(Sponsored Blog; partner-approved copy)

Three SAP Security Myths That Put Your Business at Risk

Separating fiction from reality can be the difference between securing your data and becoming the next cybercrime victim.

There's never been a better time to be a data-informed enterprise. With access to virtually limitless volumes of information—the world produces as much as 2.5 quintillion bytes of data daily, by some estimates—coming from hundreds or thousands of disparate sources. Data-hungry enterprise applications have more fuel for their critical operations than ever.

Innovative organizations across industries and geographies are migrating their core SAP systems to Google Cloud to help future-proof their businesses with greater insights, risk management, agile deployments, and enhanced sustainability.

In addition to minimal downtime for typical migrations, surveys show that companies using Google Cloud solutions such as BigQuery for SAP can reduce their time-to-insights by more than 60% while dramatically reducing their total cost of ownership to achieve a ROI of more than 300% over three years.

Public cloud platforms enable enterprises to capitalize on scalable insights enabled by artificial intelligence (AI) and machine learning (ML) applications, leveraging enterprise data with predictive analytics and deep learning to enhance their competitiveness as well as their organizational agility and resilience.

Yet, with greater opportunity comes much greater risk. Too many organizations are fooled into thinking that their SAP deployments and other mission-critical applications—complete with private, sensitive, or otherwise proprietary information — are automatically secured and protected the moment they're deployed in a popular, public cloud environment. That's despite an obvious and dramatic rise in cybercrime that's collectively expected to cost global organizations as much as $10.5 trillion USD annually.

Here are three SAP on Google Cloud security myths many IT and business leaders believe which could put their organizations (and all that sensitive information) at risk of falling into the wrong hands.

Myth 1: Cloud-native security is designed for SAP

Every public cloud platform has native security capabilities built in. Google Cloud, for example, features everything from firewalls and user protection tools to comprehensive identity and access management solutions.

But given SAP's expansive integration capabilities with other mission-critical applications that often rely on third-party security solutions, the risk of unauthorized access to sensitive systems and data across such a large attack surface significantly increases. Without the right strategies and solutions, attackers will simply enter the network environment and move every which way to find an open path to get what they want.

Enterprises using SAP applications must develop a comprehensive, SAP-centric security roadmap that incorporates essential security considerations from the initial cloud migration through full deployment. It's hard to predict the future but mapping the topology of your SAP infrastructure and broader IT environment is vital for protecting your interests now and in the future.

Myth 2: SAP application security is designed for the whole application lifecycle

Comprehensive platforms such as SAP have a lot of features and functionality, so it’s reasonable to assume that robust security is part of that package. But the reality is that no two organizations and no two SAP deployments on Google Cloud or other public cloud providers are alike.

Different business needs command different security parameters and, ultimately, the responsibility of cloud-related security — whether configuring cloud deployments directly or procuring and deploying third-party security solutions — falls to individual users and the organization as a whole.

As in Myth 1, a holistic security approach integrates various systems — the core SAP deployment and its various connection points to other mission-critical applications — into a unified framework designed to protect a range of attack surfaces throughout the numerous stages of digital infrastructure provisioning.

Myth 3: Conventional network perimeter security can repel attacks on SAP systems

From gateways and firewalls to intrusion detection systems and cloud access brokers (CASBs), perimeter security systems designed to keep would-be attackers out of your network have come a long way in the last decade.

But those advancements — adding next-gen capabilities like IPS inspection, SSH and SSL inspection, and AI-powered threat detection — still aren’t enough to secure SAP systems fully. Studies predict a new cyberattack will happen every 11 seconds in 2022, and it could take as long as nine months for security teams to identify and contain the damage.

That’s an exceedingly long time and a dangerous game to play with so much sensitive data and crucial operations housed in SAP systems. Instead, business and IT leaders must strategically plan protection for their core SAP systems, aiming to build a zero-trust environment based on the principle of least privilege (PoLP) and implementing advanced security practices across their operations — from resource onboarding through DevOps and all spaces in between.

Systematic, strategic frameworks for migrating SAP to Google Cloud

Migrating SAP applications to Google Cloud or other public clouds, by its very nature, introduces new and evolving cyber risks. Point solutions and conventional security approaches leave critical capabilities and sensitive information at an increased risk of unauthorized access and potentially catastrophic breaches.

Developing an effective cloud security strategy is essential for protecting extensible ERP applications, such as SAP applications with expansive (and growing) attack surfaces. Combining time-tested strategies for securing SAP on Google Cloud with advanced cloud and hybrid IT security solutions from Palo Alto Networks can help dramatically reduce your SAP security risk while unlocking the operational and strategic value of cloud-based systems.

Download our free white paper to learn the six best practices for successfully (and seamlessly) migrating SAP systems to Google Cloud and leave the mystery—and risk—of cloud security myths behind.

Download now (obtain link)

paloalto® NETWORKS

Palo Alto Networks is the world's cybersecurity leader. Our next-gen security solutions, expert services, and industry-leading threat intelligence empower organizations across every sector to transform with confidence. We envision a world where each day is safer than the one before.

asug

ASUG is the world's largest SAP user group. Originally founded by a group of visionary SAP customers in 1991, its mission is to help people and organizations get the most value from their investment in SAP technology. ASUG currently serves thousands of businesses via companywide memberships, connecting more than 130,000 professionals with networking and educational resources to help them master new challenges. Through in-person and virtual events, on-demand digital resources, and ongoing advocacy for its membership, ASUG helps SAP customers make more possible.