Securing SAP ERP Workloads in the Cloud

A Structured Approach to Securing SAP Migrations to Google Cloud

Table of Contents

Executive Summary

As cloud services continue to revolutionize business and expand the enterprise ecosystem, the threats to business operations have become increasingly complex. In the first half of 2021, critical industries suffered a spike in security incidents. According to Unit 42, the research group of Palo Alto Networks, retail, manufacturing, and government agencies saw an increase of security incidents by 402%, 230%, and 205%, respectively.[1] Organizations embarking on cloud transformations will need to confront challenges around exponential increases in data volume, the corresponding limited visibility and controls, and an expanded attack surface. Cybersecurity should be considered a core component of an SAP® migration to Google Cloud and an essential value driver that gives organizations the confidence to change at the speed of the business, while taking steps to put the appropriate controls and guardrails in place. Additionally, organizations should determine if they have the adequate cybersecurity talent to support the SAP ERP migration and define appropriate controls that balance security while supporting consistent business operations.

Leveraging leading cloud security practices, standards-based frameworks, and cutting-edge solution capabilities to secure an environment is a key aspect of migrating SAP workloads to Google Cloud. It can not only help enterprises address scalability and agility challenges but also enables them to leverage the artificial intelligence (AI)/machine learning (ML), Zero Trust Security and Data Analytics power of Google Cloud. Enterprises can be better positioned to gain greater insights, improve security, reduce risk, optimize IT costs, and innovate faster. Through this alliance brief, we will discuss Deloitte's approach for enterprises to secure SAP ERP workloads on Google Cloud by leaving traditional myths behind, adopting a security framework, and following the industry leading practices to enhance security capabilities supported by Google Cloud and Palo Alto Networks Prisma Cloud solutions.

Risk Posture: Why SAP Security in the Cloud Should Be a Priority

While cloud computing is maturing, cyber risk remains a top concern for boards and executives who recognize that moving to Cloud is a strategic driver and enabler of business performance and share-holder value. However, a cloud enabled transformation without the appropriate cyber integration will likely diminish these value drivers and could potentially result in financial and reputational losses, regulatory fines, and operational inefficiencies.

Organizations should invest time upfront to understand the key risks impacting SAP ERP migrations to Google Cloud and take a risk-centric approach to build security into their SAP ERP on Google Cloud environment from the ground up. Some common themes around risk posture in a cloud migration and insights are listed in figure 1.

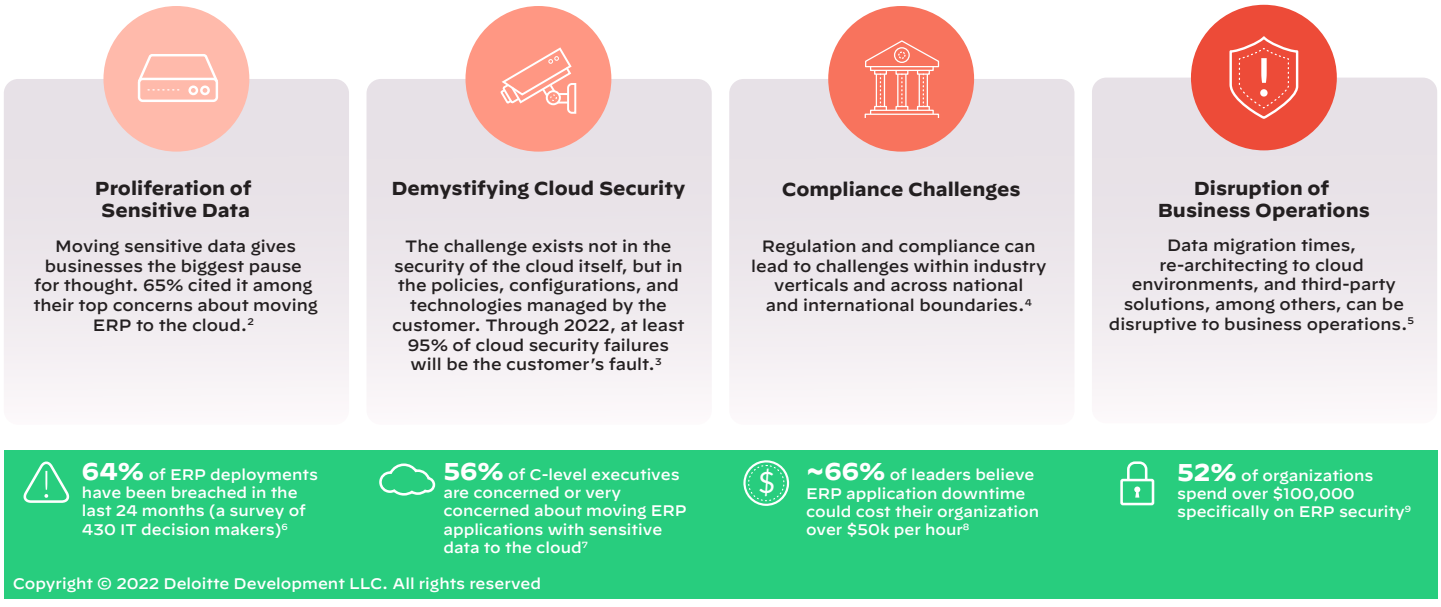

Figure 1: Common cloud migration risk posture themes and insights from analysts' surveys

Myths and Realities: Why SAP Security Is Often Overlooked

Based on our experiences, we have listed the top five common myths that highlight some of these popular, but erroneous ideas that may prevent leaders from prioritizing security investments for SAP systems in the cloud.

Table 1: Myths and Realities About Securing SAP Systems in the Cloud

#	Myth	Reality
Myth 1	The cloud shared responsibility model addresses SAP security in the public cloud.	"Security of the Cloud" is the cloud service provider's (CSP) responsibility while "Security in the Cloud" is the responsibility of the enterprise. Per Google Cloud, SAP on Google Cloud is delivered using the Infrastructure as a Service (IaaS) cloud model, which means security protections are built into the service by Google Cloud at the physical data center. However, for areas above the Google Cloud infrastructure, customers need to ensure their enterprise security controls are implemented. As an example, data security within the SAP ERP application is the customer's responsibility. Customers should plan and design access controls for securing access to sensitive data within the SAP ERP-enabled business processes running inside the application.
Myth 2	The cloud has built-in security solutions for SAP workloads.	It is true that Google Cloud has security products and capabilities that make cloud migrations more secure; however other third-party solutions are also being used that may have security gaps. The cloud provider's underlying infrastructure runs on port-based protocols like any other on-premises infrastructure which may be exposed to infrastructure related security risks. Without the appropriate protection, attackers have the ability to move laterally until they accomplish their attack.
Myth 3	Compliance and regulatory requirements are already met upon migrating SAP to Google Cloud.	Google Cloud's infrastructure and platform are compliant with applicable compliance and regulatory requirements. However, it does not imply that the enterprise SAP workloads running on them are also compliant. Enterprises need to carefully review the applicable regulations and evaluate the necessary controls and processes to comply with regulations. The collaboration between Google Cloud, Deloitte, and Palo Alto Networks provides risk-based framework and security solutions that can help clients facilitate compliance and be better positioned to meet regulatory requirements, for example: PCI DSS (Payment Card Industry Data Security Standard), SOC 2 (System and Organizations Control v2).
Myth 4	SAP application security is built-in for application lifecycle across application onboarding, development, build, and runtime/ operate.	This is a common misunderstanding. Security inside the cloud is the organization's responsibility, and a cybersecurity framework and architecture are must-haves to identify, design, and implement security solutions across the application development and cloud provisioning lifecycle (onboarding, development, build, runtime/operate) and in protecting against insider threats. Deloitte's demonstrated methodology, tools, and accelerators help enable a "security by design" approach and implementation through a defense-in-depth approach.
Myth 5	Network perimeter controls can prevent external attackers accessing SAP systems. Additional considerations on network perimeter controls are not required.	Firewalls, Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS), and Anti-Virus (AV) solutions are limited in analyzing SAP traffic or payload data. Businesses in the current hybrid work environment are enabled through a porous network perimeter which must be effectively secured by implementing a Zero Trust architecture. Google Cloud's BeyondCorp™ enterprise security solution enables simple and secure access to applications hosted on prem-ise and in the cloud without using remote access VPN. Additionally, the network access controls for core SAP systems should be planned and implemented following Principle of Least Privilege (PLP) using Palo Alto Networks Virtual Cloud Next-Generation Firewall (NGFW) to provide segmentation between SAP Internet Enabled VPC and Trust VPC, as well as Google Cloud IDS to provide visibility inside VPCs.

Road Ahead: SAP on Google Cloud Security Leading Practices

This section discusses some leading practices in cloud security, compliance, governance processes in a hybrid cloud environment, secure access service edge (SASE), and secure DevOps to help organizations improve the overall security and resiliency of their SAP on Google Cloud transformations. Looking at risks broadly by evaluating global threats, understanding the business context, regulatory, privacy and technology requirements, below are some leading practices organizations and technology leaders implement as they deploy SAP workloads on Google Cloud (see figure 2).

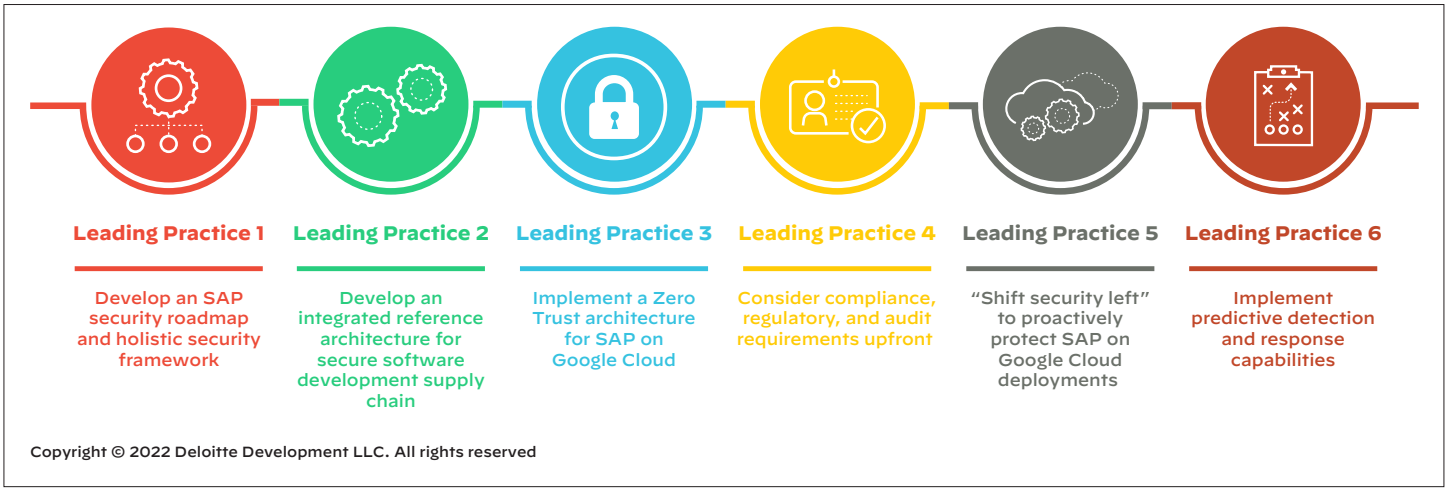

Figure 2: Suggested leading practices for deploying SAP on Google Cloud

Leading Practice 1: Develop an SAP Security Roadmap and Holistic Security Framework

Security is often not considered until after cloud migration is underway. Deloitte recommends organizations take a "shift security left" approach by integrating essential security considerations upfront as part of the cloud migration program planning process and at each step along the implementation roadmap to effectively mitigate the security risks and make security an enabler for the SAP on Cloud transformation. Figure 3 shows the recommended path that enterprises can consider to safeguard SAP workloads in the cloud and be proactive in defending against adverse cyber incidents.

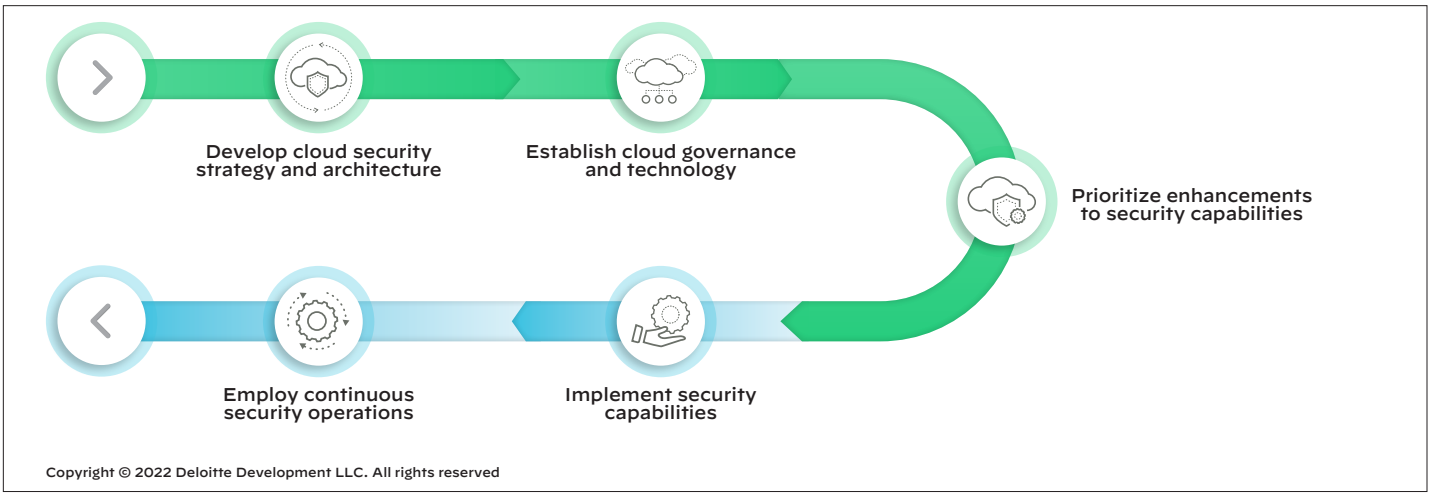

Figure 3: Path to safeguard SAP in the cloud and proactively defend against cyber incidents

A critical component to effectively implementing a secured SAP on Cloud transformation is adopting a security framework. An SAP on Google Cloud framework provides a blueprint and implementation roadmap to align the SAP on Google Cloud applications to the current enterprise security environment. It serves as the guide for SAP and technology leaders to drive the SAP transformation securely throughout the implementation, as well as during ongoing cloud operations.

Deloitte's SAP on Cloud security framework is designed to help organizations implement a "Security by Design" foundation. The framework leverages the leading practices of cloud security, along with regulatory and privacy considerations, and is designed to enforce an effective Zero Trust architecture and a set of integrated security capabilities to secure business transformations enabled through SAP on Google Cloud. Additionally, it helps organizations assess the security and compliance capabilities offered through Google Cloud and Palo Alto Networks to develop a tailored blueprint and an implementation roadmap to align SAP workloads on Google Cloud applications to their enterprise security environment (see figure 4).

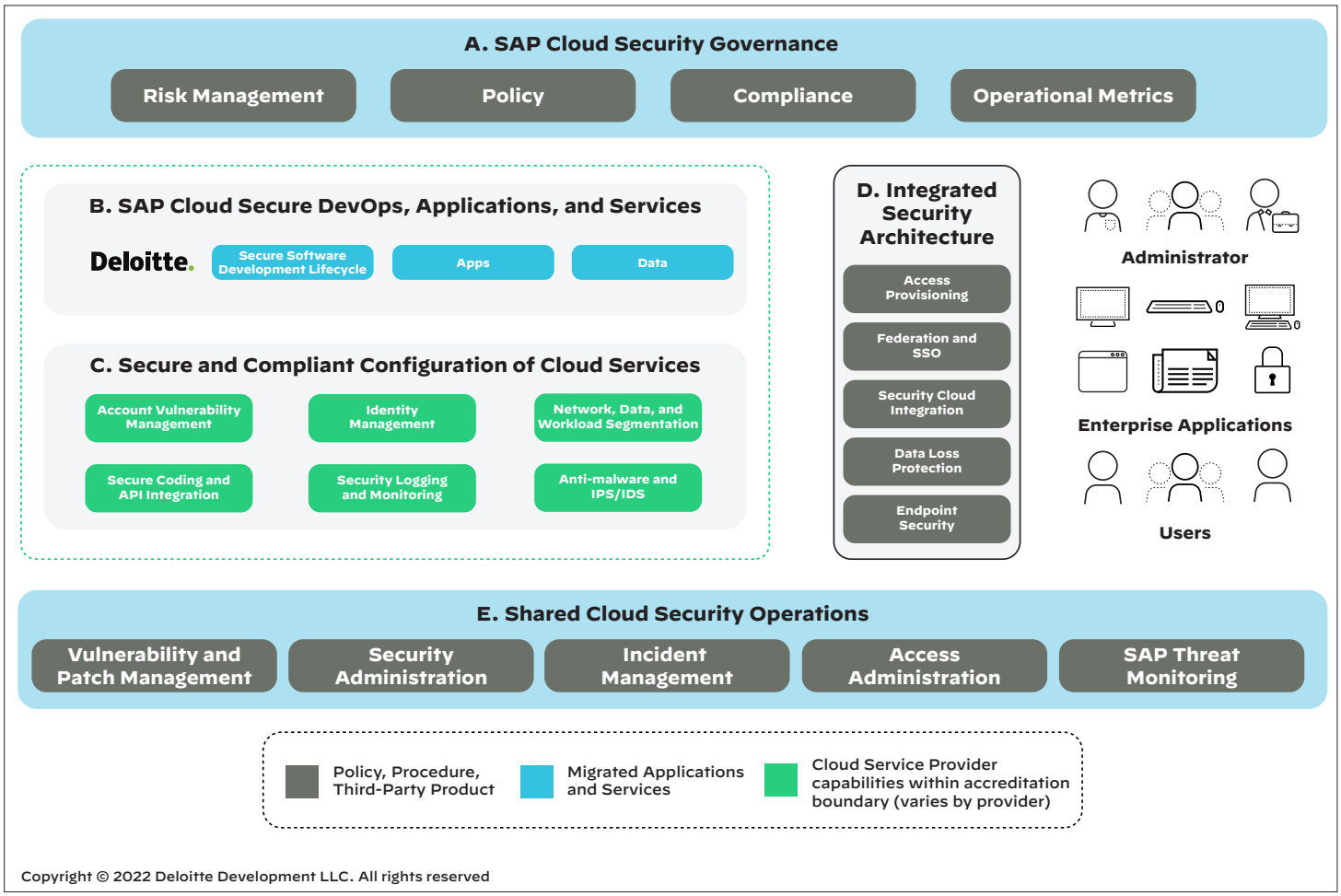

Figure 4: Blueprint and roadmap to align SAP on Google Cloud to the enterprise security environment

Core components of the SAP on Google Cloud Security Framework:

A: **SAP Cloud Security Governance**: Organizations migrating SAP workloads to Google Cloud need a security governance process that spans across the cloud platform, enterprise IT environment, and operations. An organization's current governance model needs to be evaluated against the shared responsibility model introduced by the cloud platform and subsequently enhanced to enforce the necessary governance and operational processes across the extended enterprise. Specifically, information security policies and procedures, data privacy and protection, third-party risk management, identification of cloud controls (preventative, detective, corrective), and establishment of a cloud security architecture are needed to support an effective governance model. A critical step toward establishing an effective cloud governance program is to align across security, information technology, compliance, and business process stakeholders to develop a tailored change management program to support the ongoing operational processes.

B: **SAP Cloud Secure DevOps, Applications, and Services**: Embedding cyber upfront in the development lifecycle is critical to improving the overall security and resiliency of the cloud environment. Rapid integration between current and new systems can be achieved with an effective DevSecOps process that identifies flaws during design, enables developers to work at the speed of DevOps, thereby increasing agility and velocity to improve time to market and helps decrease time to operationalize new business models. The benefit is that the effort and cost of remediation is typically much lower. Providing self-service security tools and assets to developers complements the deployment of applications and services without security acting as a bottleneck for cloud adoption. Reducing manual processes and using automation templates for application deployment and infrastructure provisioning can accelerate DevSecOps adoption.

C: **Secure and Compliant Configuration of Cloud Services**: Organizations should assess Google Cloud's native capabilities against their data security and compliance requirements to define a baseline set of security configurations. This becomes a key input to developing standardized and repeatable processes, as well as rapid and secured application onboarding to the cloud. This includes implementing a secure landing zone and cloud security posture management solution to improve security and resiliency of the SAP on Google Cloud environment.

D: **Integrated Security Architecture**: Developing a security architecture focused on securely enabling the enterprise to cloud integrations is critical for a secured SAP on Google Cloud migration. Deloitte's SAP on Cloud security framework provides organizations with baseline cloud security architecture built on Google Cloud's BeyondCorp™ Zero Trust solution to accelerate the migration of SAP on Cloud environments. Additionally, it provides a pre-configured library of tools and accelerators to extend the organization's current controls by evaluating and adapting Google Cloud and Palo Alto Networks' security capabilities as necessary.

E: **Shared Cloud Security Operations**: While Google Cloud is responsible for the ongoing operations of the underlying cloud infrastructure, organizations need to focus on implementing effective security operations for their SAP workloads running in the Google Cloud environment. Deloitte's Cloud Managed Services (CMS) provides an end-to-end solution to securely design, build, and operate SAP on Google Cloud environments, so organizations can focus on strategic business objectives. Deloitte's CMS offering includes cloud services across seven critical areas: Infrastructure Management, Service Management, Application Management, Automation and DevOps, Cyber Security, Risk and Compliance, and Optimization services to support secured and efficient operations.

Leading Practice 2: Develop an Integrated Reference Architecture for Secure Software Development Supply Chain

As organizations migrate SAP to Google Cloud, they may start to move non-production SAP workload, such as training or sandboxing first, while keeping the higher environments like quality and production within the on-premises data centers. Developing an integrated reference architecture thus becomes a critical component to secure the hybrid cloud environment and protect the organization's crown jewels.

The following diagram illustrates a typical SAP deployment in a hybrid environment and how an integrated set of Palo Alto Networks security products, along with Google Cloud security features, could be leveraged to protect the SAP deployment, as well as provide secure access to remote users in offices or at home in the hybrid cloud environment (see figure 5).

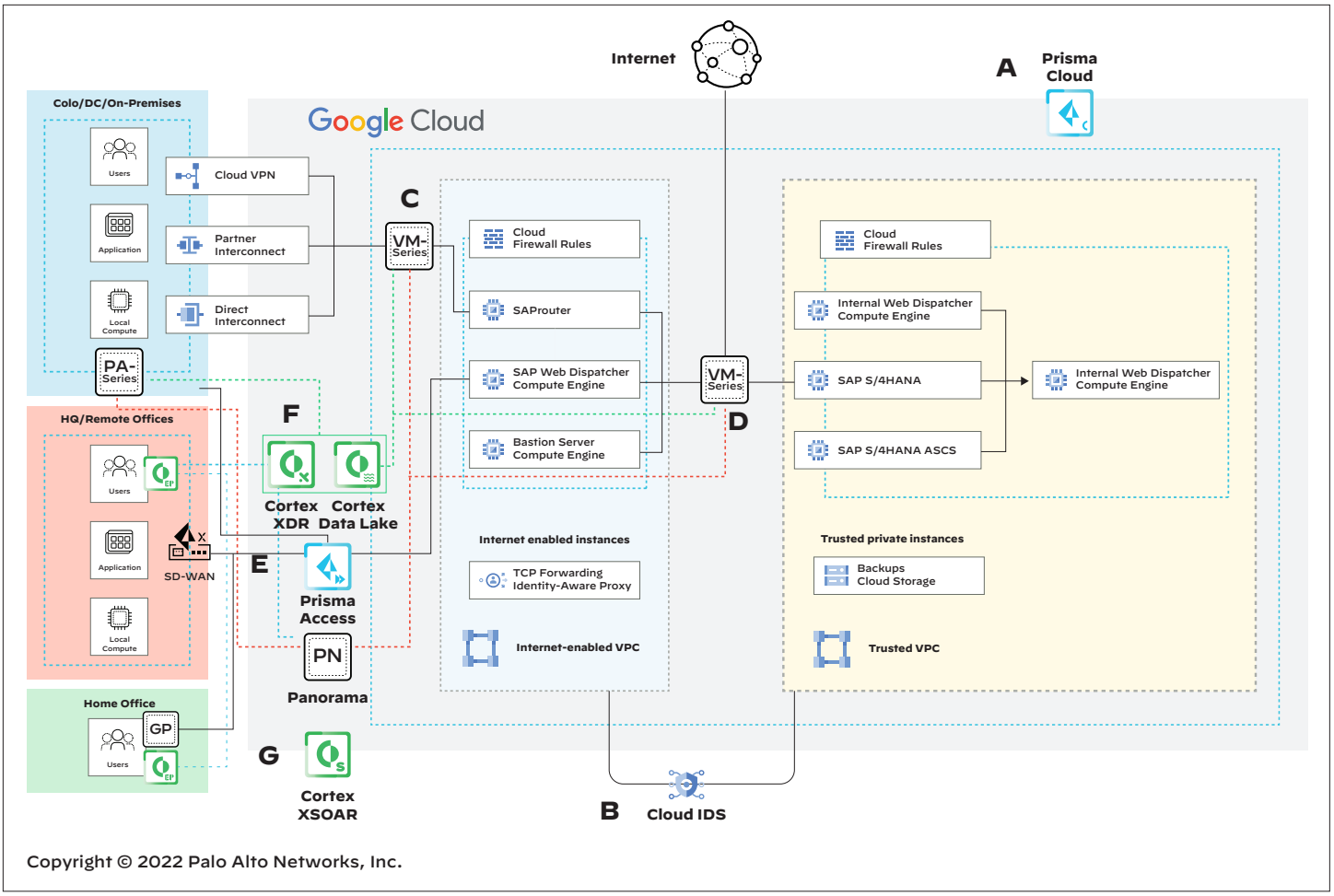

Figure 5: Hybrid cloud SAP deployment leveraging integrated Palo Alto Networks and Google Cloud security

Key security capabilities enabled through the architecture include:

A: Prisma Cloud simplifies cloud security with a single, unified platform using a single agent to secure both hybrid and multi clouds, across all leading use cases. Prisma Cloud CSPM ships with over 700 policies built in and supports custom standards. Prisma Cloud CWPP delivers full lifecycle protection across public and private clouds as well as on-premises environments.

B: Google Cloud IDS delivers cloud-native, easy-to-deploy, managed network threat detection. Cloud IDS provides visibility to the threats inside the SAP internet-enabled VPC and trusted VPC. Cloud IDS is built with Palo Alto Networks' threat detection technologies, backed by Palo Alto Networks' threat analysis engine and security research teams that identify new threat signatures and detection mechanisms.

C: VM-Series NGFWs are deployed as gateways to terminate the IPsec tunnel from on-premises data centers into the Google Cloud network. VM-Series NGFWs can also be deployed to layer application control and threat prevention policies on the IPsec VPN tunnel or Google Cloud Interconnect.

D: The VM-Series NGFW protects inbound and outbound traffic for all internet-facing applications that are running in the SAP environment and prevents data exfiltration from the SAP environment. It is recommended to deploy SAProuter, SAP Web Dispatcher, or Bastion server in an internet-enabled VPC and SAP S/4HANA®, SAP S/4HANA ASCS, and the SAP HANA® database in the trusted VPC. The VM-Series NGFW provides a layer of segmentation between the internet-enabled VPC and the trusted VPC.

E: Prisma Access provides the ability for users to access enterprise applications and SAP deployments from headquarters, remote offices, or their homes while enabling a Zero Trust architecture without backhauling users to on-premises data centers. The Prisma SD-WAN solution optimizes network access and performance for branch offices. Prisma Access and Prisma SD-WAN provide a full stack of Zero Trust SASE solutions for mobile users, headquarters, remote offices, and home offices to securely access SAP applications and deployment in Google Cloud, as well as on-premises data

centers. Prisma Access can be added to Google Cloud BeyondCorp Context-Aware Access policy for additional security control to Google Cloud resources and SaaS applications, such as Workspace or third-party applications. The access would only be allowed if the traffic went through Prisma Access.

F: Cortex XDR agents are deployed to SAP users' devices to safeguard endpoints from malware, exploits, and fileless attacks with AI-driven local analysis and behavior-based protection. Organizations can stop threats with a single cloud-delivered agent for endpoint protection, detection, and response. Cortex XDR can be added to Google Cloud BeyondCorp Context-Aware Access policy for additional security control to Google Cloud resources and SaaS applications such as Workspace or third-party applications. The access would only be allowed if the user's endpoint risk context met the Cortex XDR endpoint verification policies.

G: Cortex® XSOAR™ is a security orchestration, automation, and response (SOAR) platform that helps organizations coordinate and accelerate incident response across cloud environments. Cortex XSOAR can help provide the removal of false positives and reduce alerts that call for human intervention. Cortex XSOAR automation helps reduce incident response in SAP deployments in a hybrid environment. Cortex XSOAR integrates with the entire Palo Alto Networks portfolio, as well as Google Cloud IDS, Pub/Sub, Compute Engine, VPC Firewall Rules, Google Cloud Security Command Center, and many other Google Cloud services.

Leading Practice 3: Implement a Zero Trust Architecture for SAP on Google Cloud

The global pandemic has pushed working remotely to a new level. A recent survey indicates that 65% of respondents said they want to remain full-time remote workers after the pandemic.[10] Additionally, organizations around the world are rapidly migrating applications to the cloud. Traditional security approaches were not designed to address risks associated with an ever-expanding network perimeter (see figure 6).

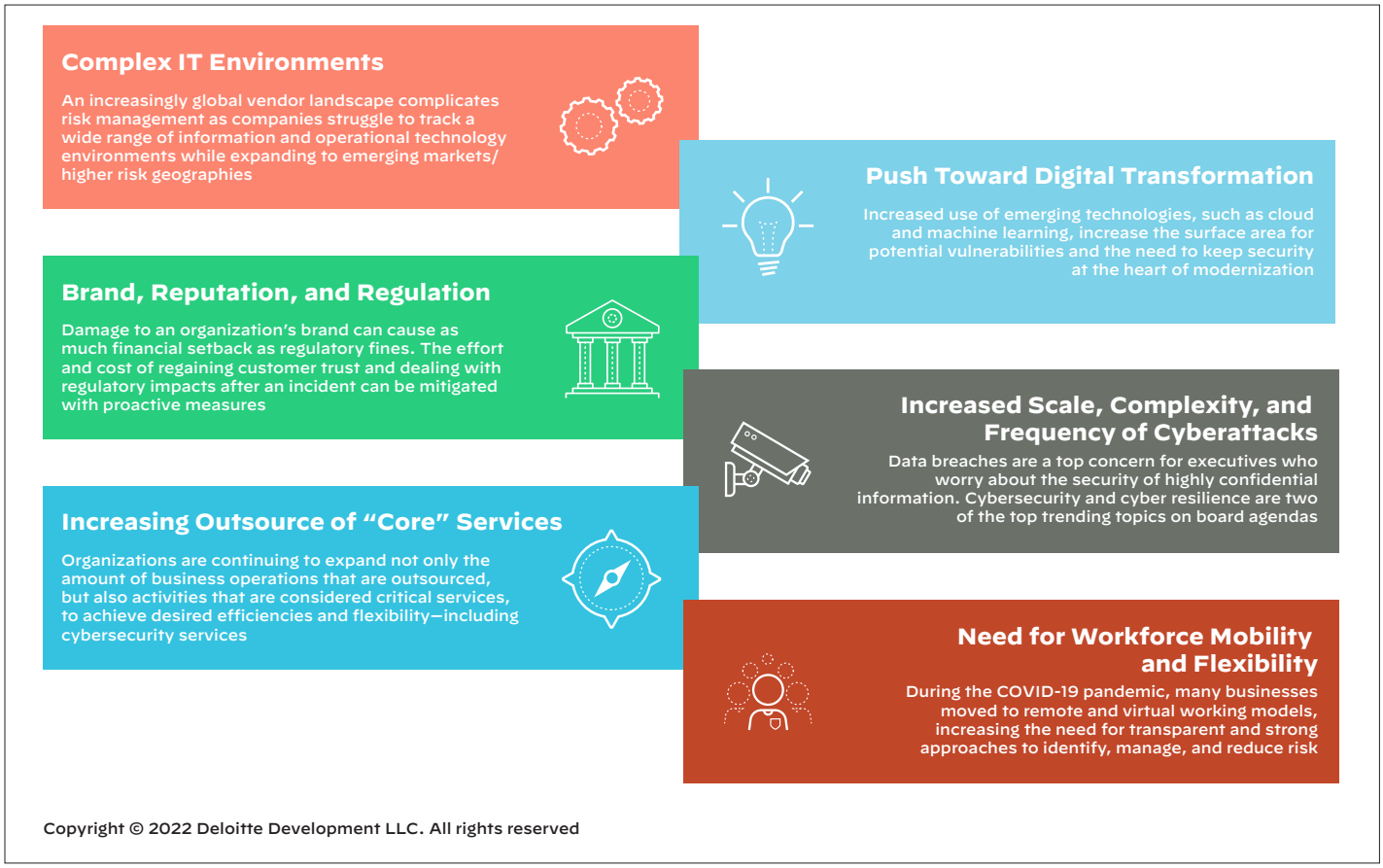

Figure 6: Limitations of traditional security approaches in an ever-expanding network perimeter

Zero Trust is a conceptual framework that helps organizations secure the ubiquitous nature of modern enterprise environments. At its core, Zero Trust commits to a risk-based approach to enforce 'least privilege' across users, networks, data, devices, and workloads. Deloitte believes "the need for Zero Trust is NOW."[11] Google Cloud's BeyondCorp enterprise security solution helps enable an efficient Zero Trust architecture and capabilities that are required to enable a hybrid cloud environment. Zero Trust is a concept that should be supported by new age technical capabilities, which is where SASE plays a strong role.

SASE is the technology that supports the "new world" architecture, combining both networking and security capabilities delivered through cloud-based edge computing. SASE enables secure access to enterprise resources at scale based on content and context, regardless of the location of the user or requested resource. Leading practices for using SASE to access a hybrid application and SAP infrastructure include:

- An enterprise-wide Zero Trust security approach and a consistent security model across the company's data centers, headquarters, remote offices, employees' homes, as well as mobile users, should be built.
- Access for users to SAP applications from anywhere and on any device. The security protections must be consistent across all connecting mechanisms.
- Security protection that is applied to an employee, contractor, or third party using a managed device or unmanaged device.
- Access control unified to all SAP applications and secured against all threats, not just web-based threats, including data loss prevention, device security and segmentation, DNS attack prevention, intrusion prevention system, zero-day malware analysis/sandboxing, and ML-driven web security, which results in reducing the risk of a data breach.
- Ability to provide exceptional user experience and a massively scalable network with ultra-low latency backed by an industry-leading SLA regardless of where the applications are hosted.

Prisma Access and Prisma SD-WAN provide a full stack of Zero Trust SASE solutions for SAP applications and deployment in Google Cloud, as well as on-premises data centers, mobile users, headquarters, remote offices, and home offices.

Leading Practice 4: Consider Compliance, Regulatory, and Audit Requirements Upfront

With the substantial increase in cyberattacks within the United States, compliance and regulatory requirements have become more critical to be adhered to and monitored by organizations Many organizations believe they are compliant with privacy regulations—however, an estimated 47% of executives are unsure which information security and privacy regulations or compliance standards apply to their organization.[10]

Recently, an executive order on improving the nation's cybersecurity was issued. Choosing a security solution that provides a strict security posture to match these compliance and regulatory requirements, not to mention other requirements set by PCI DSS, CIS, HIPAA, SOC 2 (System and Organizations Control v2), and others, is greater than ever.

SAP applications often contain data elements subject to a variety of regulations. Assessing the compliance and regulatory risks becomes even more important in the hybrid cloud environment given the shared responsibility model between the enterprise and the cloud service provider. As such, effective cloud security requires complete visibility into every deployed resource, as well as confidence in their configuration and compliance status. Organizations should invest time upfront to clearly identify and document the applicable compliance and regulatory requirements as part of the solution design and leverage the underlying cloud platform controls to implement the necessary security controls. Additionally, organizations should consider enabling continuous monitoring of cloud compliance posture and one-click reporting on compliance across all major compliance standards.

The migration of SAP deployments to Google Cloud allows companies to satisfy these compliance and regulatory requirements by utilizing the native security features within Google Cloud, as well as superior integration with Palo Alto Networks security solutions:

- Google Cloud's native security solutions, such as Google Cloud IDS, in conjunction with Palo Alto Networks VM-Series firewalls and Prisma Cloud align detection, remediation, and automation for various regulated environments.
- Prisma Access provides out of the box reporting to support leading compliance monitoring requirements. Additionally, built-in data protection capabilities ensure all sensitive data and PII (Personally Identifiable Information) are protected from both external and internal threats.

- Prisma Cloud enables organizations to view, assess, report, monitor, and review cloud infrastructure health and compliance posture. Users can also create reports that contain summary and detailed findings of security and compliance risks in cloud environments. Prisma Cloud keeps Google Cloud environments compliant with industry-leading security standards and controls, such as CSA, CIS, NIST CSF, HIPAA, HITRUST, and ISO 27001.

Leading Practice 5: "Shift Security Left" to Proactively Protect SAP on Google Cloud Deployments

Most modern organizations realize the value of shifting security left in the development lifecycle, especially as applications are becoming collections of microservices and functions, resulting in everything being defined as code. Developers can use a vast array of tools to build and deploy cloud-native applications. Operationalizing security controls that work seamlessly across these tools remains a challenge.

Shift security left involves integrating security at the earliest possible point in the development process, enabling developers to work at the speed of DevOps, thus increasing agility and velocity to improve time to market and decrease time to operationalize new business models. This strategy applies to SAP applications' full lifecycle and using infrastructure as code (IaC) to deploy SAP infrastructure in the cloud. The leading practice is to apply security control continuously throughout the development lifecycle: build, deploy, and runtime.

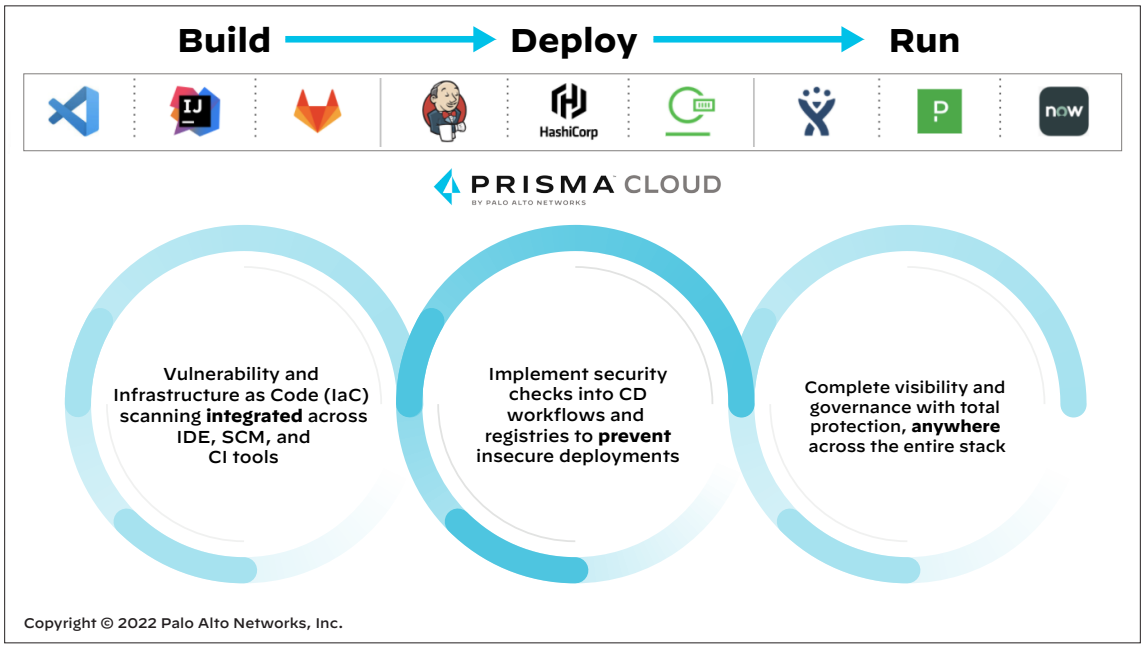

Figure 7: Applying security control continuously throughout the development lifecycle

During the build phase, developers scan virtual machine images, container images, Pivotal Application Service (PAS) droplets, and serverless functions for vulnerabilities as well as any unsecured configurations that are using native security plugins. The scan includes infrastructure-as-code (IaC) templates to find unsecure configurations used with Terraform®, AWS CloudFormation®, Kubernetes® manifests, and similar technologies. It is important to ensure any host operating systems, container images, PAS droplets, and serverless functions are free from new vulnerabilities that may have been discovered after build.

DevOps scans any container registry, serverless repository; enforces trusted code sources to ensure code is free of security issues when it is time to deploy. With vulnerable code unable to reach production, the overall attack surface is greatly reduced. The security team continuously monitors the runtime environment for newly discovered vulnerabilities and deviations of the application's behavior. The risk prioritization must be provided in any running environment, so security teams can continuously monitor all their cloud-native infrastructure and apps and quickly prioritize remediation efforts.

Leading Practice 6: Implement Predictive Detection and Response Capabilities

SAP workloads deployed on cloud infrastructure inherently create an increased attack surface with petabytes of log data from various sources. Organizations should consider a predictive, modern, and integrated analytics approach to reduce the complexity of detection and response activities. Disconnected or not well-integrated point security solutions could lead to a flood of alerts in the Security Operation Center (SOC), resulting in inefficient event monitoring (see figure 8).

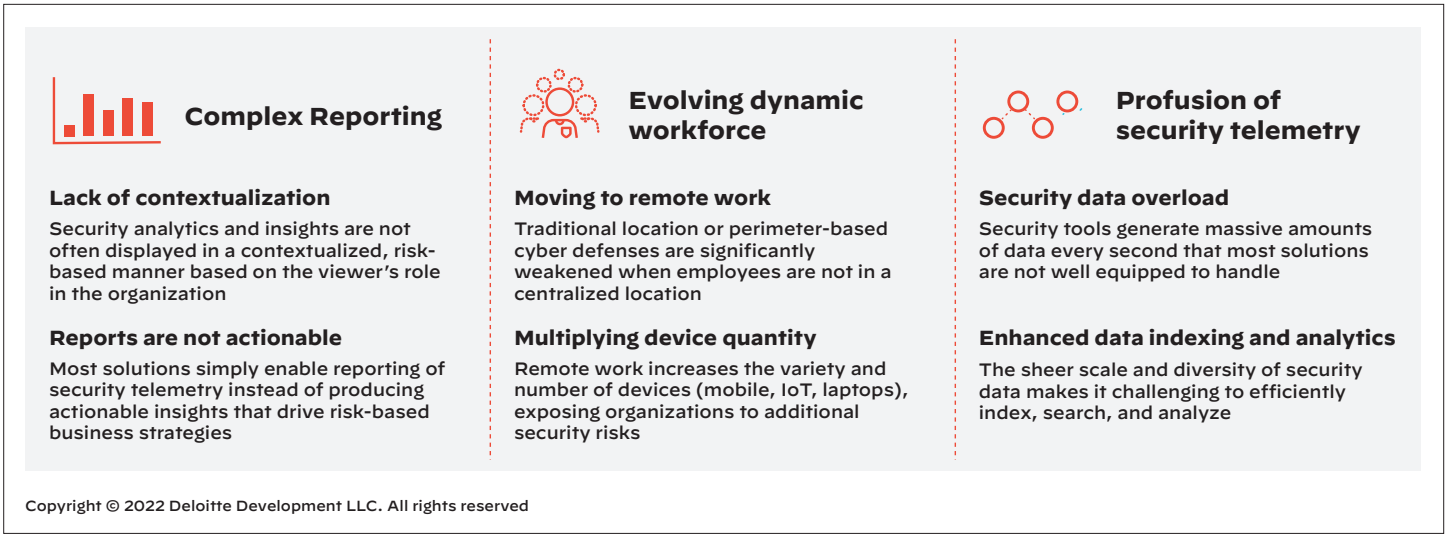

Figure 8: SOC security alert inundation from point solutions

An integrated platform enables automation for incident response. A well-designed automated incident response system takes the majority of the alerts out of Security Operation Center analysts' hands, so they can focus on the most critical events that require human intervention.

Deloitte's Predictive Analytics for Cyber in Enterprises (PACE™) was designed to enable effective security incident detection and response capabilities through predictive analytics. PACE is a cloud-native analytics solution built on Google Cloud and Chronicle's threat hunting and big data platforms—a powerful solution that combines Chronicle, BigQuery ML, and Looker™ in a single pane of glass, with integration to Google Cloud's BeyondCorp for frictionless Zero Trust based access management PACE provides faster, simpler, persona-driven decision making that brings visibility into the security posture of the enterprise (see figure 9).

PACE also integrates with Cortex XSOAR to provide push and alert-based API integrations generated using statistical inference and the predictive analytics suite of AI/ML. Security alerts, including the context of the incident, related alerting, rule detections, and security results are sent to endpoints and the Cortex XSOAR incident management system along with the enriched log and files associated with the detection. These detections can trigger a specified playbook or be integrated into an incident using Cortex XSOAR logic. Cortex XSOAR automation helps reduce incident response in SAP deployments in a hybrid environment.

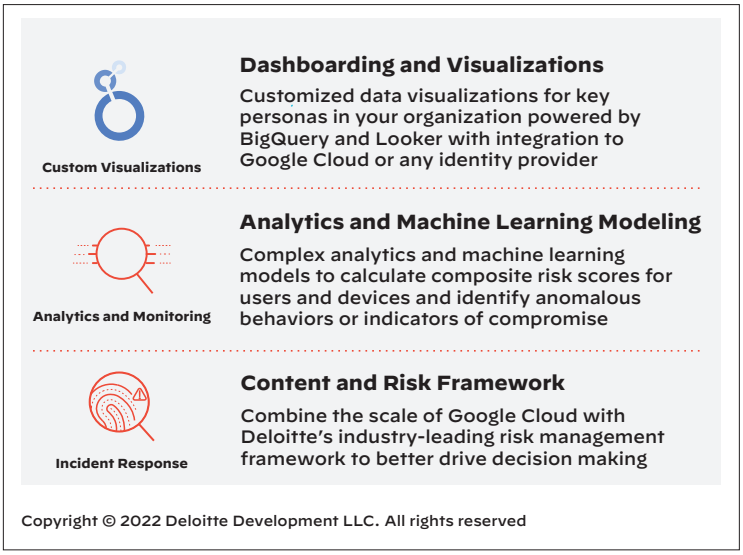

Figure 9: PACE IR capabilities

Conclusion: Taking the Next Step Toward SAP on Cloud Migration

Migrating SAP applications to the Cloud inherently introduces cyber risks that need to be effectively managed to realize the full business benefits of a cloud transformation. By adopting a "shift security left" mindset, organizations can infuse cyber into the core DNA of a cloud transformation and use cyber as an enabler for their strategic objectives. With an increased attack surface associated with the cloud environment, anytime there is a new security risk highlighted, a race occurs to deploy new tools and technologies; as such, taking a holistic cloud security approach is pivotal to implementing an integrated set of scalable and adaptable security capabilities. Developing an effective cloud security strategy is important especially when it's for large ERP applications like SAP.

The SAP on Google Cloud security leading practices outlined in this document are intended to guide organizations to implement a secured cloud transformation. In summary, here are the key takeaways for securing SAP workloads on Google Cloud:

- Take a business risk-centric approach to assess the security threat exposure throughout the hybrid cloud environment.
- Adopt a Zero Trust framework to enable the necessary SAP on Google Cloud security capabilities.
- Leverage the native capabilities offered through Google Cloud and Palo Alto Networks security products to secure the SAP cloud workloads.
- Define the right security governance and compliance processes throughout the hybrid environment.
- Implement predictive analytics and integrated solutions for threat detection and response to support ongoing operations.

Protecting SAP business critical infrastructure and systems is a complex undertaking, especially when migrating from traditional data centers, thereby creating the opportunity for blind spots in the security posture. Deloitte's SAP security framework, Palo Alto Networks' solutions, and Google Cloud's native security services are well-positioned to support your secure SAP on Google Cloud transformations.

Organization leaders who want to move strategically and secure their SAP investment in the cloud can contact us to get that conversation started.

Authors

Palo Alto Networks

- Mason Yan, Director of Technical Engagement

Deloitte & Touche LLP

- Meer Hussain, Risk & Financial Advisory Managing Director, Deloitte & Touche LLP
- Arun Perinkolam, Google Cloud Risk & Financial Advisory Lead Alliance Principal, Deloitte & Touche LLP
- Jane Chung, Managing Director, Deloitte & Touche LLP
- Pradeep Sandhu, Risk & Financial Advisory Senior Manager, Deloitte & Touche LLP
- Aparna Kotamarthi, Risk & Financial Advisory Manager, Deloitte & Touche LLP

Google Cloud

- Joshua Haslett, Principal/SME Google Cloud

Reference

1. Highlights from the *Unit 42 Cloud Threat Report, 1H 2021*, Unit 42, Palo Alto Networks, April 2021, https://www.paloaltonetworks.com/prisma/unit42-cloud-threat-research-1h21.
2. Ibid.
3. Ibid.
4. Ibid.
5. Ibid.
6. *Enterprise Resource Planning and Cloud Adoption*, Cloud Security Alliance, January 11, 2019, https://cloudsecurityalliance.org/artifacts/enterprise-resource-planning-and-cloud-adoption/.
7. "Independent Market Survey Reveals 64% of ERP Deployments Have Been Breached in the Last 24 Months," Bloomberg, October 2019, https://www.bloomberg.com/press-releases/2019-10-02/independent-market-survey-reveals-64-of-erp-deployments-have-been-breached-in-the-last-24-months.

8. Ibid.
9. Ibid.
10. Rachel Pelta, "FlexJobs Survey Finds Employees Want Remote Work Post-Pandemic," FlexJobs, April 5, 2021.
11. "The need for Zero Trust is NOW," Deloitte, August 2020, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-rfa-zero-trust-sales-sheet-2021.pdf.

Glossary of Terms	
Prisma Cloud by Palo Alto Networks	Prisma® Cloud simplifies cloud security with a single, unified platform using a single agent to secure both hybrid and multicloud environments, across all leading use cases. Prisma Cloud protects your public cloud infrastructure, including SAP on Google Cloud. With Prisma Cloud, you gain real-time visibility into your overall cloud security posture, and it ships with over 700 policies built in so you can quickly achieve compliance and improve security across multicloud environments. Prisma Access provides compliance frameworks for every major standard, supports custom standards, and can even generate audit-ready reports in a single click. Built-in data protection capabilities ensure all sensitive data and PII are protected from both external and internal threats. Prisma Cloud delivers cloud workload protection capabilities that secure any workload or application while integrating the lifecycle and protecting running workloads and applications on public and private clouds. Prisma Cloud integrates security enforcement capabilities into any CI/CD workflow by scanning hosts, container images, and functions as well as infrastructure-as-code (IaC) templates with results in native tooling and central dashboards.
Machine Learning Powered Next-Generation Firewall by Palo Alto Networks	The PA-Series ML-Powered Next-Generation Firewall (NGFW) provides network security to the infrastructure at on-premises data centers while the VM-Series virtual NGFW protects Google Cloud networks. Pairing with PA-Series NGFWs at on-premises data centers, the VM-Series may be deployed as gateways to terminate the IPsec tunnel from on-premises data centers into the Google Cloud network. Also available is the option to layer application control and Threat Prevention policies on the IPsec VPN tunnel or Google Cloud Interconnect. The VM-Series Virtual Next-Generation Firewall protects inbound and outbound traffic for all internet-facing applications that are running in the SAP environment by leveraging its advanced threat inspection. Additionally, the VM-Series protects against data exfiltration from the SAP environment. The VM-Series NGFW also provides a layer of segmentation between the internet-enabled VPC and the trusted VPC within Google Cloud. ML-Powered NGFWs embed machine learning in the core of the firewall to provide inline signatureless attack prevention. The firewall leverages cloud-based ML processes to push zero-delay signatures and instructions back to the NGFW, resulting in better security protection. ML-Powered NGFWs offer a single platform with all services natively integrated and simplified management, offering a truly comprehensive security solution. With a single-pass architecture, there is no performance degradation for enabling new services. IoT Security, DLP, DNS Security, and SaaS security are all available as Cloud-Delivered Security Services.
Google Cloud IDS	Cloud IDS delivers a cloud-native, easy to deploy, managed network threat detection. It scales north to south to inspect all of your traffic based on your organization's needs. Cloud IDS is built with Palo Alto Networks threat detection technologies, backed by their threat analysis engine and security research teams that identify new threat signatures and detection mechanisms. Cloud IDS provides visibility to the threats inside the SAP internet-enabled VPC and trusted VPC.
Prisma Access and Prisma SD-WAN by Palo Alto Networks	Prisma Access provides the ability for users to access enterprise applications and SAP deployments from headquarters, remote offices, or their homes while enabling a Zero Trust architecture without backhauling users to on-premises data centers. The use of GlobalProtect enables remote users to connect to Prisma Access through one of the 100+ locations in 76 countries. The Prisma SD-WAN solution optimizes network access and performance for branch offices by providing deep application visibility with Layer 7 intelligence for network policy creation and traffic engineering. This ensures exceptional user experience by enabling network teams to deliver SLAs for all apps including cloud, SaaS, and UCaaS. Prisma SD-WAN enables branch services such as networking and security to be delivered from the cloud, simplifying the WAN management and deployment. Prisma Access and Prisma SD-WAN provide a full stack of Zero Trust SASE solutions for SAP applications and deployment in Google Cloud as well as on-premises data centers to mobile users, headquarters, remote office, and home office.

Glossary of Terms (continued)	
Panorama by Palo Alto Networks	Panorama™ network security management centrally manages device lifecycle and network security configuration for all firewall form factors including PA-Series physical NGFW, VM-Series virtual NGFW, and Prisma Access in one unified UI. Panorama provides the ability to create and edit security rules in accordance with your organization's security policy across your enterprise firewall deployment from one central location regardless of whether the firewalls are on-premises or cloud-based. Panorama helps you obtain deep visibility and comprehensive insights into network traffic and threats via Application Command Center (ACC) and reduce administrative workload by helping manage updates, automating threat responses through policy-based actions, and utilize API-based integrations with third-party systems.
Cortex XDR by Palo Alto Networks	Cortex XDR® is an extended detection and response platform that gathers and integrates security data to stop sophisticated attacks. It unifies prevention, detection, investigation, and response in one platform for unrivaled security and operational efficiency. The Cortex XDR agent is deployed to SAP users' devices to safeguard endpoints from malware, exploits, and fileless attacks with industry-best, AI-driven local analysis, and behavior-based protection. Organizations can stop Zero Day threats with a single cloud-delivered agent for endpoint protection, detection, and response.
Cortex Data Lake by Palo Alto Networks	Cortex® Data Lake provides cloud-based, centralized log storage and aggregation for your on-premises, virtual (private cloud and public cloud) firewalls, Prisma Access Deployment, and cloud-delivered services like Cortex XDR. Cortex Data Lake is secure, resilient, and fault-tolerant, and it ensures your logging data is up-to-date and available when you need it. It provides a scalable logging infrastructure that alleviates the need to plan and deploy Log Collectors to meet your log retention needs.
Cortex XSOAR by Palo Alto Networks	Cortex® XSOAR™ is a security orchestration, automation, and response (SOAR) platform that helps you coordinate and accelerate incident response across your cloud environment. Cortex XSOAR can help provide the removal of false positives and reduce alerts that call for human intervention by up to 95%. Cortex XSOAR integrates with your entire Palo Alto Networks portfolio as well Google Cloud IDS, Pub/Sub, Compute Engine, VPC Firewall Rules, Google Cloud Security Command Center, and many other Google Cloud services. Cortex XSOAR automation helps reduce incident response times in your SAP deployment in a hybrid environment.

Copyright

paloalto NETWORKS | Deloitte. | Google Cloud

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com