State of Enterprise Resource Planning Security in the Cloud

Presented by the ERP Security Working Group

cloud security alliance®

TABLE OF CONTENTS

THANK YOU

The Cloud Security Alliance (CSA) is a not-for-profit, member-driven organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. CSA's activities, knowledge, and extensive network benefit the entire community impacted by cloud — from providers and customers, to governments, entrepreneurs and the assurance industry — and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem. CSA research prides itself on vendor neutrality, agility and integrity of results.

Thank you to our sponsor, Onapsis, for helping fund the development and quality control of our research lifecycle.

Sponsors are CSA Corporate Members who support the findings of the research project but have no added influence on the content development or editing rights of CSA research.

Sincerely,

Your CSA Research Team
J.R. Santos, Executive Vice President of Research at CSA Global

1. INTRODUCTION

Enterprise resource planning (ERP) solutions are the most widely implemented information technologies used to elevate business processes in a modern enterprise.

With the increasing adoption of cloud computing, many of these solutions are migrating to the cloud. As cloud environments are different from traditional IT environments, organizations wanting to move such functions or processes to the cloud face several challenges. This document briefly highlights some of these issues through an examination of common security and privacy risks that organizations incur during a transition to the cloud, as well as how organizations have mitigated these hazards.

The main objective of the document is to provide a brief introduction to cloud ERP security. The targeted audience of this document includes IT and management professionals who oversee the business IT assets of their respective organizations.

This document was created by the Cloud Security Alliance (CSA) ERP Security Working Group. The CSA ERP Security Working Group seeks to develop best practices to support organizations that are actively working toward the goal of securely migrating or operating their large ERP implementation (as well as all other business-critical applications) in the cloud.

The following individuals have contributed to the creation of this document:

Gururaj Adiga
Yazan Almasri
Victor Chin
Vic Chung
Tom Evgey
Aiyan Ma
Matt Mason
JP Perez-Etchegoyen
Malini Rao

2. BUSINESS-CRITICAL APPLICATIONS

Today, every modern organization in the world greatly depends on technology to run their daily business operations. The mechanisms that support these daily business operations are typically known as business-critical applications. They are responsible for setting a common platform to ensure that operational efficiency is implemented across the entire enterprise. By nature, business-critical applications handle the most sensitive and valuable data that organizations generate. As such, the need to secure these applications has become a board-level initiative in organizations around the globe.

As defined in the latest Gartner Hype Cycle for Application Security-2017[1]: "Business-critical application security is the set of processes and technologies that focus on the security, risk and compliance of business-critical applications."

When it comes to business-critical applications, two of the most well-known vendors are SAP and Oracle, which are used to underpin hundreds of different applications. Some examples are:

- ERP Solutions, or enterprise resource planning
- CRM, or customer relationship management
- SCM, or supply chain management
- HCM, or human capital management
- SRM, or supplier relationship management

Each one of these applications (examples listed previously) are running a variety of business processes, highlighted in Figure 1 below.

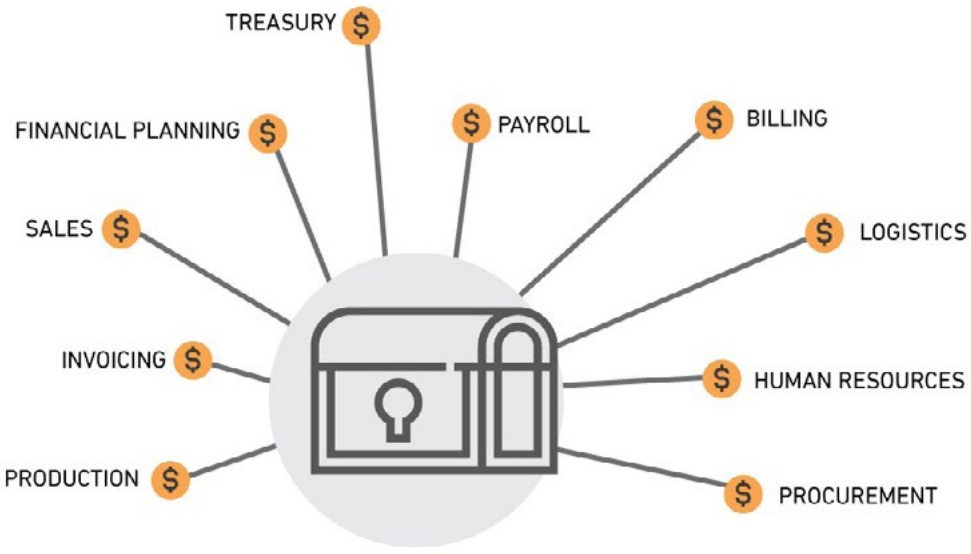

Figure 1: Examples of processes supported by "Business-Critical Applications"

But what characteristics make these applications unique? How are these applications different from our mail application, our Intranet, our internal ticketing system or our Web server? The answer is shown in Figure 2 below.

Figure 2: Key characteristics of "Business-Critical Applications"

A deficiency in any of these characteristics can jeopardize the ability of organizations to run secure business-critical applications.

3. CLOUD ADOPTION

Organizations deploying ERP systems today often have three deployment models to choose from: on-premise, hosted, and cloud-based. Cloud-based ERP solutions, in particular, are gaining a lot of momentum and discussions in the marketplace, with market-size projections calculated at between $25-30 billion over the next five years. From a strategic perspective, cloud-based ERP deployments are promising because of their simplicity and their lower cost of ownership over conventional on-premise and hosted ERP solutions.[2]

As an ERP vendor, Oracle suggests at least three advantages of running ERP applications in the cloud: faster time to value, increased innovation, and scalability with growth.[3] Enterprise resource planning cloud solutions have matured rapidly in recent years, making them a viable choice for customers when they renew their technology infrastructure or embark on digital transformation. In a recent forecast, the International Data Corporation (IDC) predicts public cloud services spending levels to reach $266 billion in 2021, with a 21.0 percent compound annual growth rate from 2017 to 2021. Customer relationship management (CRM) and enterprise resource management (ERM) are highlighted as core focuses for application-based Software as a Service (SaaS) expenditures.[4] Such forecasts set the tone for the future of cloud-based ERP applications, with adoption remaining an important consideration for many organizations.

ERP vendors are reporting double-digit growth in cloud revenue year-over-year in 2017.

From a business standpoint, ERP vendors report double-digit growth in cloud revenue year-over-year in 2017, while on-premise software revenue has increased at a steady single-digit percentage point.[5] For example, SAP reported a 33 percent increase in its new cloud bookings during the second quarter of 2017. Compounded with its in-memory business application portfolio (e.g., S/4HANA), SAP was able to raise its full-year revenue outlook by two percentage points.[6]

Business digital transformation projects have been an important driver of cloud adoption over the last few years, and cloud computing—in all its models—remains a key component to digital transformation of ERP applications. Security requirements such as assessment, monitoring and front-end visibility are often enlisted as important prerequisites for these transformational projects. As with new technologies, there are new challenges and, potentially, even an increase in the attack surface of ERP applications.

4. COMMON CHALLENGES IN CLOUD ERP SECURITY

As cloud adoption accelerates on all fronts, ERP solutions have also seen a significant expansion. Enterprise resource planning vendors are making great strides to create a homogeneous product that can be built on various cloud platforms (e.g., Azure, AWS). Currently, the SaaS and IaaS have been predominantly utilized because of the ease of deployment and scalability. Potentially, cloud ERP solutions have the capability to bring core competencies from across the enterprise together into a unified, central system, which aggregates and manages data from all disciplines.

As with any technology implemented in the cloud, security risks and challenges need to be managed and overcome. Enterprise resource planning applications are particularly at risk given the nature of their functions. Moreover, as this new technology continues to develop maturity in the cloud space, organizations rely on the cloud service provider (CSP) to implement better security measures than they would have otherwise used on-premise.

Organizations must consider those security challenges when migrating their ERP solutions into the cloud. Potential considerations may range from general security concerns to complications specific to the cloud service model being adopted. The cloud service model will drive the responsibilities and ownership of some of the key characteristics of business-critical applications. The following figure illustrates this principle as it pertains to different cloud service models, including on-premise.

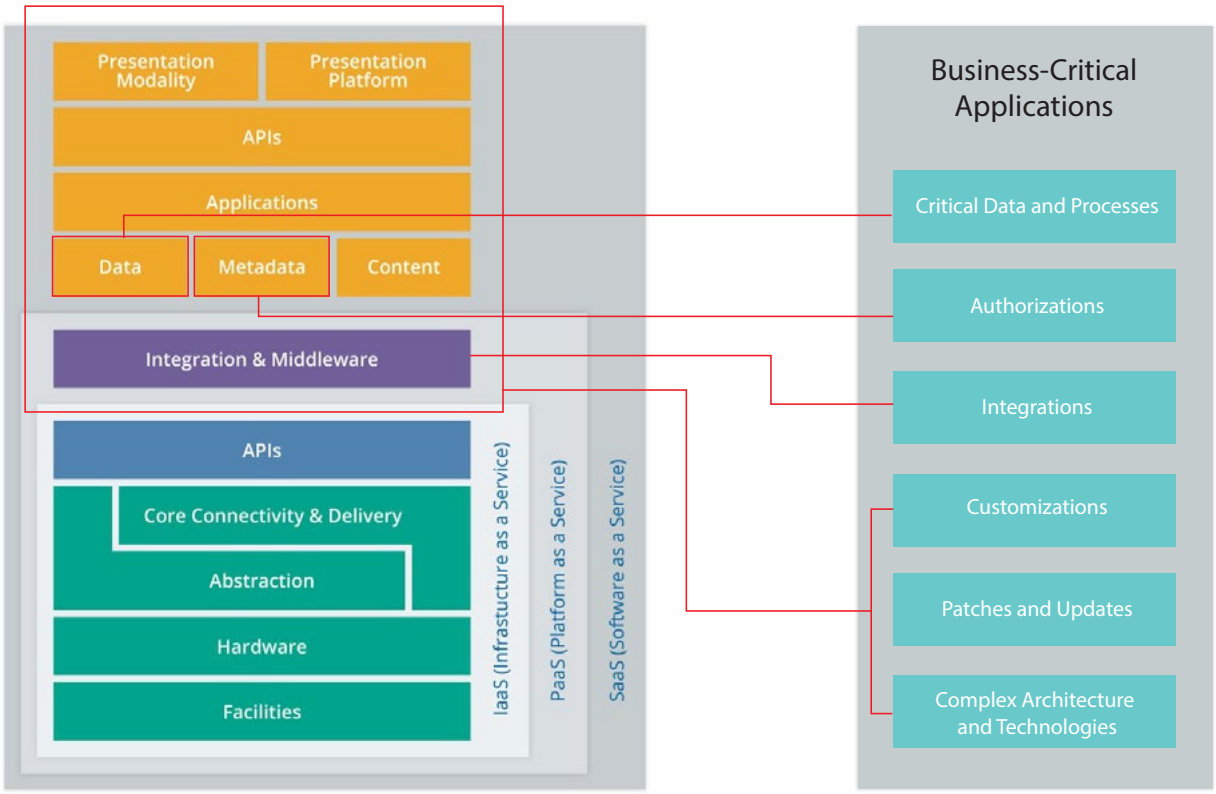

Figure 3: The cloud computing stack in relation to cloud service models[12]

It is vital for organizations to understand and evaluate all the risk factors involved with ERP migration, provisioning and consumption of such services. At the end of the day, an organization's critical data should be protected both on-premise and in the cloud, and the implementation of security controls will help minimize an organization's risk of being exposed and ultimately breached.

Over the years, CSA developed the Cloud Controls Matrix (CCM).[9] This guide was specifically designed to provide fundamental security principles that would assist cloud vendors and prospective cloud customers in assessing the overall security risks of a cloud provider. The CCM consists of 133 security controls categorized into 16 domains that can be used to secure a cloud computing environment. Enterprise resource planning customers migrating to the cloud should use these controls as a base framework to start analyzing cloud options, while complementing it with upcoming publications of the CSA ERP Security Working Group.

5. GENERAL SECURITY CONCERNS IN CLOUD-BASED ERP APPLICATIONS

Security in the cloud has been one of the biggest concerns that have prevented organizations from adopting cloud-based ERP applications en masse. However, in the last five years, there has been a marked improvement in cloud security. With the sensitivity of a business-critical application like ERP in mind, this section will present some of the concerns that should be considered for a safe shift to the cloud. Some of these concerns are addressed by technologies that help ensure ERP environments are secured, aside from any in-app security features.

Data Residency

An ERP application's most important asset is the data it holds, and this information is often subject to multiple regulations. Most cloud ERP vendors will allow the customer to choose the datacenter, and therefore the geographical location of its data. In light of the upcoming European General Data Protection Regulations (GDPR), there are restrictions and considerations which need to be addressed in regards to the privacy of personal data, the controls used and where that data resides. Compliance with these regulations may add some restrictions to customer flexibility. Other regulations, such as International Traffic in Arms Regulation (ITAR), might also mandate where the data will reside, as well as the citizenship of the people who manage it. Therefore, when choosing a cloud ERP vendor and datacenter, it is imperative that organizations consult with their legal and compliance teams to determine appropriate next steps in the process, while also confirming a cloud service provider's commitment of regulatory adherence.

User Provisioning, Authentication, Authorizations and Single Sign-On

Enterprise resource planning applications usually come with their own identity management solutions, as well as multiple single sign-on (SSO) options. There are a variety of ways to provide SSO options, but one of the most commonly used standard is the Security Assertion Markup Language (SAML) standard. The SAML standard allows single sign-on (SSO) authentication between an identity provider and multiple applications via the use of digitally signed XML documents.

The identity provider can be an on-premise service which is extended to provide authentication and authorization to cloud solutions. This option is normally taken by organizations utilizing existing on-premise identity providers. For example, if an organization is already using Active Directory, this can be extended for cloud authentication and authorization by using Active Directory Federation Services (ADFS), which allows for faster provisioning for users in cloud services.

Alternatively, an organization can use a third-party identity provider to deliver SSO to cloud services. These third-party identity providers are usually off-site and provided as a service. Additionally, when using a third-party identity provider, it is important to determine if the cloud ERP application supports the various SSO protocols. If organizations choose not to use an identity management solution or provider, most cloud ERP solutions already allow the provisioning and management of users and authorizations as a standard functionality.

User Activity and Access Monitoring

User activity and access monitoring essentially provides visibility around what the users are doing at any point in time and detect malicious and anomalous user behavior. This is important because the day-to-day functioning of large organizations require employees of various trust levels and roles to have access to ERP solutions and other business-critical applications, as well as the highly sensitive data that resides in them. Such access and the subsequent user activity has to be monitored to ensure that no malicious activity is happening.

The different cloud service models (IaaS vs. SaaS) will likely require customized solutions, but conceptually the need is the

same for both. Audit trails are typically provided by the application vendor or, if not, obtained from other sources such as an identity provider or a Cloud Access Security Broker (detailed later in the document).

Security Vulnerabilities Management

When using SaaS ERP solutions, organizations are shifting control and accountability over to the SaaS provider who manages the patching and availability of the system for the customer/organization. Organizations may need to agree to specific maintenance periods when patching can be done if they operate change management. Patching will also ensure that any new features are compatible with an organization's data and workflow. A failure to understand the importance of these steps could lead to a loss of service, corruption of data or system unavailability. Shifting the responsibility to the SaaS provider enables greater flexibility and availability to the system. While it is the responsibility of the SaaS provider to ensure that its products and services are free of vulnerabilities, organizations must ensure the provider is actually performing this management.

In IaaS, patching can be either outsourced to the cloud service provider where patching should be part of the agreement), or controlled by the organization's technical team. Ultimately, however, it is always the customer responsibility. Therefore, a validation process should be implemented to ensure the system is up-to-date with security patches.

Disaster Recovery Planning (DRP)

Disaster Recovery Planning capabilities can be considered as one of the direct benefits of shifting business applications to the cloud. Whether IaaS or SaaS, the cloud provider can shift to other data centers around the world in case of a major disruption.

Virtualization technology has dramatically bolstered the effectiveness of cloud computing, making DRP issues easier to comprehend while increasing operational efficiency. In short, there are more benefits that can be found in a cloud-based DRP. Cloud environments meticulously made the process of monitoring and validating disaster readiness easier in a scalable way.

Due Diligence and Service Level Agreements

Measuring and validating the status of compliance of ERP vendors to various standards can be challenging. Many of them provide listings of frameworks they conform to, as well as audit standards and attestations they maintain. Other vendors will not be so forthcoming. As a preventative measure, organizations are encouraged to exercise due diligence and check ERP vendor standards and attestations that have been claimed as valid. Additionally, Service Organization Control (SOC) reports and customer testimonials can be reviewed and screened through a risk management process to aid in the selection of a cloud provider.

Confounding the problem, many SaaS vendors host their products on third-party IaaS infrastructure. In these cases, the SaaS vendor may not have visibility into how that infrastructure is managed and patched. However, the SaaS vendor might procure an IaaS vendor who can provide attestation (e.g., ISO27K or ISAE3402) to an equivalent of their own standards. This would provide appropriate visibility and would then be considered within the SaaS providers ISAE3402 / SOC report.

During these initial vetting stages, it is important that organizations seeking a transition to cloud ERP applications receive full disclosure during the acquisition process. A risk management approach should then be applied to examine the benefits of the move, compared to the residual risks posed by the uncertainty of ERP provider performance related to compliance and audit attestations.

If cloud service is compromised, customer data may also be compromised, leading to regulatory control and possible fines if data is lost. Exercising due diligence when selecting a cloud provider and ensuring that it is complying with controls, such as the CSA Cloud Controls Matrix (CCM)[9] or the ISO/IEC 27000 series (i.e., ISO/IEC 27001, 27017, 27018 and 22301) is critical. These steps will lower the risk of customer vulnerabilities while ensuring that SSAE 16 SOC/ISAE3402 audits are completed and demonstrated—which can boost confidence in a cloud service provider's (CSP) operations. Finally, the CSA STAR Registry[10] is a useful tool to round out the due diligence process. The registry houses self-assessments of CSP's that have made their Consensus Assessment Initiative Questionnaire (CAIQ)[11] public and available for review.

Incident Response (IR)

Due to the nature of ERP applications, organizations need to be ready for a compromising incident. While this preparation starts with an IR plan, organizations must also be able to secure the correct data at the appropriate time from the cloud provider when an incident does occur. Establishing the ability to ask for logs and traces to the cloud provider (especially when needed for an investigation) is the most important and challenging component of building a proper IR plan. To that end, this process should be highlighted in the cloud provider service contract.

5.1 SECURITY AROUND SAAS ERP APPLICATIONS

Applications of today are more and more interconnected. Most importantly, they are Internet-facing to provide direct service and continuous availability to both organizations and their customers. Thus, they have become a primary attack surface. Cloud ERP applications (in SaaS mode) are typically exposed as web applications available to the Internet and accessible through a Web browser or mobile application from anywhere in the world.

Although there are many applications of different functions and purposes, they are—from a security point of view—usually the same or similar in nature. For instance, software design, implementation and integration of security controls remain similar.

In SaaS environments, customers should consider if vendors provide information and solutions to address key components, such as:

- Sensitive data storage, including key management
- The leveraging of the application programming interface (API) security mechanism
- Input output validation
- Security Audit and logging
- Exception handling fail (security, fail closed)
- Server side hardening, etc.
- Proper tenants and infrastructure separation

Organizations seeking visibility via ERP access in the cloud should consider using a cloud access security broker (CASB), where rules and conditions are defined to control data access, system access, data leak prevention, Tokenization, multi-factor authentication (MFA), and encryption. Cloud access security broker solutions can be deployed on-premise or as a cloud service. Accordingly, the risks of such deployments need to be considered prior to deploying into cloud services. Additionally, CASB solutions can perform user behavior analytics to identify anomalous behavior and take reactive steps that can prevent user access and/or features in the service. An alternative is to integrate logging options in the CASB with existing security information and event management (SIEM). While SIEM is a good choice for event and audit logging, it is ultimately up to organizations to decide if logging options available in the CASB are sufficient alone, or whether they

should be integrated with an SIEM solution.

5.2 SECURITY AROUND IAAS ERP DEPLOYMENTS

IaaS-based ERP applications are hosted on public, private or hybrid cloud infrastructure such as Oracle Cloud, SAP HEC, Amazon Web Services, Microsoft Azure, IBM Softlayer, Google Cloud, and SAP S/4 HANA hosted on Cloud4c Managed Services IaaS Cloud.

In this specific cloud service model, customers are running the same applications that they use to run on-premise, but in a different environment that is typically hosted in the cloud. This brings a shift of some responsibilities—especially in security—that will be reflective of the type of services and contracts that have been reached with the cloud vendor.

In most cases, the customer still needs to manage the application security level just as they would on-premise. Typically, cloud providers will secure the operating system and databases in addition to taking care of the security of other components, such as hardware and network needs. In any case, it is advised that organizations actively develop mature security postures, and take the approach of trust but verify. This means that security responsibilities are handled by a third party, but the customer still implements the means to test and validate these measures.

As mentioned previously, ERP applications are complex when running in the cloud, as it puts the customer in charge of dealing with the following security challenges:

- **Implementation of Security Patches:** Vendors of ERP applications are continuously publishing patches to address new security vulnerabilities that should be implemented to reduce risks. This is typically supported by vulnerability management solutions that help identify missing patches in ERP applications.
- **Hardening and Securely Configuring the Application:** Due to the complexity of ERP applications, securely configuring them poses challenges and needs that should be addressed holistically. Sometimes, users of ERP applications change settings that could render the entire system vulnerable to cyberattacks; this can be detected early with proper monitoring and through strict change management processes.
- **User Provisioning and Authorizations:** This is well-known to ERP applications; due to the granular level, it requires specific expertise to avoid assigning broad authorizations to users.
- **Integrations with ERP Applications:** ERP customers typically run hybrid environments, where interfaces are connecting multiple on-premise and cloud-based applications. Therefore, enabling reliable, secure, and bi-directional communication between applications and the cloud is another important security concern for cloud ERP applications. Typical examples include opening specific ports on the firewall, and enabling Web services and associated Web Services Definition Language (WSDL) files. Customers must have the capacity to leverage a consistent approach which incorporates environment-specific policies and baselines that are defined using the risk profile of an organization.
- **Application Monitoring:** ERP applications implement different concepts—such as access to reports, functions and transactions—to identify user activities. Due to the criticality of ERP applications in the cloud, continuous monitoring must be implemented to ensure that no unauthorized or malicious activity is being executed.

It is crucial to have visibility and control over the previously mentioned key security aspects of cloud ERP applications running in the IaaS service model. Organizations need to work collectively with cloud service providers to enable additional configurations and ensure that all relevant security requirements are adhered to. In reality, this type of collaboration is becoming a competitive advantage and a key differentiator of cloud providers that host ERP applications. Furthermore, some business transformation projects have been delayed or even stopped due to provider inability to add

security and protection features[11].

5.3 SECURITY AROUND ERP EXTENSIONS IN PAAS CLOUD

The biggest cloud ERP vendors provide capabilities to enhance standard ERP applications by incorporating entirely new functionalities. These extensions can be developed as new applications in the cloud, typically in a Platform as a Service (PaaS) model.

When developing these extensions, it is key to address potential security vulnerabilities incorporated by the developers. The Open Web Application Security Project (OWASP) "Top 10 Most Critical Web Application Security Risks"[7] and the Common Weakness Enumeration (CWE) are good resources for understanding risks in the PaaS ERP Web extensions universe. These should also be incorporated into design and coding best practices for all application software extensions.

To effectively tackle these challenges, Security Development Life Cycle (SDLC) must be implemented to ensure that security concerns are appropriately considered at the design phase, as well as throughout all other phases of the SDLC. Important aspects to consider include: security awareness training; threat modeling; impact analysis; static analysis; dynamic analysis; penetration testing; security review before software release; incident response protocol; patching; and other maintenance tasks.

Security assessments of application and security controls should be undertaken. Authorization must be obtained prior to conducting any of these tests, and tests should be documented. When non-compliant controls are identified, these must be corrected and retested.

6. CONCLUSION

The cloud computing ecosystem is maturing rapidly, and business-critical applications such as ERP solutions are being moved to cloud environments. With this shift, organizations are starting to explore what options they have in the cloud, and if it's possible that a cloud environment might alleviate traditional challenges that business-critical applications normally face. On the other hand, moving to the cloud raises its own security challenges as well.

The transition organizations face when deploying or operating business-critical applications in the cloud is complicated by the fact that cloud service providers must be depended on to solve many security challenges. Key security concerns include: clearly defined security responsibilities; visibility of cloud SaaS applications; and keeping up with the security of ERP applications when running them through third-party providers (IaaS).

Additionally, as business transformation drives most cloud ERP adoption, customers planning on executing such projects should ensure security is amongst the key requirements of the effort. If security is not addressed at the front line of these projects, the costs could significantly increase, potentially compromising project deadlines.

In conclusion, the Cloud Security Alliance ERP Security Working Group plans to address all of the previously mentioned security concerns in future documents. The group's goal is to provide appropriate and comprehensive guidance for enterprises seeking to operate and deploy business-critical applications in the cloud.

REFERENCES

1. Gartner (2017), Hype Cycle for Application Security, 2017
(https://www.gartner.com/doc/3772095/hype-cycle-application-security-)

2. Strategy& / PWC (2013), ERP in the cloud
(https://www.strategyand.pwc.com/media/file/Strategyand_ERP-in-the-Cloud.pdf)

3. Oracle (2014), The Benefits of ERP in the Cloud
(http://www.oracle.com/us/corporate/profit/big-ideas/072114-hcastel-2245635.html)

4. International Data Corporation (2017), Worldwide Public Cloud Services Spending Forecast to Reach $266 Billion in 2021, According to IDC
(https://www.idc.com/getdoc.jsp?containerId=prUS42889917)

5. Fortune (2017), Why Fortune 500 Companies Are Trusting the Cloud More Than Ever
(http://fortune.com/2017/09/13/amazon-microsoft-google-sap-cloud/)

6. SAP (2017), SAP Q2 2017 Quarterly Statement
(https://www.sap.com/docs/download/investors/2017/sap-2017-q2-statement.pdf)

7. OWASP (2013), Top 10 2013-Top 10
(https://www.owasp.org/index.php/Top_10_2013-Top_10)

8. Cloud Security Alliance (2016), The Treacherous 12: Cloud Computing Top Threats in 2016
(https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf)

9. Cloud Security Alliance (2017), Cloud Controls Matrix v3.0.1 (9-1-17 Update)
(https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/)

10. Cloud Security Alliance (2017), CSA Security, Trust & Assurance Registry (STAR)
(https://cloudsecurityalliance.org/star/#_registry)

11. Cloud Security Alliance (2017), CSA Consensus Assessment Initiative Questionnaire
(https://cloudsecurityalliance.org/group/consensus-assessments/#_overview)

12. Cloud Security Alliance (2017), Security Guidance for Critical Areas of Focus in Cloud Computing v4.0
(https://cloudsecurityalliance.org/download/security-guidance-v4/)

ABOUT SPONSOR

Onapsis is the pioneer in cybersecurity and compliance solutions for cloud and on-premise business-critical applications. As the proven market leader, global enterprises trust Onapsis to protect the essential information and processes that run their businesses.

Headquartered in Boston, MA, Onapsis serves over 200 customers including many of the Global 2000. Onapsis' solutions are also the de-facto standard for leading consulting and audit firms such as Accenture, Deloitte, E&Y, IBM, KPMG and PwC.

Onapsis solutions include the Onapsis Security Platform for SAP and the Onapsis Security Platform for EBS. 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.

Find them at https://www.onapsis.com.