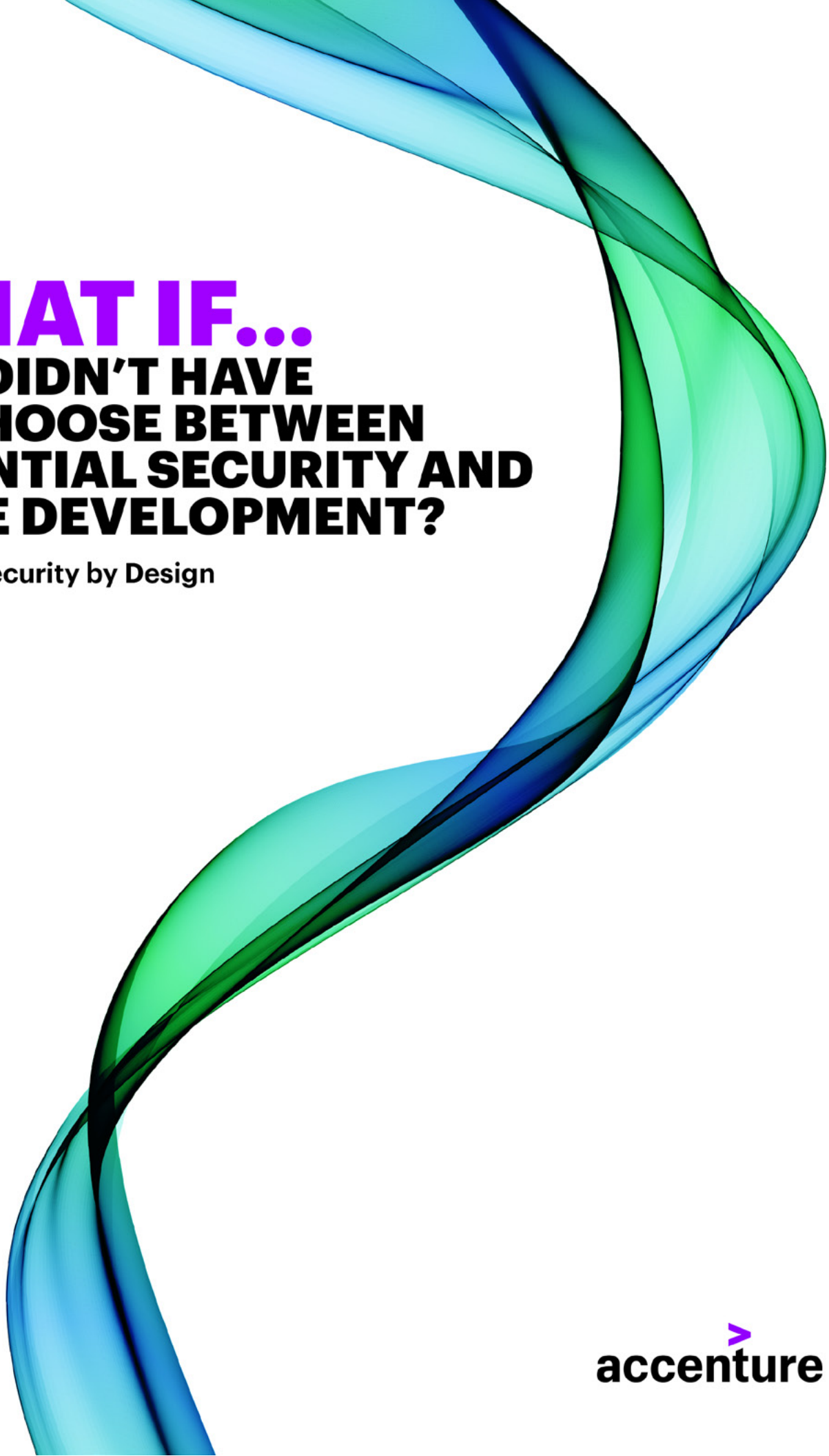
WHAT IF...

YOU DIDN'T HAVE TO CHOOSE BETWEEN ESSENTIAL SECURITY AND AGILE DEVELOPMENT?

Demand Security by Design



GUS HUNT

accenture

There's no doubt you are on the receiving end of conflicting messages: accelerate the development of new systems and capabilities to meet your user demands AND respond to ever increasing asymmetrical threats. Add to that, everyone from the President on down is championing the need for systems to be more secure in the face of a growing barrage of cyber threats.

Consider this: it's not an either or situation, you can effectively integrate security with development and more important, you need to do it now.

IT'S TIME TO EMBRACE SECURITY BY DESIGN

If you're not infusing security practices into your development efforts from the early stages you are setting the stage for a risky, and potentially devastating, outcome. One where you lose valuable time, money, and expose your organization to cybersecurity risk.

The old development model of "adding security" at the end as a "quick compliance check" simply won't cut it in a world where our adversaries continue to hold the upper hand. In our Cyber Moonshot paper we identified security by design as one of five essential elements of achieving cyber resilience: security must be engineered into the core of every system from the get-go.

ADOPTING A DevSecOps APPROACH

Over the past several years, DevOps has gained in popularity as a proven way to bridge the gap between developing and operationalizing applications. DevOps is an enabler that brings automation, repeatability, agility and speed across the entire lifecycle.

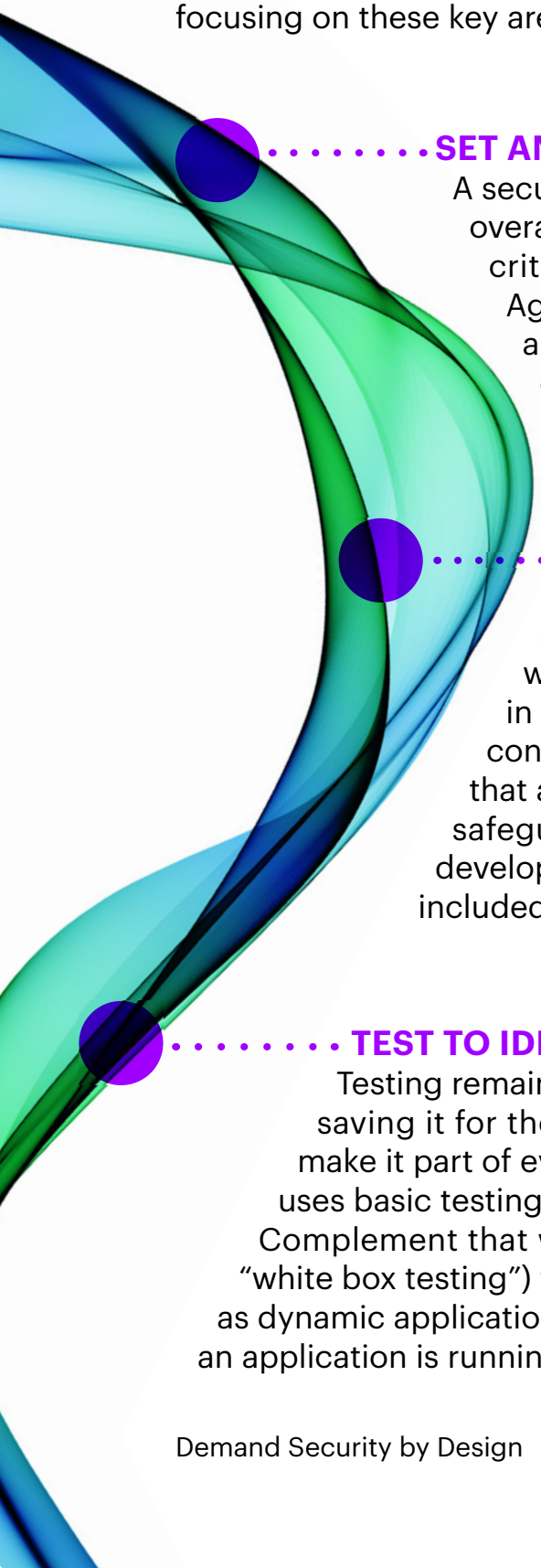
Now, with DevOps in a mature state, Federal agencies have the momentum to embed security into the approach, creating a new DevSecOps model that transforms security into another enabler for the business.

By embracing DevSecOps, Federal agencies can drive agile development – bringing all stakeholders to a high level of security understanding in a short period of time and ensuring security needs are "baked in" from the beginning.

> *Ultimately – security becomes everybody's job, speed to delivery is enhanced, budget is maximized and ...there's no surprise ending.*

THREE THINGS TO DO NOW

Whether your organization is ready to embrace DevSecOps now or not, every agency can benefit from a close examination of current application security practices. To balance business needs with security risks, start by focusing on these key areas:



SET AND ENABLE STANDARDS.

A secure technical architecture integrated within the overarching business and security architecture is a critical first step to effective application security. Agencies must also identify the necessary training and tooling needed to enable developers to effectively implement standards in clear ways that can be validated in DevSecOps pipelines.

MODEL THREATS TO ASSESS RISK.

A standard technical architecture is critical to security, but so is an understanding of the context in which an application will be used and the infrastructure in which the application will operate. Threat modeling considers that context to help in assessing the likelihood that a system will be a target and developing appropriate safeguards. Threat models can further assist in the development of security testing approaches that can be included in automated testing scenarios.

TEST TO IDENTIFY VULNERABILITIES.

Testing remains a key enabler of application security. Instead of saving it for the very end of the software development lifecycle, make it part of every development sprint. Static code analysis (SCA) uses basic testing to identify and flag areas with common mistakes. Complement that with static application security testing (SAST, or "white box testing") to see if the application can be penetrated, as well as dynamic application security testing (DAST) to evaluate security when an application is running.

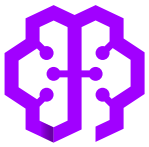
ENSURING THE RIGHT ENDING: CYBER RESILIENCE

Security by design, DevSecOps, is one of five essential technology pillars needed to establish a strong cyber resilient foundation, one that shifts the balance of power away from our adversaries and tips the scale in our favor. In our Cyber Moonshot paper we outline our thinking about each of these pillars:

EMBRACE THE CLOUD FOR SECURITY

ENGAGE IN PROACTIVE DEFENSE

DEMAND A DATA CENTRIC APPROACH



BUILD IN CYBER RESILIENCE

To find out more about each of these, and to learn more about DevSecOps, visit Accenture.com/cyber.

FOR MORE INFORMATION PLEASE CONTACT:

Gus Hunt
Managing Director and Cybersecurity Strategy Lead
Accenture Federal Services
gus.hunt@accenturefederal.com

@GusHunt_

VISIT US AT ACCENTURE.COM/FEDERAL

Follow us at @AccentureFed

Connect with us on LinkedIn

ABOUT ACCENTURE FEDERAL SERVICES

Accenture Federal Services is a wholly owned subsidiary of Accenture LLP, a U.S. company, with offices in Arlington, Virginia. Accenture's federal business has served every cabinet-level department and 30 of the largest federal organizations. Accenture Federal Services transforms bold ideas into breakthrough outcomes for clients at defense, intelligence, public safety, civilian and military health organizations.

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world's largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 435,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives.
Visit us at www.accenture.com.