is a big help. Otherwise, you probably have to send somebody out to physically patch each system, or spend tens of thousands of dollars on SCCM or SCE from Microsoft," he said.

Meanwhile, the unified interface makes tasks easier to perform and manage. "The single pane of glass lets me see a group of our users and patching states. I can push everything out from my desk. Over the course of the day, it saves me probably three hours walking around," Herron explained.

Assess and Take Action

Shadow IT is not unmanageable. It is possible to support Shadow IT, but only if the IT organization has a solution in place with robust endpoint management capabilities that enables them to see all assets and software on the network. IT then can take the critical first step in making sure applications are in line with the organization's software and vulnerability management policies.

5 Critical Questions

you should be able to answer related to Shadow IT visibility and control

What is the comprehensive list of applications your end users are using? How does this vary across departments? What functional categories do they fall into (e.g., file storage, chat, or project management)?

Which applications are finding widespread adoption? Is this due to an unaddressed need that should be sanctioned for organization-wide use? On the opposite end, which applications are redundant and are causing inefficiencies?

Which applications bear the potential to harbor sensitive, regulated, or proprietary data? Do you have full visibility into the generation, transfer, and storage of this data?

How confident are you in your ability to identify cloud applications and implement effective cloud use policies?

Are there appropriate access security controls implemented to protect cloud applications from data breaches? For both internal access and for third-parties or partners?

Your Shadow IT Solution Starts with Automated Patching, Software, and Vulnerability Management

After identifying rogue software and applications, the next step is to develop a method to update and maintain them to mitigate threat vectors that could attack your network. Any meaningful approach to managing this software requires actively managing both operating systems and third-party applications that users can self-install.

In short, the time is now to modernize your software and vulnerability management strategy.

There are three core components of a modern software and vulnerability management strategy.

3

Core Components of Modern Software & Vulnerability Management

1. Unified Management

Install, deploy, update, and patch often require different workstreams. The load on IT is tremendous and wasteful. IT needs a software management solution that specifically reduces complexity by unifying how software is managed, regardless of platform or application.

2. Comprehensive Visibility

Manually looking across a multitude of interfaces is not workable in the quick pace of today's IT environment. IT needs a solution that offers a single pane or dashboard to quickly aggregate the visibility of the vulnerability landscape relevant to the specific environment under management.

3. Scalable Automation

Auto-accept and deploy are the new normal. But IT administrators cannot blindly lose control for the sake of scale and automation. IT administrators must invoke critical control by use of profiles and policies.

Get Started Today The time to get started with a modern software and vulnerability management strategy is now.

Contact Kaseya to learn how we can help you transform your approach.

1 https://www.cio.com/article/3188726/it-industry/how-to-eliminate-enterprise-shadow-it.html
2 https://www.everestgrp.com/2017-04-eliminate-enterprise-shadow-sherpas-blue-shirts-39459.html
3 http://blog.servercentral.com/three-benefits-of-shadow-it-and-how-to-harness-them
4 https://www.quickbase.com/blog/5-shadow-it-statistics-to-make-you-reconsider-your-life
5 https://www.forbes.com/sites/forbesproductgroup/2017/02/22/shadow-it/#205a7c579fd0
6 http://www.us.logicalis.com/CIO2015
7 https://securityintelligence.com/spotlight-your-data-within-shadow-it
8 https://www.kaseya.com/resources/best-practices/2018-msp-benchmark-survey-whitepaper

About Kaseya

Kaseya is the leading provider of complete IT management solutions for managed service providers (MSPs) and midsized enterprises. Through its open platform and customer-centric approach, Kaseya delivers best in breed technologies that allow organizations to efficiently manage and secure IT. Offered both on-premise and in the cloud, Kaseya solutions empower businesses to command all of IT centrally, easily manage remote and distributed environments, and automate across IT management functions. Kaseya solutions manage over 10 million endpoints worldwide.Headquartered in Dublin, Ireland, Kaseya is privately held with a presence in over 20 countries. To learn more, visit www.kaseya.com.

06062018

Kaseya®
EBOOK