SPxSHARC® II

SECURITYFIRST®

White Paper

Securing the DevOps Sandbox

Reining in Shadow IT

April 2017

Introduction

Business success depends on IT. The ability to rapidly respond to changes in the market, to get a competitive edge, to delight customers, is fundamentally related to today's bottom line. Waiting for the enterprise IT team to review, recommend and release resources to application developers becomes just another "paralysis by analysis" bottleneck that stops the business in its tracks.

The need for cloud-based development "sandboxes" that feature quick set-up, convenience and ad-hoc development based on "just in time" release - rules the day; it simply works and is much faster than the alternative. Public cloud providers have delivered the on-demand infrastructure and tools to satisfy this mind-set, resulting in a quick release cycle that doesn't provide for formal control, testing of an application, and allows the dark, hidden, shadow IT realm - and home to its largest denizen, DevOps.

Why the concern about DevOps Sandboxes?

A sandbox sounds like a win for both the developers and the business. But this practice, void of the rigorous processes and controls of formal IT development and release oversight, can have significant drawbacks, that all impact the bottom line.

COST: These activities outside of enterprise IT often underuse server, storage and licensing capacities at the enterprise level, but significantly over-utilize and tax the network infrastructure.

PERFORMANCE: Without awareness of the shadow IT activities, enterprise operations cannot provide effective troubleshooting and remediation. Personnel get sent on wild goose chases that appear and disappear without warning and without resolution.

CLOUD LOCK-IN: Once these applications are developed and put into use, it is almost impossible to move them to more cost-effective infrastructure platforms, even back on premises. This creates additional costs and also mandates use of a single cloud provider that may not be appropriate for other lines of business or the enterprise.

Perhaps the most worrisome issues associated with these sandboxes is the security risk.

Why are sandboxes the top security concern for your enterprise?

Simply put, it's a matter of liability and risk. The concerns listed above have a measurable impact on infrastructure performance, IT effectiveness and a business unit's bottom line. But a data breach or compliance failure can quickly escalate to put the enterprise at grave risk.

Cloud-based sandboxes expose the enterprise to compliance failures and privacy breaches, and liabilities can grow to be very large due to a mix of costs that include notification penalties, auditing processes, loss of customer revenue, brand damage, security remediation and investment, as well as cyber insurance.

Even with these known consequences, enterprise business units continue to use sandboxes and other Shadow IT resources, and the trend isn't slowing. How do we eliminate or mitigate the threats posed by Shadow IT to the enterprise but provide business units the rapid access to on-demand infrastructure to help the enterprise succeed securely? An Enterprise Data Rights Management (EDRM) solution, like the Security First Corp. SPxSHARC® II, is an essential component that delivers protection against data breaches and compliance failures while providing appropriate access controls.

Bringing Shadow IT back into the fold

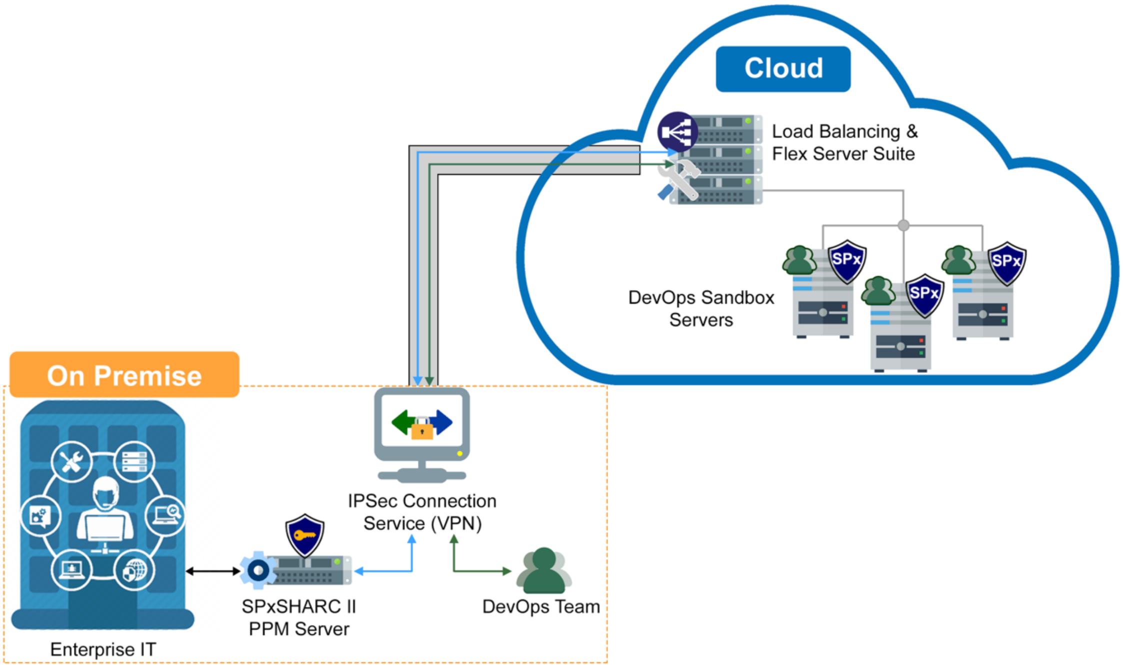
There are three critical elements to getting control over Shadow IT:

ENABLE: First and foremost, enabling the DevOps team to continue rapid development is essential to success. Allowing these teams to take advantage of cloud-based infrastructure and rapid release cycles creates a thriving environment for both the business units and the enterprise, even the core IT team. But that environment must be controlled and monitored.

DEVELOP: Enterprise IT must develop a standard sandbox environment for the DevOps team to access with little delay. This sandbox environment should contain all infrastructure components to get the DevOps team up and running at a moments notice, including secure access to the cloud and testing capabilities for rapid development and release.

DEPLOY: Using the SPxSHARC II Security Blueprint for Cloud Workloads in conjunction with an approved sandbox environment, enterprise IT departments can provide secure development environments with access allowances for the DevOps team and access control/restrictions for everyone else – including the cloud provider – all within minutes - to get DevOps activity moving fast. This ensures these key success metrics are met.

Figure 1 – Security Blueprint for Cloud Workloads



SPxSHARC II is transparent to DevOps, but secures the sandbox datasets from breach

Summary

Sandboxes exist because they produce results fast, but the practice of rapid development and release of substandard applications creates huge financial and compliance risks for the enterprise. The need for a controlled but rapidly deployable secure sandbox is essential to match business unit success with enterprise success. This SPxSHARC II Security Blueprint provides a reference architecture that can be applied to DevOps sandboxes in any external environment, bringing the Shadow IT realm back into the fold.

About Security First Corp.

Security First Corp. started in 2002 to combat the complex cyber security landscape brought on by the exponential growth of data. Building a new age of data security science, we've perfected it into the most powerful security technology, SPx$^{\text{TM}}$. Recognized across the industry for its unrivaled capabilities, we are making unsurpassable data protection possible for enterprises and governments across the world.

Contact Us

For more information or to schedule a product demonstration:

☎ 888-884-7152 ✉ sales@securityfirstcorp.com 🌐 www.securityfirstcorp.com

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” AND WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED. Availability of any products included in this document is at the sole discretion of Security First Corp. and may change without notice. Contact us at securityfirstcorp.com to get the latest details.