Scared Of Your Own Shadow IT? Addressing The Top Security Concern Around SaaS Adoption

By Uri Haramati, co-founder and CEO, Torii

The pandemic struck, and organizations were forced to embrace remote work and cloud applications. Software-as-a-Service (SaaS) apps like Zoom and Slack kept us connected, while others like Asana and Monday kept us organized. But today, businesses are reevaluating the future of work in digital HQs, and IT leaders are sharply focused on security and Shadow IT.

According to Torii's 2022 SaaS Visibility and Impact Report, 69% of tech executives reported that Shadow IT—unsanctioned technology used by employees without the IT department's knowledge—is a top concern related to SaaS adoption.

Why Shadow IT is increasing (and why it's here to stay)

It's not just the physical workplace that's decentralized. SaaS stacks and tech decisions have followed suit, driving Shadow IT adoption to a new level.

To quickly build the digital workplace with SaaS apps, organizations were willing to bend some rules—55% of organizations made exceptions to their security protocols for SaaS applications. Why? The vast majority (80%) say those applications were adopted outside IT's purview.

While 36% of tech executives reported that line of business (LOB) managers are driving the adoption of unsanctioned apps, individual employees are even more likely to experiment and implement new applications autonomously.

The reality is, if employees think their company's existing tools are insufficient to do their jobs, they'll find their own solutions. Any employee with a corporate email, three minutes to fill out a trial form, and a credit card, has instant access to thousands of applications, each with the ability to integrate with business-critical apps.

Businesses need to also consider that digital natives are taking over as the majority in the workforce. They've lived with and used cloud technology for most of their lives, and their comfortability with tech will likely continue to drive Shadow IT growth.

For the sake of innovation, experimentation, creativity and efficiency, these apps could be a major win for employees and the business overall. But where cybersecurity's concerned, shadow IT apps pose a threat if they're unmonitored.

Why shadow IT poses threats

Cybersecurity breaches are extremely costly. As we've all seen, they can cripple companies. In a time where many business leaders are trying to minimize cost, maximize ROI, and ensure business continuity, keeping security tight is mission critical.

IT leaders with Shadow IT in their blind spot are rightfully spooked. Sensitive data —which cybercriminals would be thrilled to get their hands on—flows in and out of those unsanctioned apps. And if those apps have configuration errors, weak login credentials or unauthorized users, your data is at even greater risk.

And Shadow IT's threat doesn't end with an employee's tenure. The SaaS Visibility and Impact Report found that offboarding people from applications was the second greatest concern, right behind Shadow IT. If employees leave a company or consultants complete their engagements and aren't immediately offboarded from all SaaS apps–including those procured by Shadow IT–, they can still access sensitive corporate data and information, without anyone's knowledge.

Full offboarding can only be done when you know what apps you have and who has access to them in real-time.

But with the ever-present specter of Shadow IT, how can organizations truly protect against breaches? How can they act on what they can't see? The answer is in SaaS management.

How SaaS management platforms illuminate and secure Shadow IT

Visibility is your greatest defense against security threats posed by Shadow IT, and that's where SaaS management platforms (SMPs) shine.

SMPs that are designed to automatically discover all sanctioned and unsanctioned applications on your employees' laptops in real-time, give IT security teams a single orchestration point for visibility, control and risk management. Knowing all the cloud apps in use or licensed within your company means that you can take steps to turn unsanctioned Shadow apps into known, sanctioned and secure apps.

SMPs can also make the offboarding process more secure. When integrated with HR systems, an SMP can automate deprovisioning when it detects changes in employment. In other words, if an employee is on their way out, the SMP can automatically remove their access to all sanctioned and unsanctioned apps, and the sensitive data they contain. They also provide audit trails that give visibility into who had access to what apps and when, in the event of breaches.

The Shadow IT name itself implies there are inherent threats—monsters lurking in the unseen cloud app world. But when properly monitored and secured, Shadow IT can also represent value. If business leaders or individual employees find and adopt tools that power greater efficiency, keep them engaged and that they enjoy using, why not support that? With an SMP, businesses don't have to fight autonomous decisions and experimentation with SaaS apps.

Rather than take a fingers-crossed-that-nothing-bad-happens approach, or a locked-down approach where rigid guardrails block employees from using company credentials to adopt apps unless explicitly authorized, businesses can use an SMP to put checks and balances in place so threats can't hide in the shadows.

About the Author

Uri Haramati is Co-Founder and CEO of Torii, whose automated SaaS management platform helps modern IT drive businesses forward by making the best use of SaaS. A serial entrepreneur, Uri has founded several successful startups including Life on Air, the parent company behind popular apps such as Meerkat and Houseparty. He also started Skedook, an event discovery app. Uri is passionate about innovating technology that solves complex challenges and creates new opportunities. Uri can be found on LinkedIn and at our company website: https://www.toriihq.com/