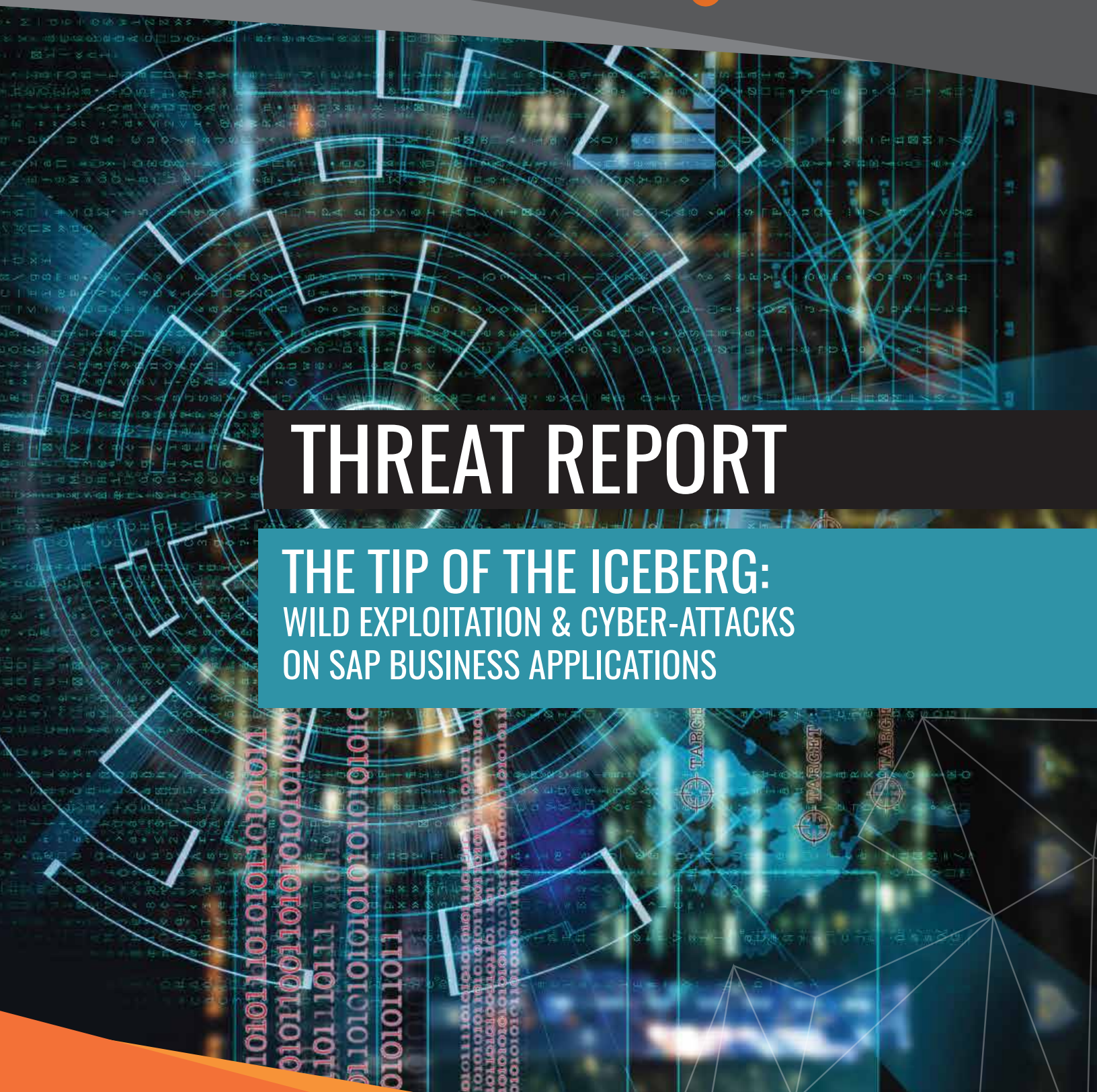
onapsis



THREAT REPORT

THE TIP OF THE ICEBERG:
WILD EXPLOITATION & CYBER-ATTACKS ON SAP BUSINESS APPLICATIONS

MAY | 2016

Version 1.0

TABLE OF CONTENTS

EXECUTIVE SUMMARY

SAP business applications run a vast number of commercial and government organizations that sustain global economies. SAP customers include 87% of Forbes Global 2000 companies, 98% of the 100 most valued brands and 44 of the world's military forces. SAP customers produce 78% of the world's food, 82% of the world's medical devices whilst 76% of the world's transaction revenue is processed by an SAP system [1]

As the leading provider of SAP and Oracle cybersecurity research and solutions, Onapsis is exclusively focused in securing these business-critical applications. As an SAP partner and the first to lecture on advanced SAP cyber threats, Onapsis experts have helped SAP SE by discovering, reporting and helping to mitigate more than 250 security vulnerabilities in SAP software, enabling SAP and its customers be more secure from the increasing risk of cyber-attacks.

IN EARLY 2016, THE ONAPSIS RESEARCH LABS DISCOVERED INDICATORS OF UNAUTHORIZED EXPLOITATION OF SAP VULNERABILITIES AT 36 GLOBAL ENTERPRISES.

These enterprises are located in, or are co-owned by corporations in the United States, United Kingdom, Germany, China, India, Japan, and South Korea, and span a number of industries including Oil & Gas, Telecommunications, Utilities, Retail, Automotive, Life Sciences, Consumer Products, Chemicals, High Tech, Engineering, Construction, Operations, Industrial Machinery and Components, Public Sector, and Higher Education.

While several threat reports disclose security incidents as the result of nation-state sponsored cyber campaigns, in this case, the reality (and what we believe makes this research even more interesting) is that these indicators had been silently sitting in the public domain for several years, until now. We regard these indicators as just the tip of the iceberg, as well as an irrefutable answer to the question "are SAP applications being attacked?"

The exploitation of the affected organizations' SAP systems was publicly disclosed during 2013-2016 at a digital forum registered in China. In all cases, the individuals leveraged a publicly-known SAP application vulnerability, for which SAP had released a security patch more than five years ago.

The exploitation of this vulnerability gives remote unauthenticated attackers full access to the affected SAP platforms, providing them with complete control of the business information and processes run by them, as well as potentially further access to connected SAP and non-SAP systems.

During April and May 2016, Onapsis alerted its customers and has worked in collaboration with the US Department of Homeland Security (DHS), in order to ensure that affected companies were informed and could mitigate the identified cybersecurity risks. Furthermore, the US-CERT has released an alert which summarizes the risks and solutions described in this document to further inform security professionals.

The goal of this threat report is to help Information Security, Internal Audit, and SAP teams protect their business-critical SAP applications from real-world cyber-attacks.

This document describes the specific vulnerability that is actively being exploited, the types of SAP systems affected, potentially compromised business processes and information, and the key recommendations on how to mitigate this vulnerability to minimize business risk.

1 http://www.sap.com/corporate-en/factsheet
http://www.sap.com/bin/sapcom/en_us/downloadasset.2014-12-dec-04-14.defence-and-security-sustaining-responsive-and-effective-defense-forces-pdf.html

ANALYSIS OF THE OBSERVED ATTACK VECTOR

All security incidents described in this threat report exploited the same fundamental vulnerability. In this section we analyze the nature of this vulnerability, the affected SAP solutions and the impact resulting from a successful exploitation.

SAP Java platforms have a wide of set of built-in functionality, providing a comprehensive framework of libraries and services to support the development and deployment of SAP applications in Java.

One of these functionalities is the Invoker Servlet, which is part of the standard J2EE specification of Sun (now Oracle). It was conceived as a rapid development instrument, allowing developers to test their custom Java applications. When enabled, developers and users can call servlets directly, without authentication or authorization controls.

The observed exploitations targeted SAP systems that had the Invoker Servlet enabled, and bypassed authentication controls to access a sensitive SAP Java application called Configuration Wizard/Template Installer, which provided functionality to execute arbitrary operating systems commands and create SAP user accounts.

The exploits can be performed by sending specific HTTP(S) requests to the vulnerable SAP system, which further increases the risk of attacks from remote locations and networks such as the Internet.

In summary, the impact of this attack is the worst possible outcome: a remote attacker can execute arbitrary operating systems commands with high-privileges and/or create SAP administration users, simply using a web browser and without the need to initially have a valid SAP user id and password in the target system.

As described before, SAP released security patches for these attack vectors several years ago. They have also disabled the Invoker Servlet functionality by default in newer SAP Java platforms.

The Onapsis Research Labs warned about this threat in 2011, publishing an SAP security in-depth whitepaper titled "The Invoker Servlet – A Dangerous Detour into SAP Java Solutions"[2].

It is very important to note that while the Invoker Servlet may be disabled globally, this setting may be overridden by specific or custom SAP Java applications. This introduces additional risks and makes it critical to also review custom applications and to deploy a continuous monitoring solution to ensure custom applications are not jeopardizing

KEY TAKEAWAYS

COMPANIES IMPACTED

Some of the largest global companies were impacted, including:

- One of the top ten highest annually grossing companies.
- 13 enterprises which each generate over $10B in annual revenue.
- Members of the Oil & Gas, Telecommunications, Utilities, Retail, Automotive, Life Sciences, Consumer Products, Chemicals, High Tech, Engineering Construction, Operations, Industrial Machinery and Components, Public Sector, and Higher Education.

THE ATTACK VECTOR

- Applications exploited were outdated and/or misconfigured SAP NetWeaver Application Server Java systems ("SAP Java platforms"). These serve as the foundational technology stack for several key SAP business solutions, information and processes.
- The vulnerability exploited has been identified as the Invoker Servlet vulnerability which was patched by SAP in 2010, and is being leveraged in tandem with a sensitive SAP Java application to remotely gain full administrative access to the SAP systems.

2 http://www.onapsis.com/research/publications/sap-security-in-depth-vol4-the-invoker-servlet-a-dangerous-detour-into-sap-java-solutions

the security of the entire system.

The SAP Java platform is a technology stack, which may not be easily recognized by business executives as being part of their SAP implementation. However, depending on the solution version, it is possible that this platform could be providing the base framework for many SAP business solutions that are currently in use by the organization. These include:

- SAP Enterprise Portal (EP)
- SAP Process Integration (PI)
- SAP Exchange Infrastructure (XI)
- SAP Solution Manager (SolMan)
- SAP Enterprise Resource Planning (ERP)
- SAP Customer Relationship Management (CRM)
- SAP Supply Chain Management (SCM)
- SAP Supplier Relationship Management (SRM)
- SAP NetWeaver Business Warehouse (BW)
- SAP Business Intelligence (BI)
- SAP NetWeaver Mobile Infrastructure (MI)
- SAP NetWeaver Development Infrastructure (NWDI)
- SAP Central Process Scheduling (CPS)
- SAP NetWeaver Composition Environment (CE)
- SAP NetWeaver Enterprise Search
- SAP NetWeaver Identity Management (IdM)
- SAP Governance, Risk & Control 5.x (GRC)

If any of these solutions are in use at your organization, it is highly recommended that you analyze whether they are leveraging the SAP Java platform (also referred to as the SAP J2EE Engine), regardless of whether it is in single stack or dual-stack mode. If these solutions are in use, and are not properly secured, they may be exposed to the attack vector described in this document.

ANALYZING THE BUSINESS IMPACT

As described in the previous section, a wide range of business solutions run on top of SAP Java platforms. This means that a significant number of critical business processes and information could be breached if these applications are compromised.

While many executives and security professionals consider SAP as a "backoffice financial system", in reality SAP applications are the lifeblood of many businesses, managing critical information such as intellectual property, HR data, pricing, purchasing agreements, bank accounts, credit cards, financial reports, manufacturing recipes, strategic plans, etc. Furthermore, they support and run processes related with areas such as sales & distribution, materials management, logistics execution, financial and managerial accounting, supply chain, payroll, e-recruiting, and many other functions.

Failing to properly secure SAP installations could have huge cost implications for an organization, including economic impact and compliance violations.

Economic impact will vary by organization depending on specific circumstances and use of the SAP applications, such as value chain affected. As a reference point, the CISO of a Fortune 100 company has estimated losses from an attacker breaking into and shutting down his organization's SAP systems at $22 million per minute.

Additional C-Level contacts at various Fortune 500 enterprises have disclosed that a compromise or termination of SAP-enabled processes could cease essential business functions and would potentially be categorized as an "extinction event" for their organization.

Moreover, as SAP runs several of the largest commercial and governmental organizations globally, a wide-scale attack against these applications could have macro-economic impact on most modern economies.

> "If SAP systems are taken offline, the expected average financial consequence for companies is $4.5 million. These costs include direct cash outlays, direct labor expenditures, indirect labor costs, overhead costs and lost business opportunity.
>
> **Ponemon Institute**

MITIGATION - PROTECTING YOUR SAP BUSINESS APPLICATIONS

Mitigating the Invoker Servlet (and related) vulnerabilities

To mitigate this vulnerability, it is necessary to disable the Invoker Servlet. This can be done by following the steps below:

1. Check if the property "EnableInvokerServletGlobally" is present in the SAP Java system. In case it is not, implement SAP Note 1445998. The implementation of this note will create the property that enables the disabling of the Invoker Servlet. It's important to note that SAP has disabled Invoker Servlet by default in 7.20 (in the patch levels described in SP Patch Level section of Note 1445998) and in the initial shipment of 7.30 version of the J2EE Engine. However, administrators could have changed this setting due to technical or business requirements and rendered the systems insecure.

2. Start the SAP J2EE configuration tool, select the "Global Server Configuration" in the cluster-data tree. Click on the services node and select "servlet_jsp". In the global properties list set the "EnableInvokerServletGlobally" to FALSE. Save the options and restart the instance.

3. Several business applications run on top of SAP Java systems. In the case that one of the following applications is running on your environment, make sure the mentioned SAP Security Notes are reviewed and implemented, otherwise business functionality may be disrupted or certain risks may remain active:
   - SAP Enterprise Portal - SAP Note 1467771
   - SAP BillerDirect – SAP Notes 1537663 and 1802092
   - SAP Virus Scan Engine – SAP Note 1900752
   - SAP CRM – SAP Notes 1598246 and 1488846
   - SAP Classified Advertising Management – SAP Note 1535301

4. Start the SAP J2EE configuration tool, select the "Global Server Configuration" in the cluster-data tree. Click on the services node and select "servlet_jsp". In the global properties list set the "EnableInvokerServletGlobally" to FALSE. Save the options and restart the instance.

Furthermore, as described before, specific or custom SAP Java applications may override the global setting for the Invoker Servlet, therefore it is important to review and mitigate these risks. These applications should use local specific servlets within their web.xml files. In order to achieve this, locate the <servlet-name>invoker</servlet-name> configuration in the web.xml file of the application and set its parameter InvokerServletLocallyEnabled to "false". Bear in mind that this may require reengineering the code of the application. More information can be found in the attachment in SAP Note 1445998.

STRATEGIC RECOMMENDATIONS

These findings highlight the existence of a dangerous blind spot for CISOs and CIOs: how can the applications which house an organization's crown jewels and run the most important business processes be exposed to such a critical security vulnerability, for which the vendor provided a patch more than five years ago? In light of these risks, we highly recommend SAP customers to:

- Understand their SAP implementation, its primary usage and processes as well as the key informational assets it manages.
- Continuously identify existing vulnerabilities and SAP interfaces to understand the attack surface.
- Correlate vulnerabilities to corporate risk posture to determine top risks to the business and prioritize remediation efforts and potential compensating controls.
- Maintain SAP cybersecurity standards, guidelines and patching processes to stay aligned with the latest security patches and improvements provided by SAP.
- Implement detective monitoring capabilities to gain visibility into indicators of compromise regarding the use of known SAP exploits, zero-days and suspicious SAP user activity.
- Integrate Information Security, Audit, SAP Security & BASIS teams into an SAP cybersecurity program

CONCLUSIONS

Business-critical applications running on SAP house the "crown jewels" of any large organization, and they are no longer confined to "internal" or isolated networks. SAP implementations have transformed through trends like cloud, mobile, big data and IoT, all of which expand the attack surface of a company and these applications. Effectively securing SAP applications is critical to accelerate the adoption of these new technology paradigms and to enable companies to realize the maximum value from their investment in SAP solutions.

As the leading SAP partner in cybersecurity, Onapsis has seen first-hand how SAP is significantly increasing its efforts in providing more secure business software. At the same time, it is important for customers to recognize that SAP is not a cybersecurity company and, just like with any other major software vendor, applying security patches and recommended security configurations depends on your own organization and cybersecurity partners.

These findings are a clear example of how attackers are leveraging an organizations' lack of governance over the security of business applications, as SAP made a security patch available several years ago.

While this is the first threat report that undercovers the active exploitation of SAP systems publicly, we know for a fact that this is just the tip of the iceberg. These findings only refer to the exploitation of a single vulnerability. SAP has released over 3,000 security patches to date, issuing on average over ~30 security patches per month .

Based on our experience engaging with large SAP customers, we often find vulnerabilities present in systems despite SAP having released patches as far back as 10 years ago. This is very common in a vast majority of the implementations we've seen, and provides both insiders and remote attackers with wide-open doors into the heart of large enterprises. Our team has also been engaged in a number of SAP forensics & incidents response projects, resulting from real-world breaches to SAP applications.

Still, many organizations lack the proper preventative, detective and corrective controls to secure a company's SAP applications, and have a reigning false sense of security provided by generic security products, GRC solutions and traditional Segregation of Duties controls and audits. While all these efforts, processes and technology are necessary to protect SAP systems, they are not designed to provide deep visibility, control and protection against remote cyber attackers and malicious insiders targeting SAP business applications.

The status-quo is not sustainable. According to IDC "because over 75% of all transactions occur on business-critical applications, data from these systems is endlessly valuable to attackers". In this scenario, business applications provide the best possible economics for cyber attackers: The world's largest organizations running on the same highly-complex technology platform, which is usually exposed to known vulnerabilities and has high-value business assets and processes by definition. On top of that, attackers enjoy of reduced chances of being detected, due to several organizations still missing the right governance model and specialized solutions.

Given the cross-functional nature of these applications, it is imperative to implement a proper SAP cybersecurity program that is aligned to effectively secure SAP applications and data. As with any security initiative, it takes the right combination of people, process and technology to be successful.

WE HOPE THAT THIS THREAT REPORT HELPS BRING VISIBILITY TO THIS OVERLOOKED AREA, AND EMPOWERS EXECUTIVES TO MITIGATE WHAT WE BELIEVE IS ONE OF THE MOST CRITICAL CYBER RISKS TO THEIR ORGANIZATIONS.

ABOUT ONAPSIS

Onapsis provides the most comprehensive solutions for securing SAP and Oracle enterprise applications. As the leading experts in SAP and Oracle cybersecurity, Onapsis' patented solutions enable security and audit teams to have visibility, confidence and control of advanced threats, cyber-risks and compliance gaps affecting their enterprise applications.

Onapsis provides the most comprehensive solutions for securing SAP and Oracle enterprise applications. As the leading experts in SAP and Oracle cyber-security, Onapsis' patented solutions enable security and audit teams to have visibility, confidence and control of advanced threats, cyber-risks and compliance gaps affecting their enterprise applications.

HEADQUARTERED IN BOSTON, ONAPSIS SERVES OVER 200 GLOBAL CUSTOMERS INCLUDING MANY OF THE GLOBAL 2000.

Onapsis solutions include the Onapsis Security Platform, which is the most widely-used SAP-certified cyber-security solution in the market. Unlike generic security products, Onapsis' context-aware solutions deliver both preventative vulnerability and compliance controls, as well as real-time detection and incident response capabilities to reduce risks affecting critical business processes and data. Through open interfaces, the platform can be integrated with leading SIEM, GRC and network security products, seamlessly incorporating enterprise applications into existing vulnerability, risk and incident response management programs.

These solutions are powered by the Onapsis Research Labs which continuously provide leading intelligence on security threats affecting SAP and Oracle enterprise applications. Experts of the Onapsis Research Labs were the first to lecture on SAP cyber-attacks and have uncovered and helped fix hundreds of security vulnerabilities to-date affecting SAP Business Suite, SAP HANA, SAP Cloud and SAP Mobile applications, as well as Oracle JD Edwards and Oracle E-Business Suite platforms.

Onapsis has been issued U.S. Patent No. 9,009,837 entitled "Automated Security Assessment of Business-Critical Systems and Applications," which describes certain algorithms and capabilities behind the technology powering the Onapsis Security Platform™ and Onapsis X1™ software platforms. This patented technology is recognized industry wide and has gained Onapsis the recognition as a 2015 SINET 16 Innovator.

For more information, please visit www.onapsis.com, or connect with us on Twitter, Google+, or LinkedIn.