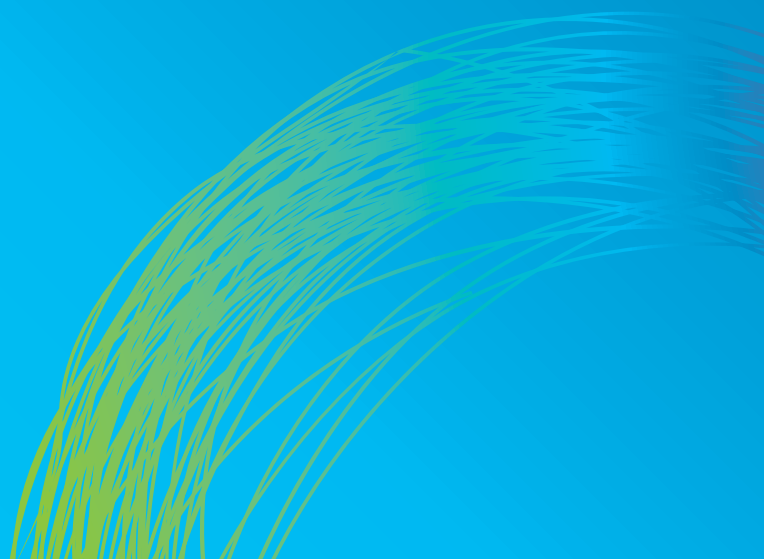
Shadow IT vs. Information Security

Whitepaper



Introduction

Prior to about 2005, storing your files on the internet was hard work. Most software came on a CD-ROM. Doing something like creating Network Attached Storage (NAS) required hundreds of dollars in equipment, plus the intervention of an IT professional (for business users) or dozens of hours reading online tutorials (for users at home). No one anticipated that the cloud would revolutionize productivity - just as no one realized the potential consequences for information security.

In 2005, of course, Box made its debut, followed by Amazon Web Services, followed by DropBox, followed by the cloud-migration of what seems like every piece of enterprise software ever created.

At this time, the cloud became easy to use, and basically free. According to the NIST, one of the primary features of cloud computing is that it must enable users to essentially self-provision. In that regard, cloud storage and other SaaS services have delivered magnificently - users can sign up for online storage, file-transfer, data-visualization, IP phone, and IM services, all without the assistance of a single admin. None of these services require a user to install a single program other than their browser.

For IT professionals, the widespread proliferation of cloud services has been somewhat less than thrilling. Imagine, for example, that scientists discovered how to make nuclear weapons out of baking soda and vinegar. Much in the same way, cloud services have made dangerous activities easy. Users are now able to easily take sensitive information and put it in the hands of vendors who were never vetted for security. What's worse, if these vendors are hacked, IT will never know that data was lost.

Collectively, these unaccounted cloud, SaaS, and software applications represent the problem known as shadow IT. Much has been written about how the problem of Shadow IT has thrown huge hurdles in the path of governance, compliance, and data-loss prevention. These are all serious problems, but Shadow IT presents another serious risk - it is very nearly an open avenue for malware.

Threats Descending from Shadow IT

There are many justifications surrounding the use of Shadow IT - when business unit leaders or IT professionals decide that a given software or SaaS service is the preferred tool for a particular job, it shuts other employees out. Many employees will decide that they would rather use other software that they're already familiar with. Others will decide that the approved software does not adequately fit their needs. And then there are teams and departments who feel like they need tools and don't even consider IT as an approver – they can buy them online themselves. According to a study from IDG, 33% of IT spend will take place outside the IT department by 2019. No matter the reason that Shadow IT is chosen, the fact remains that these employees are exposing themselves to threats that they might never even have considered.

Here are a few scenarios that might lend themselves to a malware infection via Shadow IT:

Malicious File Upload

This scenario is also known as a "man-in-the-cloud" attack. It's relatively simple, and takes advantage of the fact that business units will often create unauthorized cloud storage in order to easily share and collaborate on their work.

The problem with these unauthorized cloud storage implementations is that their protection is only as strong as credentials of their least computer-literate user. Remember, it's relatively easy for attackers to steal users' credentials, and if a cloud storage isn't set up by IT, it may not be enabled with common protections such as multi-factor authentication, a cloud access security broker, or single sign-on.

Once a criminal has access to an unauthorized cloud storage, they could simply steal everything that's in there, and move along. Of course, there might be no valuable data in there, or the attacker might sense a larger payday. In that event, making a lateral move onto a corporate-owned endpoint is nearly child's play. The attacker simply has to upload a file infected with malware, and then change the settings of the cloud storage to sync that malware onto every connected device - desktops, laptops, and smartphones. From there, the criminal has nearly free reign.

MITM Attack

Say that shadow IT users aren't using a file storage app like Dropbox. Maybe instead they're using Google Sheets, Smartsheet, or some other service that doesn't lend itself quite as well to a malicious file upload. An attacker is far from thwarted in this scenario - they can simply go from being the man in the cloud to being the man in the middle.

Most users on the internet have probably experienced a man in the middle (MITM) attack - and some users undergo attempts several times a day. That's because MITM attacks are essentially the payload of many phishing emails out there, the kind that say "Your [SaaS service] may have been compromised. Please login here in order to rectify this problem."

Some of these attacks are pathetically transparent, of course, but a percentage of users will always fall for even a pathetic attack. As far as a more targeted attack is concerned, however, all bets are off. The success rate of targeted phishing attacks is staggering. According to the 2015 Verizon Data Breach Investigations Report, 23 percent of recipients will open phishing emails - and over ten percent will open attachments.

Once the target clicks on a suspect link, they're taken to a website that is constructed to look exactly like the frontend of a commonly-used SaaS application. This malicious site may be used for a number of purposes. Most commonly, they're used to capture credentials. More sophisticated versions of these malicious sites can even be used to capture and transmit the one-time passwords that are used for two-factor authentication. Harvested credentials can be used to loot connected cloud accounts, or plant malicious files for a man-in-the-cloud attack.

These sites can also be programmed to drop malware into the browser, however. With the browser thus infected, attackers can initiate a man-in-the-browser (MITB) attack. This kind of attack works on the same principle as MITM, but allows attackers to more completely capture the data that is transmitted between the browser and applications, potentially bypassing SSL, TLS, and other secure transmission protocols.

Watering Hole Attack

Building a convincing fake frontend is time consuming, and there's always a chance that users won't fall for targeted spear-phishing attacks. In some cases, it's easier for attackers to just take over the real deal, in what's known as a watering hole attack.

This tactic obviously wouldn't work - or at least one would hope - with the larger, more well-known SaaS applications like DropBox, Salesforce, Outlook, and so on. However, this works in favor of attacks against Shadow IT. DropBox, Salesforce, and Outlook are very likely to be the official cloud solutions of choice for the enterprise. Shadow IT users are much more likely to invest in smaller, lesser-known solutions that they believe offer better options for their workflow. These services may not have the same level of security as the larger SaaS options.

Once infected, these services will infect a large-percentage of users that visit them. One popular technique is the use of Angler, an exploit kit that can bypass many common Windows protections. Angler, in turn, is popularly used as a conduit to load ransomware onto users' machines. Depending on the popularity of a given Shadow IT service, and an enterprise's ability to detect malicious software, an entire business-unit's worth of endpoints might become infected before anyone notices.

Strategies for Dealing With Shadow IT

The big weakness in the enterprise is that all SaaS applications, whether they're approved or not, tend to go through specific ports in the firewall. These ports tend to be unmonitored for that reason. Shutting down those ports, or monitoring them with a firewall/IDS, could lead to a commensurate slowdown in business-critical applications.

Many strategies for dealing with shadow IT suggest that the operative technique is lenience: "just let employees use the tools they want to!" To a certain extent, this is good practice. Penalizing employees who want to use services that the enterprise hasn't approved will simply encourage them to hide their activities better. This exposes the organization to security risks. It is far better to encourage employees to tell IT when the most-favored solution isn't working for them, and the place those services under the protection of the enterprise security architecture.

Common strategies include adding formerly unaccounted SaaS offerings to a single sign-on (SSO) platform, in order to deter credential theft. These services can also be monitored by data-loss prevention (DLP), which would prevent employees from uploading sensitive data to certain parts of the cloud. Lastly, a next-generation firewall might be able to monitor connections to SaaS services that a traditional third-generation firewall might miss.

These strategies are all incomplete, however. No incentive towards full disclosure will ever be one hundred percent successful - there will always be one employee who will decide to use a SaaS app without telling IT. What's more, if your employees telecommute, and use computer that our outside the corporate network, they may be able to de facto avoid security measures such as DLP and next-gen firewalls.

Because it is still so easy for employees to use SaaS services that were never cleared by IT, firewalls have effectively been rendered porous. Endpoints, not firewalls, are the true perimeter of an enterprise network. The only real way to protect the enterprise is to protect the endpoint.

SentinelOne

SentinelOne offers a next-generation endpoint protection solution that is highly resilient to forms of advanced malware, including ransomware. This solution relies on full-context behavioral detection, not signatures, in order to identify and deflect malware. What's more, this system can trace any malware infections back to their origin - thus allowing administrators to see which Shadow IT services might be the root cause of an attempted breach.

Shadow IT doesn't need to be treated like a world-ending threat. Notionally, at least, the ability to select their own tools and evolve their own workflows will turn employees into happier, more productive workers. Like any new experiment, however, allowing Shadow IT into the workplace comes with a certain amount of danger. With SentinelOne, administrators can explore every potential upside of unlimited SaaS adoptions - while thoroughly minimizing the risk involved.

To request a 1-1 demo or evaluation of SentinelOne's Endpoint Protection platform, visit www.sentinelone.com/contact, or reach out to your local channel partner.