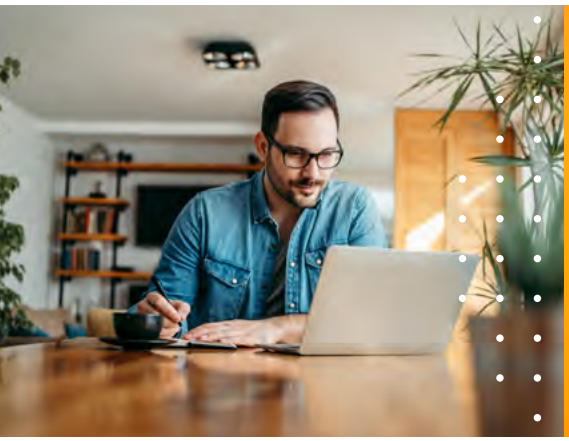
ONAPSIS

WHITEPAPER

5 Reasons Why You Need **Vulnerability Management** for Business-Critical Applications



At the center of every enterprise organization are certain critical applications for core functions such as finance, manufacturing, human resources, sales, and supply chain management. Whether they exist on premises, in the cloud, or as a mix of both, an attack against any of them has the potential for a devastating impact across the entire organization. To protect these business-critical applications, enterprise organizations commonly employ a "defense-in-depth" security model (i.e., applying layers of technology to protect critical systems), but, unfortunately, not enough consideration is given to the last layer of security for the critical application itself, especially since these systems are frequently managed by information technology professionals focused more on development and continuity rather than security.

An attack against a business-critical application could weaponize the rights and privileges of an administrator. If an administrator role is hijacked, the attacker could bypass all controls of the application, as well as its business data and processes. Successfully exploiting a vulnerable system allows an attacker to execute a wide range of malicious activities—from impacting supply chains and manufacturing processes to redirecting financial payments to compromising highly sensitive data, most of which is subject to compliance regulations.

The need to have a solution in place that is tailored to protect these business-critical systems is more urgent than ever before. Here are five reasons why you need vulnerability management capabilities specifically designed for your most business-critical systems.

[1]

Market Conditions of the Last Year Have Accelerated the Pace of Digital Transformation

Business-critical applications (or the "crown jewels" as they are often referred to) hold the most valuable business data, such as patents, processes, financial data, customer and employee data, and other sensitive information. Traditionally, best practices were to keep these systems on-premises and to install layers of security around them, creating a theoretical and impenetrable fortress of castle walls and moats. However, the shift of the traditional on-premises perimeter to a distributed hybrid cloud model, and the need for every organization to transform how it does business digitally has changed this paradigm.

SUPPLY-CHAIN DIGITIZATION IS ACCELERATING AT A PACE OF 3 TO 4 YEARS SOONER THAN PLANNED.[1]

[1] McKinsey Digital and Strategy & Corporate Finance Practices How COVID-19 has pushed companies over the technology tipping point—and transformed business forever October 2020

[2]

The Shift to the Cloud Leaves Business-Critical Applications Vulnerable

Digital transformation projects were underway before 2020, but the global impact of the COVID-19 pandemic accelerated the digitization of business across all fronts. From customer demands for increased digital interactions to completely remote workforces, the COVID-19 pandemic has given digital transformation a new sense of urgency as well as a mandate to prioritize digital readiness above all else. This shift has left organizations vulnerable to new risks, both because of a larger number of externally-facing critical systems and far fewer resources to implement security best practices. According to a global survey of executives, companies have accelerated the digitization of their customer and supply-chain interactions and their internal operations by three to four years. The share of digital or digitally-enabled products in their portfolios has accelerated by seven years.[2]

Digitized operations and products means business-critical applications and their data now reside in cloud-based, often public-facing systems and not within on-premises infrastructure. This has greatly increased the risk of exploitation. Organizations trying to keep up with the fast pace of acceleration may also be overlooking risks that potentially leave them susceptible to exploits, including the due diligence of security best practices.

50% OF RESPONDENTS TO FORRESTER'S JANUARY 2021 REPORT, THE KEY TO ENTERPRISE HYBRID CLOUD STRATEGY, ADMIT THAT UPGRADE DELAYS RESULT IN SECURITY VULNERABILITIES.[3]

Migrating business-critical applications to either public-cloud infrastructure or a hybrid, on-prem/cloud infrastructure increases enterprise risk. A recent survey of IT professionals found that 85% of firms surveyed stated that on-premises is a critical part of their hybrid cloud strategy, noting that cloud infrastructure cannot accommodate all workloads and performance environments.[4]

More concerning is that many of the same organizations surveyed also admitted they were delaying upgrades to their on-premises systems, and 50% responded that these delays resulted in security vulnerabilities.[5] There is an interesting dichotomy taking place—diminishing budgets and staffing yet increasing urgency to implement digitization projects faster. The COVID-19 pandemic accelerated the pace of digitizing everything across the business—from supply chains to customer interactions to workforce resources simultaneously. This has resulted in security best practices frequently falling by the wayside. Limited IT resources are being allocated to transform—not secure—organizations and their business-critical applications.

Yet there can be significant consequences when focusing on speed instead of security. Overlooked security vulnerabilities are often related to misconfigurations, user access, and user privileges and can be easily exploited. For example, a default setting that gives a user access to perform any function within a critical application can be overly applied to many users. Default credentials and passwords that may be reused can remain in place despite their ability to be easily exploited by an attacker to gain entry to a business-critical application. An exploited vulnerability in one of these on-premises systems could lead to a compromise for that unpatched critical system with far-reaching consequences.

[2] McKinsey Digital and Strategy & Corporate Finance Practices How COVID-19 has pushed companies over the technology tipping point—and transformed business forever October 2020

[3, 4, 5] A Forrester Consulting Thought Leadership Paper Commissioned By IBM January 2021 The Key To Enterprise Hybrid Cloud Strategy: An Annual Forrester Consulting Study Commissioned By IBM

[3]

Business-Critical Applications Are Increasingly at Risk From Bad Actors

Vulnerabilities in business-critical applications can be exploited by bad actors, and the risk to organizations has been growing over time. According to the United States Department of Homeland Security Cyber and Infrastructure Security Agency (CISA), there have been five US-CERT alerts about business-critical applications since 2016. US-CERT is the US Cyber Emergency Readiness Team and part of CISA. US-CERT is responsible for disseminating cyber-threat warning information as well as analyzing cyber threats and vulnerabilities. The organization collaborates with governmental agencies as well as the private sector. **Onapsis Research Labs** has been at the forefront of developing the research behind these alerts.

It is critical for organizations to understand the risks presented by these vulnerabilities. CISA has issued multiple US-CERT alerts for business-critical systems, noting that affected organizations could be subject to "theft of sensitive data, financial fraud, disruption of business-critical business processes, ransomware, and halt of all operations."[6] However, it is still challenging to implement effective vulnerability management processes even for organizations that are well aware of these risks. This is due to the decreased amount of time between a vulnerability being identified and disclosed and a bad actor taking advantage of the vulnerability.

Onapsis research has found that there can be as little as 24 hours between the disclosure of a vulnerability and observable scanning by attackers looking for vulnerable systems, and just 72 hours before a functional exploit is available.[7] Many organizations do not have security best practices, tools, or staffing levels in place to address vulnerabilities within this accelerated time frame. Bad actors are not only exploiting vulnerabilities in business-critical systems, they are doing so at a faster pace than ever before.

[6] https://us-cert.cisa.gov/ics/alerts

[7] Onapsis Threat Intelligence Report Active Cyberattacks on Mission-Critical SAP Applications

[4]

Existing Defense-in-Depth Strategy Deployments Insufficiently Protect the Business-Critical Application Layer

The concept of building a secure fortress around the "crown jewels" of business-critical applications and data is a longstanding security strategy. However, the traditional security layered stack approach of metaphorical high walls and a moat around the kingdom no longer offers sufficient protection. Although organizations should absolutely deploy a defense-in-depth strategy, a vulnerability can still be (and frequently is) found and exploited within any one of these layers of defense.

Ransomware (and malware), misconfigurations, or stolen credentials can be leveraged to breach any layer of security in front of the application layer, allowing a threat actor to move laterally to infiltrate business-critical applications. Some threat actors are even knowledgeable enough to attack the application layer directly.

60% OF IT AND SECURITY PRACTITIONERS CITE APPLICATION PROTECTION AS A TOP OBJECTIVE.[8]

A recent Onapsis Research Labs threat report found conclusive evidence that attackers who have sophisticated knowledge of business-critical applications target and exploit unsecured SAP applications.[9] This is achieved by using a variety of techniques, tools, and procedures. These attacks are not only brute-force attempts made directly against the application. Some attacks chain multiple vulnerabilities together in order to target specific applications and gain access to its operating system.

It's not that IT professionals don't realize how vulnerable they are. According to a recent Ponemon survey, 60% of them acknowledge that application protection is a top security objective.[10] However, nearly two-thirds of these same survey respondents admit that it is difficult to reduce the risks to critical applications because they cannot monitor and prevent attacks at the application layer.[11]

Identifying vulnerabilities across an IT landscape is a manual, laborious effort. This is why many, if not close to all, organizations deploy traditional vulnerability management solutions that scan for known threats and vulnerabilities. These solutions focus on a broad range of systems and applications, including network security systems, the layers of protection that surround business-critical applications, and data. Vulnerability management tools commonly perform scans and compile a list of highlighted vulnerabilities and recommendations for remediation, mitigation, or acceptance. Unfortunately, by design, they are designed to highlight issues across many systems and are ill-equipped to scan business-critical applications for vulnerabilities that may be used as attack vectors. These traditional solutions are ineffective at identifying a large number of application vulnerabilities such as misconfigurations, overprivileged roles, or unapplied patches. More critically, there's still the human element. Even if a vulnerability is found, the time to resolve it is long. The average time it takes to fix critical cybersecurity vulnerabilities is 205 days.[12]

IT TAKES AN AVERAGE OF 205 DAYS TO FIX CRITICAL CYBERSECURITY VULNERABILITIES.[13]

[9] Onapsis Threat Intelligence Report Active Cyberattacks on Mission-Critical SAP Applications

[8, 10, 11] Reducing Enterprise Application Security Risks: More Work Needs to Be Done Ponemon Institute Publication Date: February 2021

[12, 13] https://www.zdnet.com/article/average-time-to-fix-critical-cybersecurity-vulnerabilities-is-205-days-report/

[5]

Even the Best Teams Are Challenged to Do More With Less

Gartner predicts that nearly $4B of global security and risk management will be allocated to application security in 2021.[14] Regardless, budgets are finite and even with hiring budget, there is often a lack of qualified candidates.

Even an organization with a well-staffed team is challenged with limits on their time as they prioritize workloads. Complex security notes with multiple vulnerability patches and instructions and varying levels of severity are released on a monthly basis. This makes it extremely challenging especially for enterprises managing dozens of business-critical applications in production.

ACCORDING TO GARTNER, $4 BILLION WILL BE SPENT ON APPLICATION SECURITY GLOBALLY IN 2021.[15]

Managing all of these patching efforts is a time consuming process and an additional burden for the team. This can result in a rushed or sometimes complacent patch management process. Critical patches may be ignored or deprioritized (in relation to other jobs to be done). Additionally, there may be long backlogs and lead times until patches are actually implemented and verified. Patch management is only one part of mitigating risk for business-critical applications. Misconfigurations or overprivileged "all-access" roles are also viable threat vectors used to gain access. All of these leave enterprises vulnerable to attack.

Because business-critical applications are at the core of every organization, an exploitation of a vulnerability has significant consequences. Due to the valuable data these systems contain, there has been a rise in threat actors targeting their vulnerabilities. The accelerated pace of digital transformation and the rapid migration from on-premises to hybrid and cloud infrastructure have dramatically increased the risk to these systems. Yet despite the increased risk, these applications are often out-of-scope for traditional vulnerability management tools and security teams. They are typically managed by information technology professionals who are focused on development and uptime as opposed to security. This further compounds the complexity associated with protecting these applications from vulnerabilities.

[14, 15] https://www.securityweek.com/gartner-global-security-spending-will-reach-150-billion-2021

There Is A Better Way To Protect Your Business-Critical Applications.

Introducing **Onapsis Assess**. It provides focused and comprehensive vulnerability management enterprises require for their most business-critical applications such as SAP and Oracle. Onapsis Assess provides deep visibility into the entire business-critical application landscape, deep, automated assessments with detailed solutions and descriptions of associated risk and business impact. InfoSec and IT teams gain automated assessment and prioritization capabilities including step-by-step remediation instructions for simple and straightforward resolutions.

Onapsis Assess is one part of the Onapsis Platform, a comprehensive suite of security tools focused on business-critical applications. The Onapsis Platform is powered by the threat intelligence, research, and insights of the Onapsis Research Labs, the team responsible for the discovery and mitigation of more than 800 zero-day vulnerabilities in business-critical applications. We protect 20% of the Fortune 100s business-critical applications.

*Visit the **Onapsis homepage** to learn more about how **Onapsis Assess** can play an integral part of your new or existing vulnerability management programs, protecting your business-critical applications.*

ONAPSIS

Onapsis protects the mission-critical applications that run the global economy, from the core to the cloud. The Onapsis Platform uniquely delivers actionable insight, secure change, automated governance and continuous monitoring for critical systems—ERP, CRM, PLM, HCM, SCM and BI applications—from leading vendors such as SAP, Oracle, Salesforce and others, while keeping them protected and compliant. For more information, visit www.onapsis.com. Published 09/21.