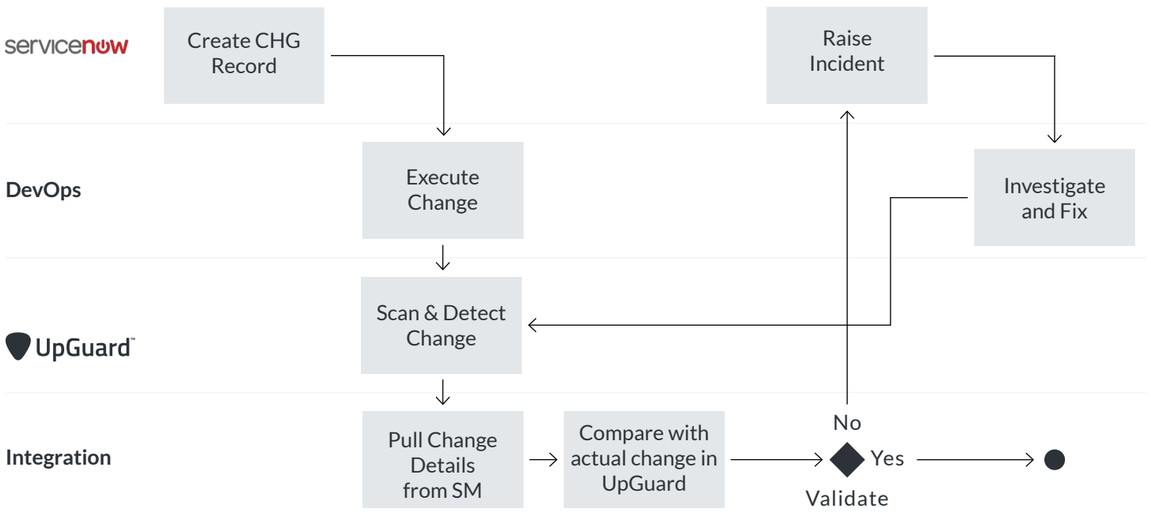
UpGuard™

Enabling Visibility with UpGuard and ServiceNow

WHITEPAPER

INTRODUCTION

ServiceNow® customers optimizing their IT service delivery and management processes require deeper context and detail level behind IT asset changes--information the leading help desk automation and incident reporting platform does not provide. In this report you'll learn how UpGuard lls this visibility and awareness gap, keeping ServiceNow® in line with the true state of your environment. You'll also learn how UpGuard and ServiceNow® work together to give enterprises a comprehensive framework for both reducing downtime and preventing miscon gurations from threatening business continuity.



ABOUT UPGUARD

UpGuard was founded in 2012 by industry veterans to address contemporary IT needs in the areas of vulnerability detection, compliance monitoring, con guration drift detection, and infrastructure discovery, among others. The UpGuard platform was born- in-the-cloud and embraces current paradigms such as DevOps, Agile, and continuous integration and software delivery.
UpGuard's CSTAR system for quantifying and scoring cyber risk combines deep internal scans with reputable external data sources for accurately gauging an organization's cyber risk pro le and quantifying it in a single FICO score-like number.

UpGuard's comprehensive visibility and integrity platform monitors, scans, and tracks servers, network hardware, cloud services, web apps, infrastructure, and more for vulnerabilities, misconfigurations, and security gaps. The platform validates that all IT asset configurations in any given environment are as expected at all times.

THE INTEGRATION

Enterprises managing their IT services with ServiceNow® require a mechanism for capturing and validating the minutiae behind con guration changes. UpGuard satisfies this critical need and provides the following benefits:

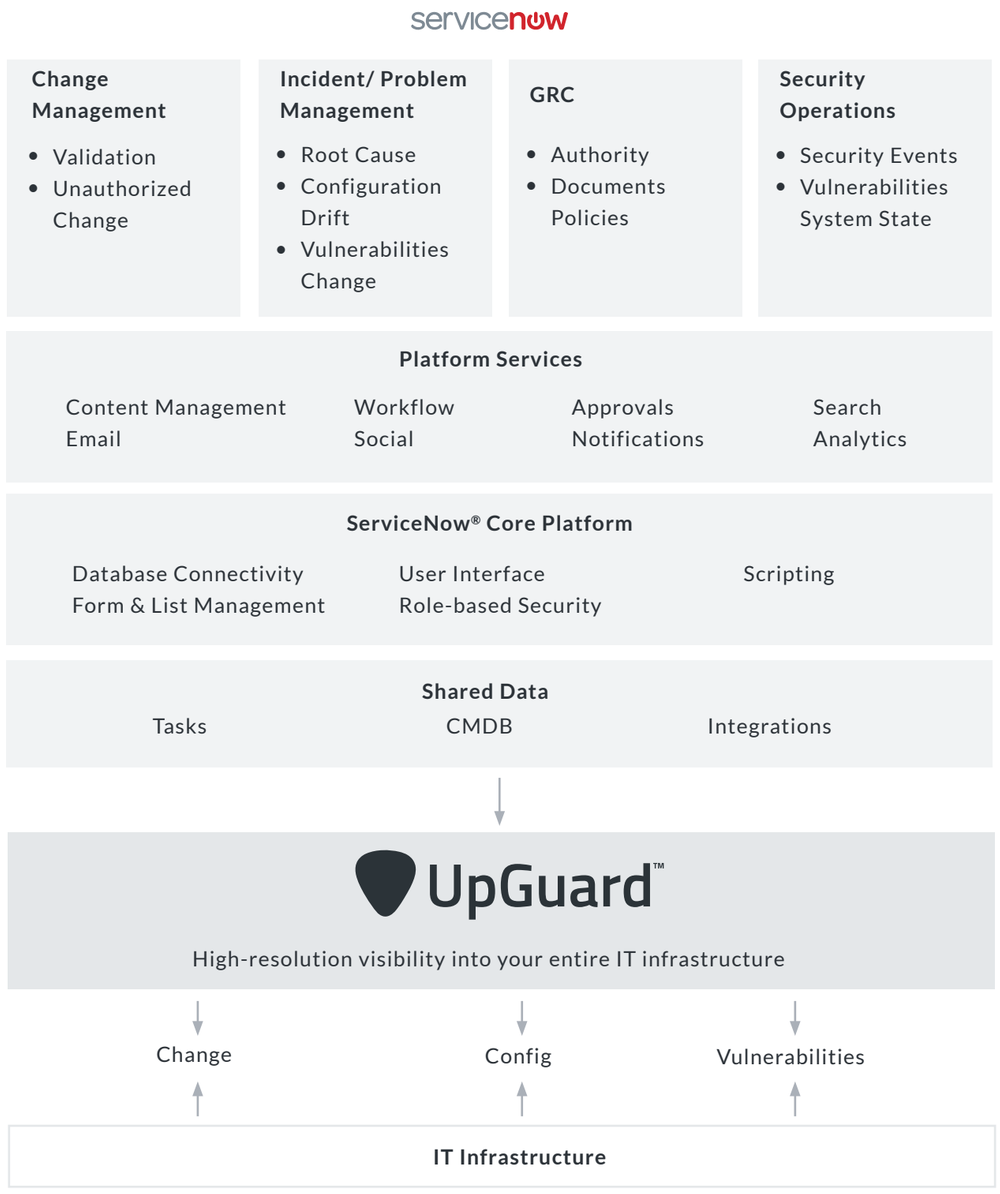
- Powerful Change Validation - UpGuard validates that changes and releases owing through ServiceNow® are authorized, accurate, and/or expected.

- Better Incident Management - UpGuard augments ServiceNow®'s IT helpdesk ticketing system with granular details of the changes, miscon gurations, and vulnerabilities causing service disruptions.

- Deeper Insights and Analytics - UpGuard provides detailed analytics and forensics for determining the root cause of issues, in turn giving IT operations the insights for taking proper preventative measures.

- Risk Assessment and Management - ServiceNow® captures enterprise IT processes, activities, and IT knowledge in its service-oriented platform; UpGuard transforms these and other large volumes of complex technical data regarding your IT assets into business risk information.

- Improved Cybersecurity and Awareness - UpGuard tracks unauthorized changes, security policy violations, and vulnerabilities, automatically raising incidents in ServiceNow® for faster security incident resolution and remediation.



UpGuard's integration with ServiceNow® gives enterprises deeper contextual information about the changes occurring in their environments. This information is critical for reducing the risk of business interruptions, enhancing change management and release times, and improving the enterprise's compliance and security posture.

IMPLEMENTATION

UpGuard will validate that any changes detected in your environment have a corresponding open change request in ServiceNow®. If not, a ticket is raised alerting you of the unauthorized change.

- Once UpGuard detects a change in the environment with no matching approved change request, a ticket is raised in ServiceNow® alerting you of this. (Figure A)

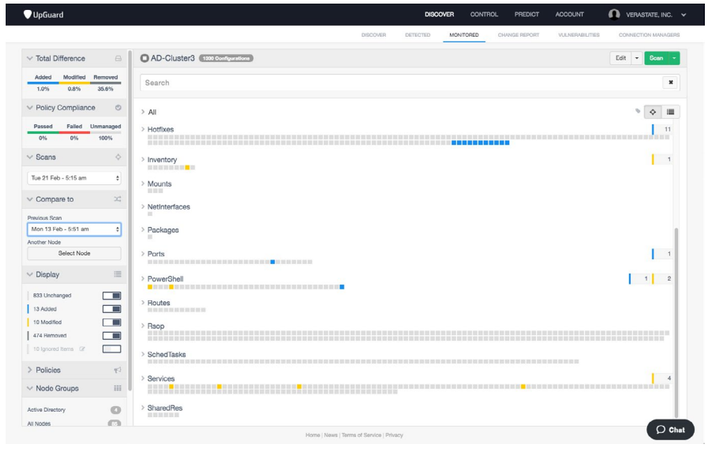


Figure A - UpGuard detects changes in the environment.

- UpGuard will populate ServiceNow® with the necessary contextual information for managing the incident--including a direct link to the corresponding node report in UpGuard. The platform also validates that changes requested via ServiceNow® are completed as planned, giving IT operations the means to validate that ServiceNow® is in alignment with the true state of your infrastructure. (Figure B)

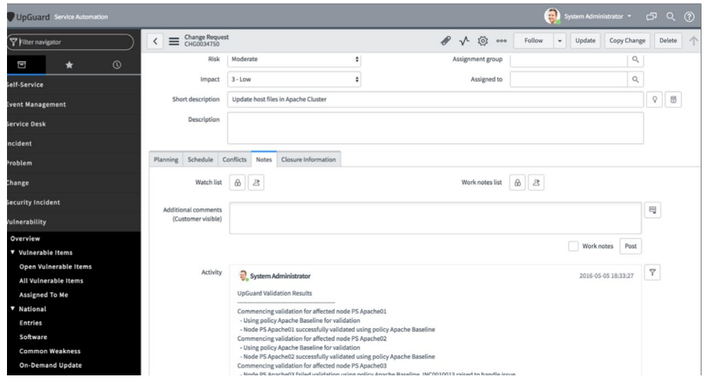


Figure B - UpGuard raises an incident in ServiceNow alerting you of the unauthorized change

MANAGING RISK WITH UPGUARD AND SERVICENOW® GRC

ServiceNow®'s Governance, Risk, and Compliance (GRC) module provides risk management tools like internal process testing and auditing that automate the measuring and management of adherence to policies like Sarbanes-Oxley and HIPAA. UpGuard integrates with GRC to ensure that your environment's IT assets are always in line with policies de ned in ServiceNow®, enabling more detailed and accurate risk assessment and cyber resilience.

Policies defIning frameworks, regulations, and standards are stored in GRC as authority documents. For example, the Center for Internet Security (CIS) maintains a set of secure con guration benchmarks for improving security (e.g., the CIS Security Benchmarks). GRC captures them in a corresponding authority document that de nes the speci c policies and controls for meeting the benchmark. UpGuard provides the foundation data regarding the true state of your environment and its constituent components-- servers, network devices, software, and all their con gurations-- to GRC for measuring and managing adherence to policy. And when any granular changes occur in your environment that are out of line with policies de ned in GRC authority documents, UpGuard will raise an incident in ServiceNow® alerting you of this.

CONCLUSION

There's no arguing that innovations like the cloud and virtualized infrastructures have spurred unprecedented business agility and innovation-- they have also created environments of unprecedented complexity and heterogeneity. ServiceNow® gives enterprises a scalable, service-oriented platform for managing IT assets in these complex environments; UpGuard bolsters ServiceNow® by validating its records against the true state of your environment. The platform provides rich, contextual details behind the changes occurring in your infrastructure, allowing you to close the feedback loop on incidents and change management processes.

REFERENCES

http://searchcio.techtarget.com/de nition/ITSM

http://blog.itil.org/2015/08/allgemein/csi-2-0-make-it-service-management- happen-through-agile-scrum/

https://www.ticomix.com/service-now/

http://wikibon.org/wiki/v/ServiceNow®:_Rede ning_Enterprise_IT_Service_ Management

http://www.cio.com/article/2388639/software-as-a-service/it-service- management-moves-to-the-cloud.hl

http://cloudindustryforum.org/news/827-uk-cloud-adoption-rate-climbs-to-84- nds-new-research-from-the-cloud-industry-forum

UpGuard™

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

WP_0006 / 02.22.2017