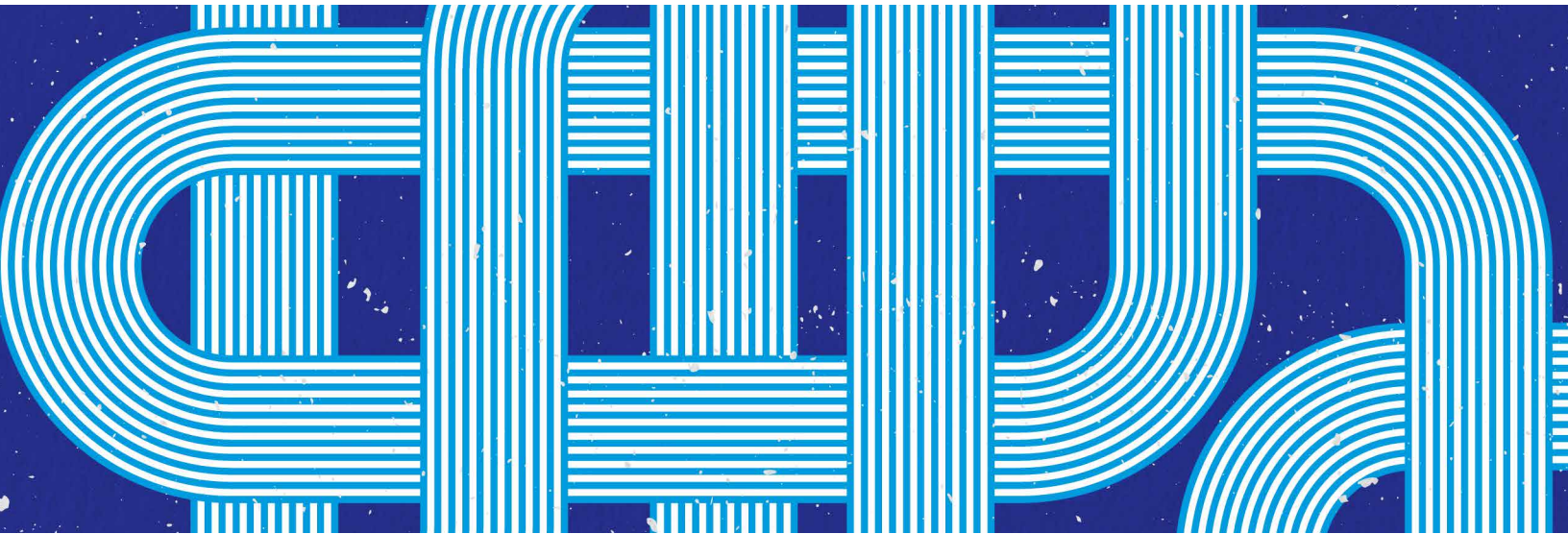


THE IT
MANAGER
WHO SHATTERED
SHADOW
IT





Confronting Shadow IT and Taking Back Your Software Stack

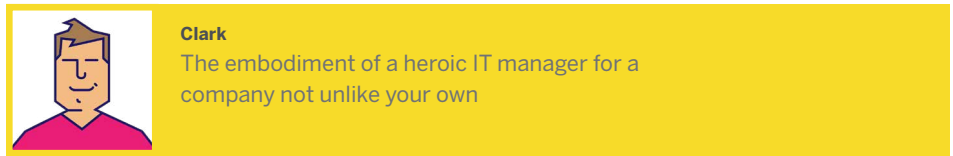
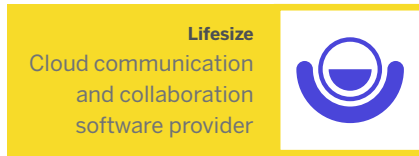
Shadow IT has become a household (or office-hold) name in today's modern businesses, but what a lot of organizations don't realize is the number of risks involved in ignoring those rogue technology installations. [According to one study](#), the average large enterprise uses around 1,220 individual cloud services, which is more than 13 times the 91 services recognized by IT departments. Not only does Shadow IT go directly against IT departments, it can also create security vulnerabilities and unnecessary costs. Employees typically engage in Shadow IT because they think it will save their company, and IT department, time and money. In reality, going around IT just bypasses the critical management, integration, and security and compliance-related safeguards that they support.

Imagine a world in which Shadow IT has permeated every inch of the enterprise, and, more than anyone ever could have imagined, threatened the security, profitability and efficiency of the entire company. It's the Wild West — gunfights in the streets, damsels in distress and old-sounding saloon pianos chiming in the background. Enter Clark the IT manager (and hero of this story), his boss Cynthia the CIO and his trusty sidekick Steve the sys admin. The three sit silently together. Their department has lost control, and no one knows for certain which technologies are being used across the organization. The consumerization of IT, or the cycle of employees bringing popular consumer market technologies from home into the office, has made it easy for employees to deploy technology while leaving the IT department in the dark.

This problem isn't a unique issue for Clark and his team. In an [Intel Security survey](#), 23% of respondents said their departments handle security without IT's help.

One day, Clark decided to draw the line. He was sick and tired of being controlled by the whims of Shadow IT, sick and tired of not knowing what technology was being used to keep the business running. So he decided to do something about it. He rallied his team, built a plan of action and charged headlong into battle against Shadow IT.

As a company that depends heavily on the approval of the IT department, we wanted to learn more about Clark's thoughts on rogue applications and get a better understanding of his systematic approach to confronting Shadow IT and building a more transparent IT management culture.



Lifesize: How did you find the problem? What did you do to find the worst offenders?

Clark: It started with an article I read that claimed, "[Seven out of every 10 executives don't know how many Shadow IT applications are being used within their organization.](#)" I was curious to see if that fact was true in my company. Oftentimes my team would hear about all these different applications that departments used in the office, but no one would come directly to us about it. And while some were benign, others were potentially malicious — and we couldn't afford to risk anything. We started to monitor closely to see if any new and unknown tools or applications popped up in our regular scans, which resulted in an enterprise-wide vulnerability scan.

Lifesize: Did you receive pushback when your IT organization couldn't support some of the desired tools of a department?

There are programs specifically created to spot new applications on the network. Network sniffers and security scanning tools can provide detailed information on new and unknown data streams. Of course, monitoring doesn't completely remove the threat of shadow IT, but it does provide insight. Not only did this scan show us that our employees were using tools we were unaware of, it gave us enough information to start risk assessments and, in the worst cases, research alternative solutions that better aligned with our requirements.

Lifesize: How did you get your employees to come forward with information about their Shadow IT? That must have been challenging.

Clark: Of course. We support a lot of teleworkers at our company, and one of the challenges we quickly discovered is that if you don't have IT-approved ways of enabling employees to work remotely or on the go, they'll find their own ways to do so. That's when things get risky, with unsecure document transmission, lost or stolen devices, and so on. We found that by being transparent about our security and network requirements and encouraging our employees to reach out to IT during the discovery phase of new software, we were included in more discussions and better positioned to make the final selections. You'd be surprised how happy people are to have your help searching for and selecting solutions instead of beating around the bush and trying to figure it out on their own.

Lifesize: How did you maintain consistency with this strategy? Your Shadow IT problem is fixed now, but how do you ensure it doesn't creep back into your company?

Clark: It was at first. Shadow IT represents an unmitigated hazard only for those companies unwilling to address it, so we addressed it. The tendency is for IT organizations to break down doors and threaten jail time to those using unapproved software, and that seemed a little harsh for my taste. We decided to take the peaceful approach, so we offered safe haven for those departments utilizing Shadow IT. Instead of taking these programs over immediately and shutting them down, we took a step back, determined the risk and offered comparable solutions where needed to achieve the outcome the business units were looking for. That also allowed us to open up a dialogue about the risks associated with each program. This exercise really got us all on the same page and established a trust and candidness between "us" and "them."

Lifesize: Having successfully combated Shadow IT, what advice do you have for IT departments just starting to deal with the issue in their organizations?

Clark: You know, a lot of people have asked me this question, and the answer is fairly simple. It comes down to relationships. I built a rapport with every department head, met regularly to discuss technology strategy and created an open dialogue between the departments and the IT organization. Furthermore, it was essential that my boss, Cynthia the CIO, maintained close contact with the rest of the e-staff on technology transparency and the potential risks of adopting unapproved technologies.

Clark: Take advantage of creating an open dialogue with your colleagues across the company — your customers. Listen to their feedback, learn more about the problems they're trying to solve and be willing to provide input. I once had a request to review a tool that was already approved and deployed by another department in the organization. In this case, it was a lot easier, and a lot cheaper, to adjust our plan to add a few more licenses than it would have been to start a whole new contract. The last piece of advice I'll leave you with is don't underestimate the power of a simple user interface. Be sure to balance your security and network requirements with the end usability of the applications. One of the things I like to look for is a solution that integrates with our SSO. That will just reduce the number of passwords that employees need to keep track of and update throughout the year.

The IT Manager Who Shattered Shadow IT



Combining poor password practices with Shadow IT applications can create significant security vulnerabilities. Check out our blog, [The Best Defense Against IoT DDoS Attacks](#), to protect your network.

About Lifesize

Lifesize is an IT-approved collaboration system because we're built with IT in mind to provide security, resiliency and network reliability. We have more than a decade of experience designing HD cameras and touchscreen phones under our belt, and our intuitive interface and shared directory gives users everything they need to collaborate more effectively through IT-approved applications — eliminating the need for additional rogue applications. Lifesize communication streams support 128-bit AES and TLS (Transport Layer Security) encryption for all signaling by default, and we operate on a private 2,000 Gbps fiber network through IBM Cloud. To top it all off, we stand behind our award-winning service with a financially backed service-level agreement (SLA) with 24x7x365 support.

[Take a Tour of the Lifesize App](#)

[Download a Free 14-day Trial](#)

Learn More

[Eight Challenges Solved by Cloud Video Conferencing](#)

With cloud video conferencing, you can collaborate at any time at any place with anyone. Check out our guide to see how cloud video conferencing solves common business challenges and changes your organization for the better.

[Mind the Gap — Five Ways to Enhance Connectivity in a Scattered Workforce](#)

Cloud video conferencing plays a crucial role when communicating with a remote workforce. Listen to our webinar to learn how to enhance workplace relationships and be more collaborative, even without physically being there.

[Lifesize Icon Series Guide](#)

Lifesize knows that a one-size-fits-all system could never be the right fit for all the different meeting spaces in your office. From software to hardware, our products are built to serve you. We have more than a decade of experience designing HD cameras and touchscreen conferencing phones, so find what product fits best for your company by checking out our guide.

[Five Must-Haves for any Great Huddle Room](#)

Huddle rooms, or small meetings spaces, have taken the modern office by storm for a reason. Not only do they promote collaboration, they're also agile and cost-effective. See what else your huddle rooms need to be the most productive they can be.

SOURCES

<http://blogs.cisco.com/cloud/shadow-it-rampant-pervasive-and-explosive>

<http://www.csoonline.com/article/3083775/security/shadow-it-mitigating-security-risks.html>

<http://www.digitallistmag.com/resource-optimization/2016/02/11/2016-state-of-shadow-it-04005674>

HEADQUARTERS

Austin, Texas, USA
+1 512 347 9300
Toll Free US +1 877 543 3749

APAC REGIONAL OFFICE

Singapore
+65 6631 2831



www.lifesize.com
E-mail: info@lifesize.com



EMEA REGIONAL OFFICE

Munich, Germany
+49 89 20 70 76 0

© 2017 Lifesize, Inc. All rights reserved. Information contained in this document is subject to change without notice. Lifesize and the Lifesize logo are registered trademarks of Lifesize, Inc. All other trademarks are the property of their respective owners.

Guide_Shadow-IT_0117