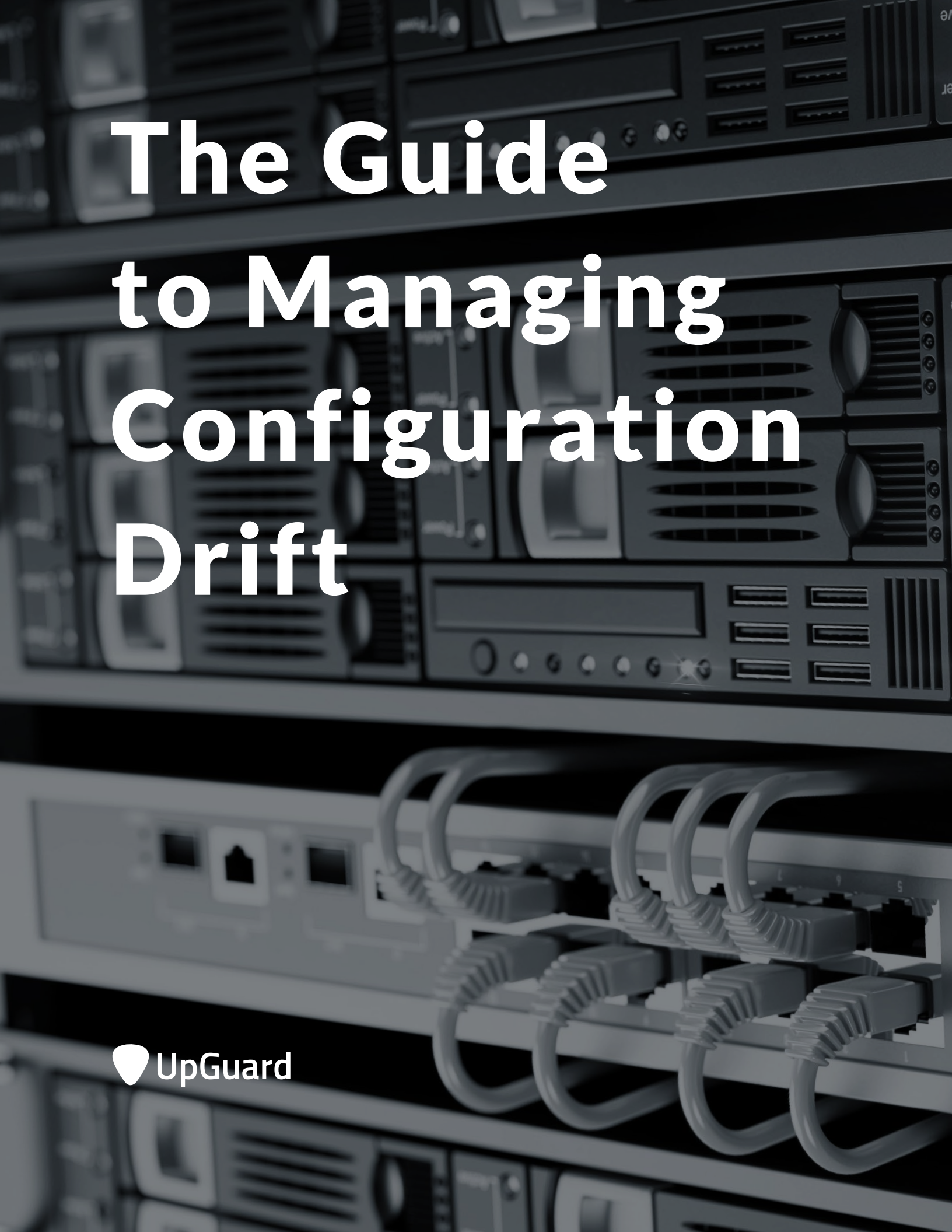


The Guide to Managing Configuration Drift

UpGuard

Introduction

How much does a server misconfiguration cost these days? Unfortunately, for many enterprises the price tag may surpass the value of the entire business. You may remember Knight Capital, the high-flying global financial services firm that was at one point the largest equities trader in the United States, commanding 17% on both the NYSE and NASDAQ with an average daily trading volume in excess of 3.3 billion trades and $21 billion. On August 1st, 2012, untested software was manually deployed to a production environment, triggering an obsolete function resident in one of the servers to incorrectly process orders en masse. The result was nothing short of devastating: the company suffered a $460 million dollar loss in a span of 45 minutes as a result of the glitch.

With only $365 million in cash and equivalents on hand, Knight Capital was effectively bankrupted by the event. The company's stock price would also eventually collapse, sending shares lower by over 70%. Getco LLC eventually acquired the firm in December 2012.

"During the deployment of the new code, however, one of Knight's technicians did not copy the new code to one of the eight SMARS computer servers. Knight did not have a second technician review this deployment and no one at Knight realized that the Power Peg code had not been removed from the eighth server, nor the new RLP code added. Knight had no written procedures that required such a review."

—SEC Filing, Release No. 70694, October 16, 2013

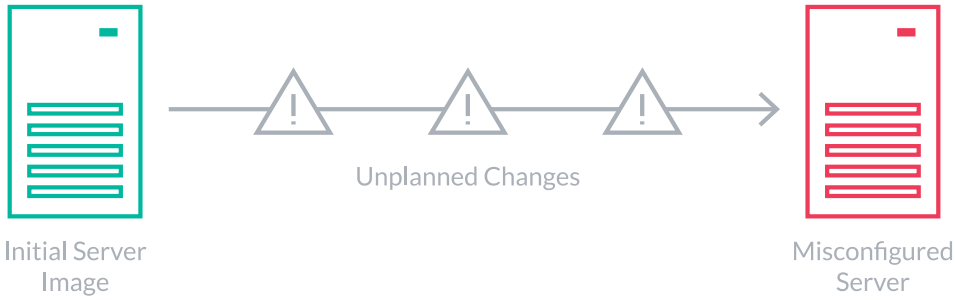
Knight Capital may be the most spectacular IT failure to date, but it's hardly the only prominent enterprise to incur misconfiguration-induced losses. Online retail giant Amazon.com recently suffered 13 minutes of downtime that resulted in $2,646,501 in revenue loss; similarly, Southwest Airline's 2016 computer system failure resulted in the cancellation and delay of over 2,000 flights and lost revenue/increased costs between $54 and $82 million.

It's hard to imagine that misconfigurations and environmental inconsistencies could have such devastating results, but this is the reality of doing business in today's digital landscapes. In many of these cases, configuration drift is the primary culprit—and its proper detection and management is critical to preventing operational disasters from befalling the enterprise.

Defining Configuration Drift

Over time, IT systems and their configuration items (CIs) invariably move towards a state of disorder. This is the case with all things, as dictated by the second law of thermodynamics. But it doesn't take a physics degree to understand the minutiae of why configuration drift occurs in IT infrastructures: ad-hoc modifications, isolated tests and code changes, server patches, and other activities lead to test and staging environments drifting away from production configurations and/or baseline specifications.

Left unchecked, these continuous changes to the environment's software and hardware result in performance degradation, unanticipated downtime, data loss, non-compliant systems, cybersecurity events, and data breaches. And without visibility into the changes occurring in the environment (i.e., software/hardware changes are not reliably tracked in a systematic manner), the time it takes to restore operations to a system—or mean time to repair (MTTR)—is drastically increased when service disruptions occur. For enterprises that measure downtime in terms of millions of dollars per minute, every second counts: a recent IDC survey of Fortune 500s revealed that the average cost of a critical application failure was $500,000 to $1 million per hour.



The average cost of a critical application failure is $500,000 to $1 million per hour.

For the Fortune 1000, the average total cost of unplanned application downtime per year is $1.25 billion to $2.5 billion.

The average hourly cost of an infrastructure failure is $100,000 per hour.

The average cost of a critical application failure per hour is $500,000 to $1 million.

- IDC, "DevOps and the Cost of Downtime: Fortune 1000 Best Practice Metrics Quantified."

Controlling Configuration Drift

To combat configuration drift, enterprise IT has several technologies at its disposal; most organizations employ a myriad of tools in parallel to properly detect and manage drift. At the most basic level, IT admins require a system for storing configuration information about their infrastructure's components: hardware devices, servers, network addresses, software versions, applied updates, and more.

The CMDB

Configuration management databases (CMDB) are popular among enterprises for storing information about CIs in the environment, spurred on largely by IT Infrastructure Library (ITIL) best practices standards around their usage. With a CMDB, CI information is ostensibly always up-to-date and accurate—in practice, however, these data stores quickly grow stale and outdated. This is typical of documentation that's not executable—no mechanisms for self-validation. Improving existing, manual efforts is required for keeping the CMDB updated.

Automation Tools

Solutions like Puppet, Chef, and Ansible are indispensable tools for combating configuration drift, since they automatically rectify machine images that may have drifted away from their desired states. IT admins more often automate the deployment of servers and configurations repeatedly to keep machines in line on a constant basis. However, visibility is still a key prerequisite for automation, and not knowing what you have prior to automating builds can nonetheless lead to inconsistencies in the environment. Additionally, automation tools may report the successful completion of jobs, but IT admins cannot easily validate that environments are in line with expectations using these tools alone.

"Configuration drift and unauthorized configuration changes account for nearly 80% of all IT service outages."

-Gartner Research

Integrity Monitoring with UpGuard

UpGuard's Cyber Resilience Platform was designed to help IT admins create and maintain controlled, consistent environments. The solution's powerful drift monitoring and detection capabilities help save enterprises from costly IT systems downtime, software failures, and rollbacks due to configuration drift-related issues. Our platform preserves the integrity of environments by detecting and monitoring for changes and discrepancies in all node types: servers, desktops, routers, web applications, databases, and more. The platform integrates with popular CMDB offerings such as BMC Atrium and ServiceNow, as well as popular automation tools like Puppet and Chef for a streamlined drift remediation pipeline.

Conclusion

Combating configuration drift starts with proper visibility and validation—to this end, UpGuard automatically ingests the state of your whole infrastructure and captures “golden images” of your preferred configurations. Policy-driven monitoring validates that your systems are always in line with these expectations and integrates with existing enterprise ticketing systems like ServiceNow for proper alerting and elevation of events. And when the cause of the configuration drift is determined, UpGuard integrates with your favorite automation tools for quickly rolling out corrective measures. Finally, our platform provides the proper validation for ensuring that changes have been implemented as expected to the systems and/or environment. Entropy may be one of nature’s most pervasive laws, but it doesn’t have to bring your IT department to its knees. UpGuard’s configuration drift monitoring and detection capabilities allow enterprises to reap the rewards of digitization while maintaining control of its shortcomings.

Businesses depend on trust, but breaches and outages erode that trust. UpGuard is the world's first cyber resilience platform, designed to proactively assess and manage the business risks posed by technology.

UpGuard gathers complete information across every digital surface, stores it in a single, searchable repository, and provides continuous validation and insightful visualizations so companies can make informed decisions.

909 San Rafael Ave.
Mountain View, CA 94043
+1 888 882 3223
www.UpGuard.com