SAPinsider

This article appeared in the Apr ▪ May ▪ Jun 2016 issue of *SAPinsider* (www.SAPinsiderOnline.com) and appears here with permission from the publisher, WIS Publishing.

WIS pubs

# Protecting the Digital Enterprise

## Executive Q&A with SAP's Justin Somaini

Today's enterprise is no stranger to protecting its inventory, intellectual property, and employee information — most organizations have well-established security measures in place for this purpose. But as companies go through digital transformations, their security challenges transform as well. They are now connected to an expanding network of customers, suppliers, devices, and partners, meaning that the threat landscape is changing. Now companies must protect themselves against both internal and external threats while continuing to provide the speed, agility, and ease of use that customers demand. In this interview, Justin Somaini, SAP's Chief Security Officer, explains how SAP's solutions and services for security and governance, risk, and compliance (GRC) are helping organizations protect themselves in the changing landscape of the digital economy.

### Q: What does digital transformation mean for the future of enterprise security?

**A:** Digital transformation is moving businesses from just managing their technology to letting technology drive the business. This allows the enterprise to become a smart, agile, dynamic, fast, and competitive business that can better serve its customers by harnessing increased visibility into consumers, providers, and third-party vendors.

A digital security transformation is no different; it merely takes place in the security world. Historically, security has been very much technology-driven, swimming upstream to be business-oriented. Within this framework, it's been difficult to completely interject the operational and revenue models of the business with security concerns.

As we look ahead, what was difficult for the business in the past is now a huge opportunity, not just to secure the delivery of the business, but to secure the funnel — the pre-sales mode — of how we go to market, from marketing, to customers, to vendors. Security is no longer limited to being a tactical, reactive response that secures a business output; rather, it is about how to truly integrate security into the business.

### Q: How does a digital economy change the threat landscape?

**A:** Security demand has exploded dramatically in response to rising threats and the integration of new digital technologies. Organizations need a stronger hold on their content and transactions to give them the visibility and control they need not only to govern themselves, but to combat threats.

In the past seven or eight years, we've seen a shift in the threat landscape from nuisance-oriented activities, such as spam and malware, to an organized crime approach that exploits vulnerabilities and attacks to generate significant revenue. This places significant pressure on security organizations to view security not merely as a technical solution, but as a platform to tackle business security problems. A much deeper integration of security into the enterprise is needed to withstand attacks and reflect the new technologies that permeate every facet of a digital existence.

## Justin Somaini

Chief Security Officer, SAP

### Q: How must the digital enterprise adjust to this new security dynamic?

**A:** Historically, organizations focused on protecting themselves by implementing firewalls, vulnerability scanners, and other technologies, either to identify attacks or to harden their environment to resist attacks. This evolved into including protections in basic processes, such as change management, process management, and project management, to ensure that security is integrated with a company's technology efforts.

As we begin to secure customers in a digital world, however, we realize that this is not enough. Because of the connections that organizations now have, businesses need to consider the security of their entire ecosystem of customers, third-party vendors, Internet of Things (IoT) technologies, and other assets as part of their process management strategy. This means that a security platform has to adapt in response to changing business models. It needs to provide better analytics to the business as well as better governance and risk management capabilities, so the organization can prevent and react to possible threats. This is what it means to have a sound enterprise security strategy in today's digital business environment.

### Q: Can you give an example of what this type of security might look like in a digital enterprise?

**A:** A common thread throughout much of the digital world is the pursuit of agility. We are starting to see the concept of security become one of agility as well.

Consider the cloud, an integral element of the digital world that is a great example of enabling companies to increase their agility. Due to the cloud's very nature of interconnectedness, this enhanced agility extends into these companies' entire value chains and across their ecosystems — to their customers, their providers, and so on.

Now think about security in the same way — as having the same level and reach of agility that the business achieves with the cloud, able to respond to changing requirements quickly and nimbly. Just as the cloud enables customers to be dynamic in the vendors they choose, for instance, agile security enables real-time visibility into the risk profile of these vendors — not just one at a time, but dynamically and in near real time to enable smart, fast, and agile decisions.

### Q: How can an organization adopt an agile, proactive governance and security platform and still focus on securing its mission-critical SAP business applications?

**A:** I don't think it's an either/or scenario. Whether mission-critical systems are on premise or in the cloud, security services are part of the application as something that is core to what we do. So how do we create an ecosystem around that product — be it on premise or as a service — so that it integrates with the customer's security ecosystem?

There has always been 24/7 operational support against attacks or fraudulent transactions going into the system, with an understanding around authentication and authorization rights. Going forward, the goal is the ability to incorporate application signals to provide an agile, real-time risk profile as well as an agile mechanism for controlling that

> Security is no longer limited to being a tactical, reactive response that secures a business output; rather, it is about how to truly integrate security into the business.

risk in conjunction with changing business models and business plans, changing vendors and providers, and mergers and acquisitions.

### Q: How has SAP's GRC portfolio evolved to be more agile?

**A:** Throughout my career, security has always been a very dynamic and shifting landscape. And so the products that we drive — whether GRC, identity authentication for the cloud, or code vulnerability analysis (CVA) scanners — need to be dynamic and need to continue to mature accordingly. We do that in a couple of different ways, beginning with internal development, but also opening it up to the partner landscape to ensure specific use cases that are unique to customers.

Our partnership with Greenlight Technologies, for example, has been incredibly important for serving our customers. The SAP Regulation Management application by Greenlight fills a compliance and risk management need by giving companies better analytics, from business users up to the board and C-level. This is just one example of how SAP has responded to customer needs by considering security and GRC concerns to be a part of what drives the business from a strategic level. Source code analysis is an example of how SAP has also continued to evolve its internally developed GRC solutions. We've helped customers analyze code for vulnerabilities, and our partnership with Fortify has now pushed this capability out into other languages, helping meet the needs of today's global companies.

This is what SAP itself is doing with its own security landscape. In addition to a significant number of security experts at SAP looking to ensure that products, services, and the internal framework are secure, we're also leveraging our own security and GRC tools to govern ourselves. Ultimately, our concerns as a corporate security team are no different from the problems that our customers face in managing their own environments.

### Q: Threats are always changing. How does SAP's GRC and security platform help companies prepare for the future?

**A:** A forward-looking GRC system should be able to identify security issues and place them in context relevant to the business. The enterprise must be able to identify issues from a regulatory and compliance landscape — from around the world — and determine if it is on target to meet the expectations of its customers and regulators. And this is great, but it isn't the whole picture. The question then becomes how to translate the complexity of security vulnerabilities, malware, and cyber attacks into an understanding of the real impact these have on the business from the perspectives of revenue, reputation, and operations. Whether an organization is in manufacturing, healthcare, retail, or even creating a service, how will an attack or threat affect its ability to deliver its products to its customers?

A modern GRC and security platform, like the one provided by SAP, addresses these concerns by extending us out of the security world that we've been in — a world where security is a deeply embedded tactical issue — and into a simplified model where the business is a proactive participant in governance. This is how to protect the digital enterprise of today. ■