Leveraging Security to "Innovate with Intention"

Spirent provides actionable intelligence to guide innovation and manage risk.

Introduction

For years, companies have been trying to bridge the "innovation gap," which is the difference between the desire to ignite innovation and success in doing so. In a well-known landmark survey by McKinsey & Company nearly 10 years ago, 84% of executives said innovation is extremely important to their growth strategies, but 94% were unsatisfied with their innovation performance[1].

Why does this gap persist? A closer look reveals two important misconceptions about innovation. The first is that cybersecurity impedes innovation because it adds enormous complexity and delay to the development of new products and services. The second is that innovation is the result of unstructured creativity, or "Eureka!" moments.

This paper will clearly demonstrate the fallacy of both assumptions. It will illustrate how security can actually be a catalyst and an accelerator for innovation; and it will show that harnessing intelligence generated by Spirent security solutions can empower companies to **innovate with intention**—to take responsible risks based on actionable intelligence—and thereby innovate more effectively.

1 McKinsey & Company Global Survey, "Innovation and Commercialization," August 2010.

Leveraging Security to "Innovate with Intention"

Spirent's Innovation Advantage

Our unique combination of capabilities sets us apart in empowering your company to innovate with intention. We are the one and only partner who can provide all of the following:

Attitude: Spirent views security as an innovation accelerator rather than an obstacle, something to be built in proactively rather than bolted on.

Emulation: Spirent replicates attack and hacker scenarios precisely, using real attack vectors that real cyber criminals put on the wire, as opposed to simulation that only "resembles" such scenarios.

Risk Assessment: Spirent solutions enable customers to manage and mitigate security risks, compliance risks, and the business risks of security deficiencies.

Flexibility: Spirent offers a full range of security and performance assessment solutions and customers can easily change the mix between product and service solutions, thereby improving the speed of innovation.

Ecosystem: Spirent works with ideas from everywhere, harnessing the collective insights of customers, partners, providers and users of global communication networks, research firms, government, and internal R&D teams.

Intelligence: Spirent gathers actionable intelligence from many sources and makes it available to help customers innovate with intention.

Expertise: Spirent has seasoned consultants with decades of experience in cybersecurity and its customers are leaders in multiple industry segments, giving us a broad spectrum of sector-specific knowledge and insight.

Leadership: Spirent is at the forefront of innovation, actively establishing, supporting, and contributing to industry standards such as CTIA IoT Cybersecurity and NetSecOPEN.

Seeing Security as the Catalyst for Faster, More Effective Innovation

Security is often portrayed as a brake pedal that slows innovation. One reason is that all too often security is applied to innovations after the fact—bolted on—to manage the risks inherent in new ideas.

For example, a new app that DevOps just created must be evaluated prior to deployment against a barrage of security standards, compliance guidelines, and benchmarks to make sure it does not introduce new vulnerabilities and risks that are difficult to manage. This typically involves expense and delay as security specialists do their work, impacting time-to-market.

Given the steady stream of new security threats, new attackers, new

compliance regulations and new security policies—combined with proliferating devices, applications, networks, systems, clouds, and supply chain partners to protect—meeting security requirements can quickly become overwhelming. The net result: product development and innovation initiatives slow to a crawl.

At Spirent, we start with a completely different assumption about security, based on many years of real-world experience. We have seen that when organizations include security in all business conversations from the outset, and when they proactively embed security into new products and services, security becomes the accelerator for innovation rather than the brake.

The reason: once security is assured, teams can innovate faster, with more confidence and less risk. Security is no longer about avoiding the unthinkable; it becomes the catalyst for exploring more ideas faster.

Spirent solutions take this concept a step farther. Our security assessments deliver the intelligence companies need to innovation with intention—to guide their innovation decisions in a way that manages and mitigates risk to minimize time-to-market of new products and services and maximize competitive differentiation.

Our approach is all about integrating security from end to end to tame the massive complexity of meeting security requirements.

We combine the expertise; the proactive approach to security; the end-to-end capabilities in infrastructure, applications and services; the partner ecosystem; and the flexibility to enable our clients to speed up innovation while reducing risk, disruption, and expense. More specifically, we enable your enterprise to do three things:

#1: Proactively Build Security into Every Innovation

Spirent solutions enable companies to address security issues and elevate security influence earlier in the development process—so they can build and deploy innovations that are inherently secure. For example, we've helped a global hospitality company set security standards for all of their applications, so that when innovation teams start to build creative new web and mobile apps they can be sure security is built in. Spirent then assesses their new apps against the standards on a quarterly basis, ensuring continuous compliance. The result: the company can create more innovative ways to engage with customers, with less worry and less risk.

CyberFlood: Security Assessment of Critical Infrastructure

One way Spirent helps companies build security in is by assessing and validating the security of a huge array of infrastructure products that are in turn used to build new innovations at other companies.

For example, there is virtually no data communications equipment on the market today that has not been touched in some shape or form by Spirent. Using CyberFlood, our L4-7 assessment solution, companies can emulate realistic application traffic while validating their security coverage with real attacks and malware from enterprise to carrier-grade network capacities.

Unlike other test solutions that use "simulated" traffic with the same packet payload over and over again, CyberFlood provides authentic, customizable payloads for hyper-realistic security, load, and functional testing. In addition, CyberFlood keeps up to date with the latest Malware, DDoS and exploits to test the effectiveness of security operations. By using CyberFlood or CyberFlood Virtual, customers can validate their security posture, Quality of Service (QoS) and Quality of Experience (QoE) quickly and easily.

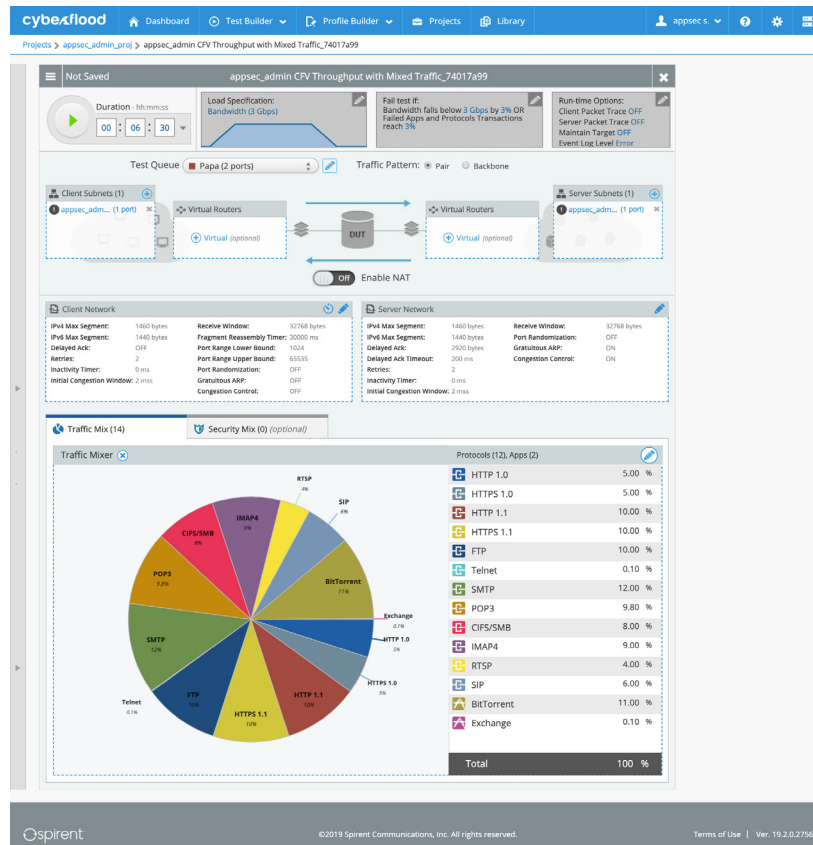## Leveraging Security to "Innovate with Intention"

Figure 1: CyberFlood generates thousands of realistic application traffic scenarios and attacks to
test the performance, scalability and security of application-aware network infrastructures.

The connection between built-in security and accelerated innovation is clear: By helping customers assess the security of infrastructure elements such as IDS/IPS, firewalls, DPI, IoT devices and more. CyberFlood enables both the companies that make these products and companies that use these products to innovate with greater speed and confidence – we provide assessment from product inception through production network deployment.

CyberFlood TestCloud: Accelerate Application and Performance Testing

The same concepts described above apply to application and performance testing. CyberFlood TestCloud provides access to thousands of up-to-date applications so companies can generate traffic with authentic user scenarios for realistic security, performance load and functional testing.

CyberFlood creates tests with the latest apps from TestCloud while also allowing users to import their own applications to recreate custom applications at scale. Teams can quickly and easily determine how security polices work to defend against attacks while allowing legitimate user traffic to pass through as unimpeded as possible.

Embedding Innovation is Always the Priority

Spirent's comprehensive security platform is built with innovation teams in mind, whether at enterprises, service providers or network equipment manufacturers (NEMs). It improves testing today while evolving for the future, so organizations can stay ahead of the security curve and keep their focus on innovation.

Equally important, by helping our customers embed security proactively into every facet of operations, we also help them create and support a risk management culture. Simply put, they can identify the vulnerabilities sooner and take the right action to remediate unacceptable risks, right away.

#2: Minimize Risks Through an Intelligence-Driven Approach

Our solutions give you the intelligence you need to identify, quantify, and respond to security risks, compliance risks, and business risks before they impact your live production environment. This intelligence supports proactive risk management, enabling your company to innovate with intention because now you can focus on creating the right features and functionality knowing that security is always addressed.

For example, many companies are leveraging advances in facial recognition technology in order to combine convenience and security in their innovations. However, the complexities of leveraging multiple devices and applications, and the diverse communications infrastructure they rely on to operate expands the threat landscape enormously, complicating proactive security assessment. Once vulnerabilities are identified, how do you decide which need to be mitigated, or how to prioritize mitigation?

SecurityLabs Web Portal: Graphical Intelligence and Insights

Spirent provides company-wide vulnerability intelligence with its SecurityLabs web portal. The portal provides automated, deep and dynamic scanning and graphical risk metrics displayed on a dashboard. This allows users to gain quick insights into potential vulnerabilities across various networks, devices and applications without the physical presence of a security expert.

Our reporting tools are highly customizable, with the ability to provide a big picture or drill down into specific vulnerability details. The intelligence the portal provides about vulnerabilities in your applications, networks, devices and source code helps you prioritize risk and remediation efforts, so you can innovate with intention.
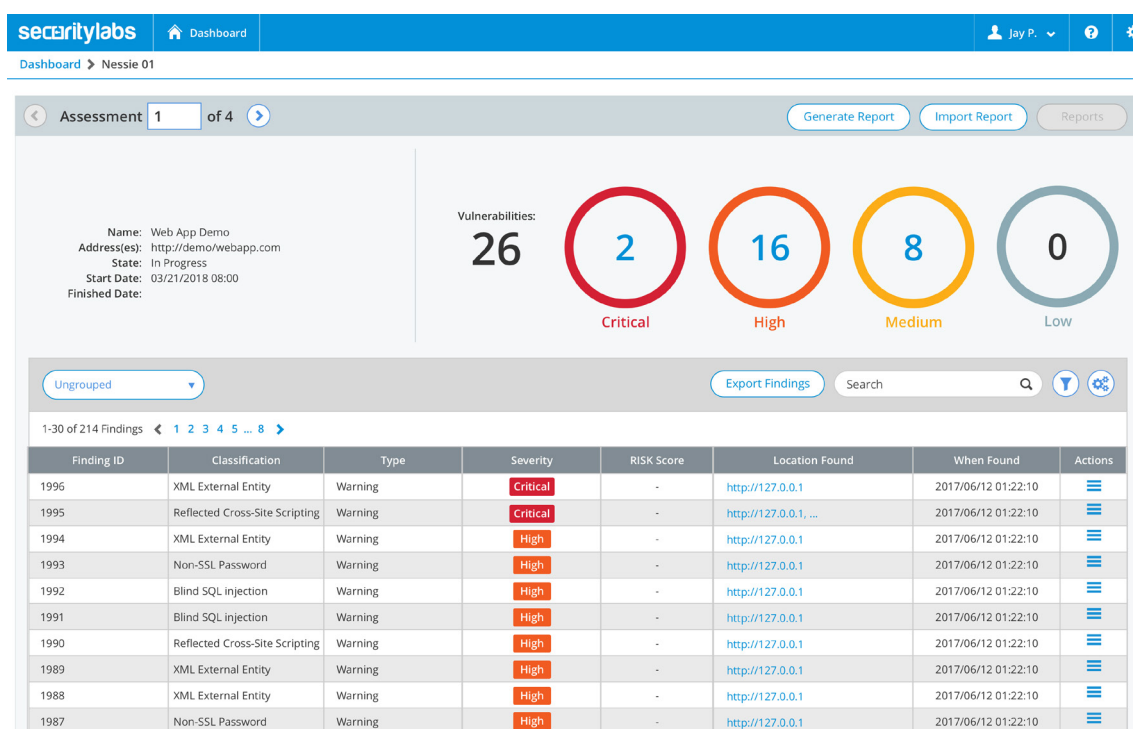

Figure 2: The SecurityLabs web portal graphically presents security intelligence that can be used to guide innovation projects and initiatives.

Leveraging Security to "Innovate with Intention"

The intelligence provided by Spirent solutions can also be used to dramatically improve the performance of security-related equipment, for example a firewall. With most firewall devices, the intent is that safe traffic goes through, and bad traffic is stopped. However, if the firewall inspects every bit of every traffic coursing through the network, performance bogs down to unacceptable levels. Armed with the intelligence provided by Spirent solutions, companies can determine the optimal configuration based on their unique risk tolerance and adjust firewall inspection policies accordingly.

CyberFlood Data Breach Assessment

In production environments, Spirent's CyberFlood Data Breach Assessment leverages a wide range of constantly updated threat intelligence feeds to provide accurate, continuous, thorough, and automated assessment of the organization's security posture, including:

- **Applications** ranging from Netflix to Salesforce to Skype, allowing security teams to validate app ID policies

- **Attacks & exploits** targeting known vulnerabilities, enabling teams to verify IDS/IPS security coverage

- **Malware threats** including near zero-day scenarios, so teams can verify malware prevention capabilities

- **Data Loss Prevention (DLP)** emulation, including corporate intellectual property and customer protected data, allowing teams to validate such sensitive data does not escape your organization's filters and policies

CyberFlood Data Breach Assessment also identifies security policy accuracy and policies that can degrade performance without providing additional security coverage. This enables companies to make changes and verify the balance between performance and security continuously.
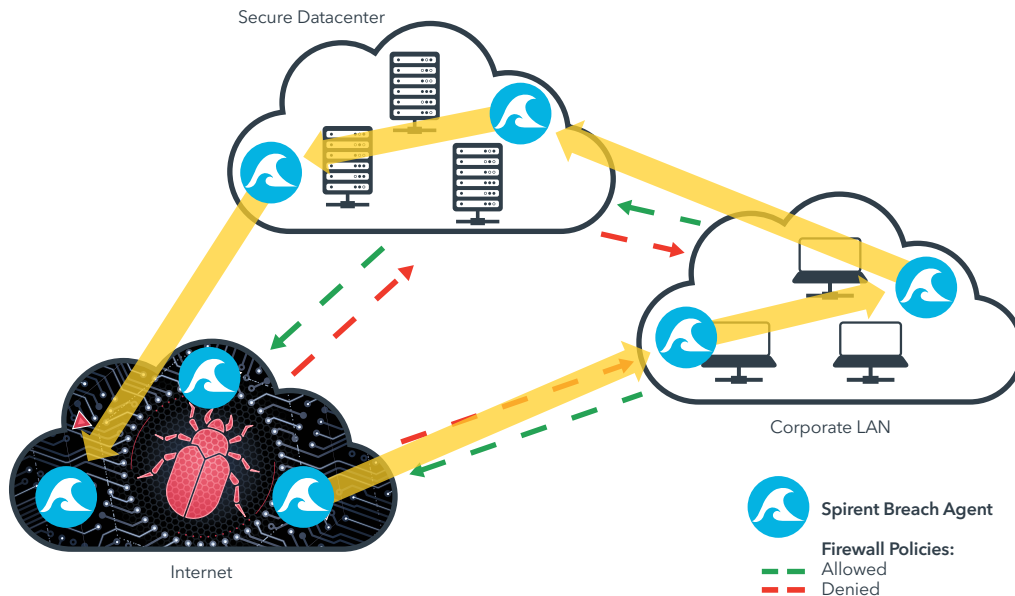

Figure 3: CyberFlood Data Breach Assessment makes it easy to find and fix security vulnerabilities—accurately and continuously.

In addition, the solution submits and tracks discovered issues into the most popular issue tracking systems such as ServiceNow, JIRA, and ZenDesk and even automatically re-runs assessments after remediation. This gives you a complete, end-to-end assessment including traceability from issue detection to resolution.

Bottom line: you can focus on creating new innovations without worrying about compromising on either security or performance.

#3: Leverage Ideas from Everywhere

Spirent believes that great ideas come from everywhere, and great ideas should be shared. That is why we deliver and support a community-oriented approach to innovation.

Our internal R&D teams work extensively with external teams from customer organizations; Network Equipment Manufacturers (NEMs), Service Providers (SPs) and other partners; research firms; and government organizations. The combined experiences and knowledge of this community informs and guides our own innovations as well as those of our community members.

The result for our customers is that we have implemented market-leading solutions that deliver the resources and agility to react quickly to changing market dynamics.

We are actively supporting and contributing to industry standards such as CTIA IoT Cybersecurity and NetSecOPEN as a founding member. Our support of these organizations continues with methodologies and practices to test against the standards.

Equally important, by harnessing the collective insights of both providers and users of global communication networks we are able to continue our tradition of innovating with intention, and we enable our customers to adopt that capability themselves.

Lowering the Barriers to Breakthroughs

Building security into all all aspects of product development accelerates innovation because it removes the obstacles to innovation—on multiple fronts. Specifically, it allows customers to:

Cut the cost of failure: Nothing dies harder than a bad idea. When security is not embedded into development, discovering a fatal security flaw just before deployment creates enormous expense and opportunity cost. With Spirent, it is far easier to validate good ideas because teams can test every idea quickly with total confidence in the security of the development process. Bad ideas fail faster, good ideas come to light sooner, and the investment in innovation is maximized.

Find the big idea faster: Incremental innovations such as product line extensions or feature improvements may generate modest incremental revenue, but studies have consistently shown that big revenue jumps come from big ideas. So how can teams sort through the good ideas and determine which ones are great? Many companies let potential breakthroughs die on the vine or be exploited by competitors because they can't get them to market in a timely way. With security embedded into operations, customers can transform ideas into products and services sooner, see which are gaining traction with real-world customers faster, and take them viral sooner.

Innovate without disruption: One of the key objections to traditional innovation processes is that they're disruptive to critical business processes— "change breaks things." With Spirent, innovation initiatives do not have to be huge undertakings that derail or redefine normal operations. Innovation can happen with small teams and small budgets, with the knowledge, approval, and involvement of all stakeholders, not through a back door or as an afterthought.

Formalize an innovation program: It's a vicious cycle: many companies have difficulty executing on new ideas, so they do not bother putting formal innovation practices in place, causing their innovation initiatives to continue to flounder. By making innovation with intention both possible and practical, Spirent can serve as a catalyst for instilling a culture of both innovation and security, while creating productive and sustainable ideation practices.

Leveraging Security to "Innovate with Intention"

About Spirent Communications

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks.

We help bring clarity to increasingly complex technological and business challenges.

Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

For more information, visit: www.spirent.com

Security: A Catalyst for Innovation

Spirent and its customers have seen that when security is built in rather than bolted on, and when security is used as a source of actionable intelligence, innovation initiatives can move ahead faster and more effectively. We encourage your organization to start seeing security as a catalyst for innovation rather than an obstacle, and to explore the myriad ways Spirent can help you innovate with intention.

spirent™
Promise. Assured.

Contact Us

For more information, call your Spirent sales representative or visit us on the web at www.spirent.com/ContactSpirent.

www.spirent.com

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com

Rev A | 07/19