Winter 2023

SafePaaS™

Leading Policy-based Access Governance Platform

SafePost Quarterly

A message from our CTO

Hennie Vermeulen

We wish all our customers, partners, and communities a safe and successful 2023!

As we wrap up 2022 and move into 2023, SafePaaS continues to design, build and deliver cutting-edge enterprise governance capabilities on the platform to meet the growing needs of our customers. In the fourth quarter, we released 15 new enhancements across product suites, including enhancements to control inherent risks in application roles, streamline periodic identity verifications, and prevent risks in access change requests. We have also introduced new API services to simplify secure data transfer from any on-premise and cloud data source. That brings the total number of releases to 414 in 2022.

According to the 2022 Ponemon Institute State of Cybersecurity and Third-Party Remote Access Risk Report, 54% of organizations experienced a cyberattack in the last 12 months, while 75% of respondents said they've experienced a significant increase in security incidents. As we move into 2023, **SafePaaS takes a giant leap forward into the access governance space** whilst continuing to innovate and invest deeply in R&D to provide governance across the enterprise and protect our customers from the bombardment of emerging security threats, ever-evolving compliance regulations, and audit scrutiny. New capabilities will help and empower our customers to actively govern their enterprise by mitigating risks and security threats to ensure compliance and reduce audit findings.

We continue our mission to provide the most useful platform that effectively governs the enterprise. The scope of modern access governance extends beyond simply managing access to resources in siloed IT systems. Access governance defines access controls, data policies, and security protocols for all information systems and data across the enterprise. SafePaaS now supports any ERP, any application, any database, and any cloud infrastructure to ensure enterprise-wide governance.

SafePaaS recognizes the need for organizations to maintain a strong security and cyber posture with reduced budgets through consolidating point solutions for IGA, PAM, and GRC into a unified platform that meets the needs of the CISO, CIO, CAO, and CFO.

Read on to find out how our customers turn risk insight into a stepping stone for their success.

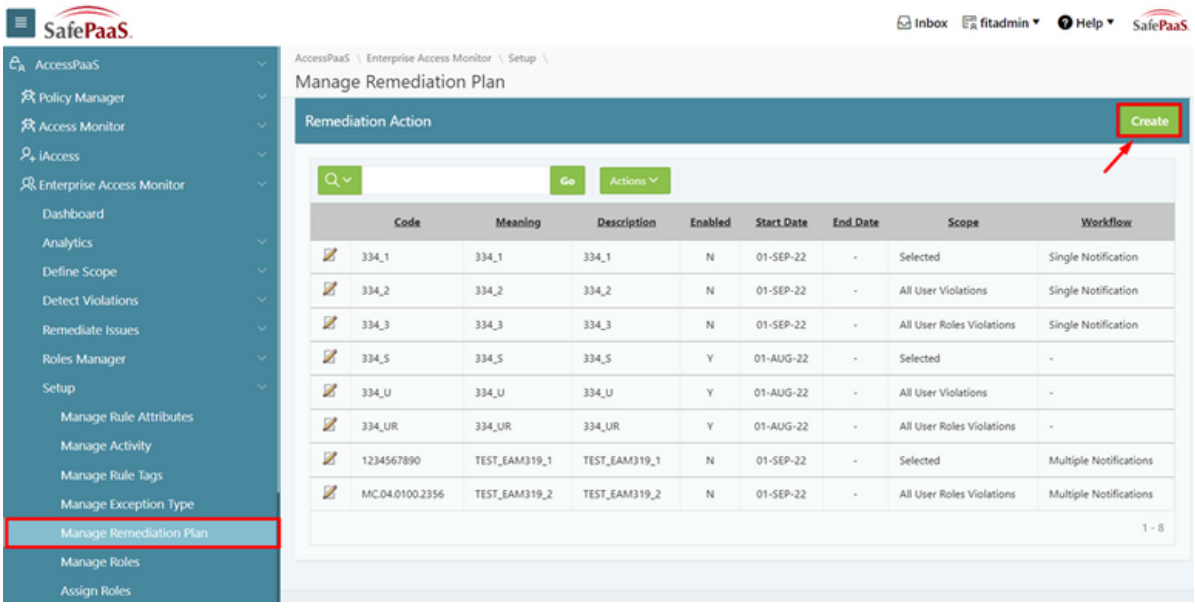
WHAT'S INSIDE THIS ISSUE?

Oracle E-Business Suite customers can now move to the latest Enterprise Suite

SafePaaS customers who currently use the platform for Oracle E-Business Suite can take advantage of special offers this quarter and move to our Enterprise Suite. This will allow customers to:

- Automate scheduled data transfer for Segregation of Duties (SOD) controls monitoring.
- Seamlessly connect to any other applications (including Cloud apps and homegrown apps) or data sources in scope for SOX/ITGC controls monitoring.
- Have access to enhancements that reduce the cost of remediation and streamline compliance activities across EBS and access management systems such as IDM (Azure, Okta), ITSM (ServiceNow, Remedy).
- Improve SOD compliance effectiveness by assigning managers to periodically review their employees' SOD violations and issue corrective actions.
- Mitigate security risks by including database and operating systems or Oracle Cloud Infrastructure (OCI) identities in the periodic access certification process.
- Prevent audit findings due to variances in user access requests managed in ITSM systems such as ServiceNow versus the access grants in Oracle EBS.

The following screen shows how the SafePaaS admin can remove remediation bottlenecks by sending corrective action requests to managers responsible for the segregation of duties controls.



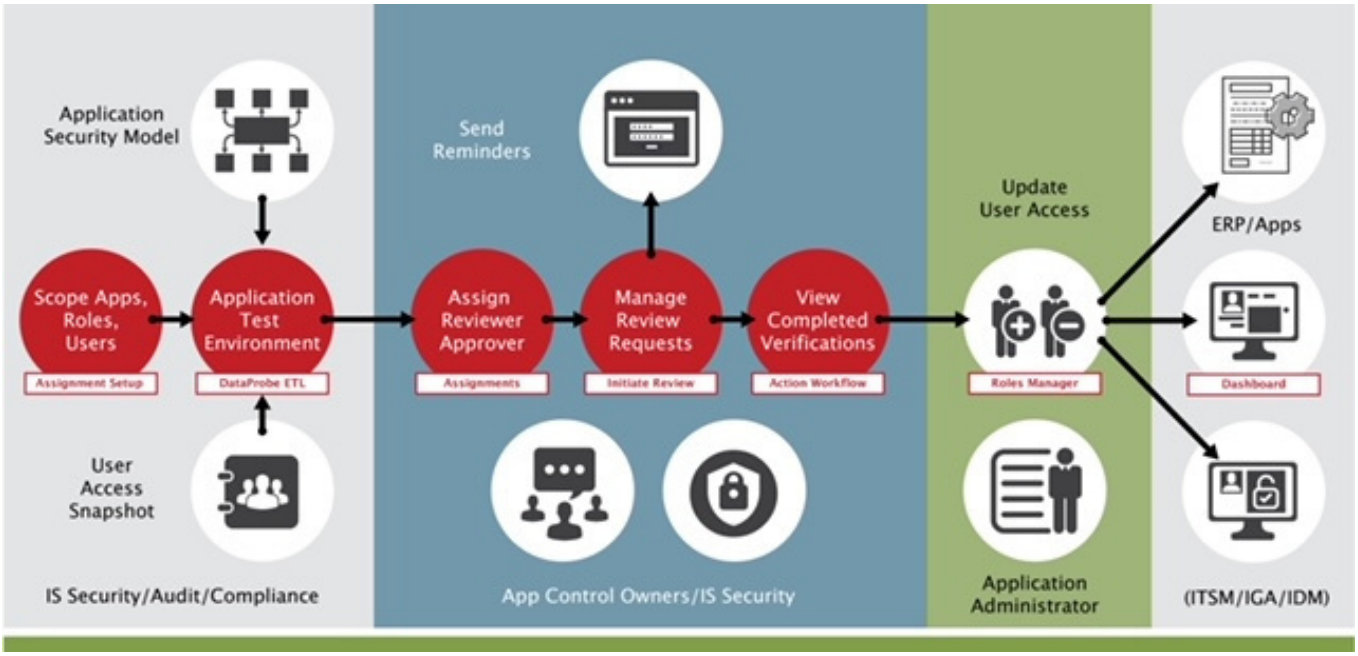
*As the 2022 Cost of Insider Threats: Global Report reveals, insider threat incidents have risen 44% over the past two years, with costs per incident up more than a third to $15.38 million.

*Ponemon Institute

Performing access certification is crucial for avoiding access violations. Without access certification, the risk of security breaches increases. Regularly scheduled access reviews allow users to be assigned only the necessary access to perform their jobs. Access reviews are triggered when someone changes departments, job roles, or departs the organization to verify that employees have not accumulated excessive access while with the organization. Access certification also ensures that employee access does not continue after departure from the organization.

An enterprise's ability to improve reach while managing risk is the foundation of identity and access management. Automating Access certification sparks initiatives in this area in many ways. Access certification is responsible for consolidating and connecting identity and access data, which can be used in user provisioning and role management. Access certification filters the consolidated data, leaving a sturdy, trustworthy foundation.

SafePaaS customers are quickly adopting our end-to-end certification capabilities to comprehensively view roles and privileges that malicious insiders can attack and exploit. Undetected risk can impact your business - by having visibility into identities across the entire enterprise, you can ensure audit readiness and maintain compliance.



Enterprise-wide user access request management

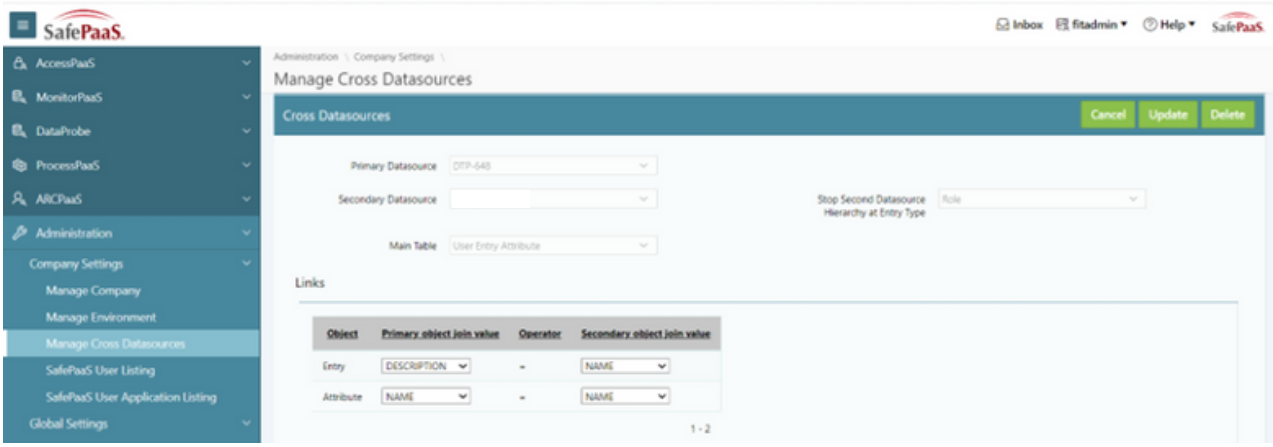
Risk has materially increased in user access request management as a result of the following changes:

- Digitalization
- Evolution of business and IT landscapes
- Increased adoption of hybrid work models
- Adoption of hundreds of cloud applications, and
- Legacy on-premise applications

Organizations with complex enterprise systems require Identity Lifecycle Management solutions to control access for onboarding employees, contractors, and third parties. Any change to work assignments or departures from the organization requires immediate updates to security privileges in compliance with access governance policies to ensure users only have access to what they need while removing access they don't need. Policy-based access management also improves user productivity while preventing unauthorized users from accessing business-critical systems.

SafePaaS' cloud-native identity access governance platform advances and complements Microsoft Azure AD allowing you to enable authentication and role-based access and achieve comprehensive identity access governance with attribute visibility based on zero trust.

SafePaaS' identity access governance hub for Microsoft Azure AD gives you the visibility and control your certification managers need to support your compliance, risk, and governance efforts without slowing down or putting your business at risk.



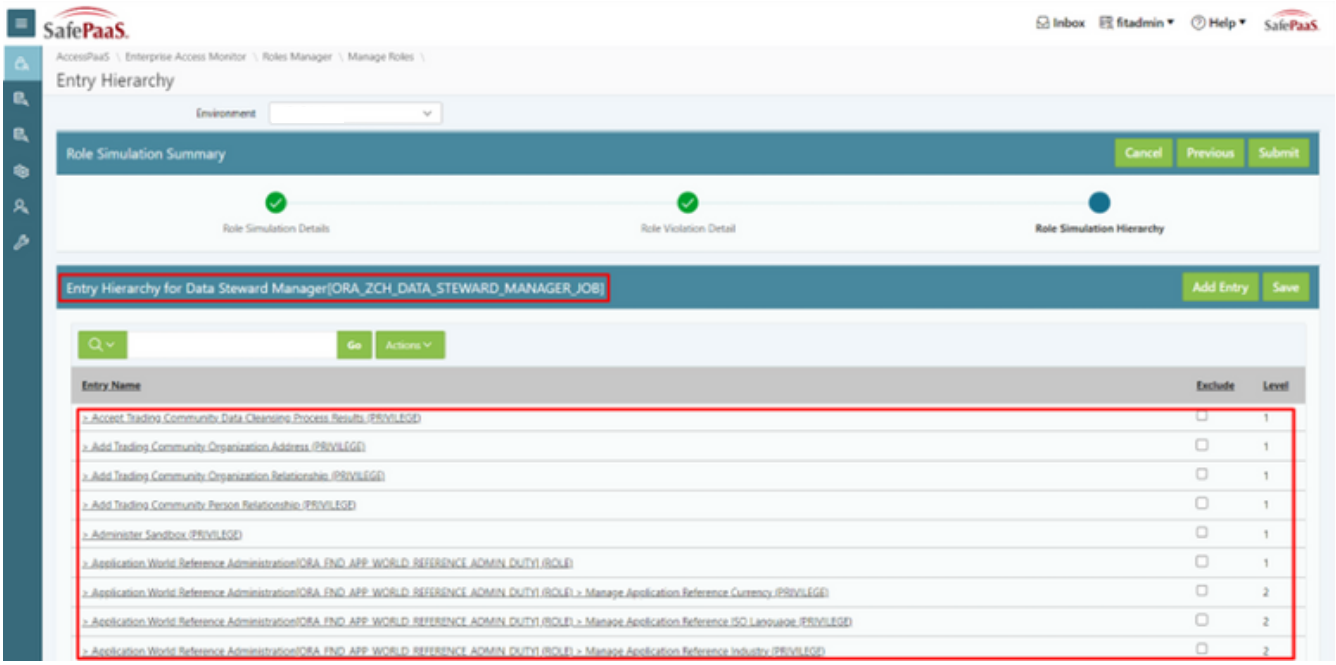
The following page shows how you can cross-link data sources to ensure that the roles catalog in your provisioning systems e.g. Azure AD, Okta, ServiceNow can reference the security attributes granted to the users to ensure effective compliance with access policies.

Enterprise Roles Management

Today, many organizations manually maintain changes to security privileges that enable role-based access controls (RBAC) to critical business information systems. The downside: the manual management of roles does not simulate or prevent security risks that can result in cyber attacks, security breaches, and audit findings. Roles are requested and assigned to users using high-level descriptions from outdated or inaccurate catalogs.

ERM automates the roles management process and prevents security risks by simulating the risk based on changes to fine-grained privileges and reporting security risks to assigned security and control owners through a closed-loop workflow for approval.

The following screen shows how Oracle ERP administrators can remove SOD risks in the seeded roles and design new roles to meet business needs by editing the privileges, simulating and generating custom roles that fit business needs.



Roadmap 2023

Q1
SafeInsight - Audit Analytics

Organizations are seeking new ways to transform their rapidly growing data into insight that mitigates risks and unlocks new opportunities. However, using traditional reporting tools to look for unusual patterns in large data sets is like finding a needle in a haystack. SafePaaS customers can use SafeInsight to integrate disparate data across systems for a single source of truth and:

- Improve bottom line,
- significantly reduce cash leakage and post-audit
- recovery costs,
- improve revenue recognition timing,
- safeguard
- the integrity of financial statements,
- reduce the cost of internal
- and external audits,
- increase visibility into the controls environment
- and mitigate exposure to fraud.

Automated QA Process

As the speed of innovation grows at SafePaaS, with our new and improved continuous, automated testing capabilities, customers can immediately adopt the new software being released.

Faster Diagnosis and Resolution

Customers can benefit from a simpler process to test controls to ensure effectiveness through enhanced logging and error handling.

Q2
Enhanced Access Governance for SAP

ERP customers can continuously stream data into SafePaaS for continuous controls monitoring to detect and prevent risk.

Roadmap continued

Security Data Lakes

To overcome the challenges of scale, cost, structure, and detection capabilities, SafePaaS customers can take advantage of an enterprise security data lake to separate storage from compute.

An enterprise security data lake is a centralized repository designed to store, process, and analyze all security meta-data from data sources that represent security threats to an organization. Security meta-data can be consumed using industry-standard message formats such as JSON, XML, CSV/Flat-file, etc, and transfer methods including SOAP, REST, JDBC, sFTP, etc. The housed data can be cross-linked, parsed, searched, classified, masked, and encrypted for enterprise-wide security management to prevent cyber threats and regulatory compliance penalties.

Q3
Flexible Data Residency

SafePaaS customers can move their applications across environments and across regions to ensure data residency compliance. SafePaaS makes it easy for organizations to move entire instances from one system to another.

Enhanced DataProbe for input from ANY system

SafePaaS makes it easy for customers using legacy and mainframe systems that don't support the standard protocols such as SOAP and REST to bring data into SafePaaS to ensure enterprise-wide controls coverage.

Q4
360° Data Consumption

With this new capability, customers needn't ever worry about inconsistent data again. 360°data consumption makes it easy for customers to normalize data across the entire enterprise for complete reporting and insights about controls and processes. Once the data is normalized, it can be used for performing effective threat detection and investigations. You can collect and analyze logs from all the data sources including applications, databases, servers,s and SIEM event logs. Security events can be enriched by adding event and non-event contextual information such as identity context (user, host, IP addresses), vulnerability context (scan reports), business context, and more. Context plays an important role in eliminating False Positives, which in turn helps prioritize higher-risk threats.

Customer Success Spotlight

Our customers worldwide continue to lead in their industry by adopting the platform to align their strategies with execution.

We are delighted to welcome one of **Europe's largest producers of waste-based biodiesel** to the SafePaaS community. The Oracle ERP Cloud customer chose SafePaaS to replace manual, error-prone identity governance with consolidated IGA and GRC through the use of AccessPaaS™ and ARCPaaS™. They will also be able to monitor changes to key configurations and master data with autonomous change tracking and automate workflows with MonitorPaaS™ to lower the IT cost of ownership and mitigate the risk of significant deficiencies in audit findings.

A **government agency** in Central America responsible for operating **one of the world's largest canals** has selected SafePaaS to control and manage the segregation of duties in Oracle E-Business Suite.

A **US-based brand of clinical skincare products** upgrades and redesigns its ERP controls with SafePaaS to increase productivity with well-designed roles and prevent high-impact security breaches and mass access control failures.

A **global fast food chain** innovates its access certification process to include databases and operating servers by replacing a time-consuming manual process with centralized management for enterprise-wide certification workflow.

A **British multinational insurance company** deploys Enterprise Roles Manager to monitor changes to fine-grained role attributes and prevent RBAC deficiencies in Oracle ERP Cloud that will allow them to prevent high-impact security breaches and mass access control failures. They can now simulate the impact of role attribute changes to ensure effective controls and usage before deployment.

Industry Headlines

This month, the US burger chain Five Guys experienced a data breach caused by "unauthorized access to files on a file server."

Identity and authentication provider Okta also suffered another breach after a hacker accessed its source code following a breach of its GitHub repositories.

Amazon fell victim to a multi-million dollar fraud scheme by two employees, again highlighting the importance of segregation of duties. "Wortham, the leader of the scheme, provided fake vendor information to unknowing subordinates and asked them to input the information into Amazon's vendor system." It seems that once the information was entered, the employee approved the fake vendors, enabling the vendor accounts to submit invoices to Amazon. The employees then submitted fictitious invoices for payment.

New Hires

We continue to grow as a company and expand our international teams to ensure a culturally diverse environment at SafePaaS, offering global customers uninterrupted customer service and the ability to identify evolving local market demands.

We welcome Sreerekha Jayadevan, who joins our India team as Sr. Developer - Engineering. Sreerekha joins us from Wipro and offers extensive development expertise in PL/SQL technology.

We also welcome Brett Layton, based in California, as Business Development Manager. Brett brings a wealth of experience to the Sales and Marketing team, allowing him to play a critical role in our growth.

Siddhanth Sarkar also joins us, based out of India as Lead Nurturing Specialist. As the demand for Access Governance continues to grow and customers realize the full potential of a platform approach to governance, Siddhanth's knowledge and skills will help us continue on our mission to safeguard commerce, so businesses succeed, people prosper and communities flourish.

Forward Thinking Events 2023

Detecting Threats in Oracle ERP Cloud

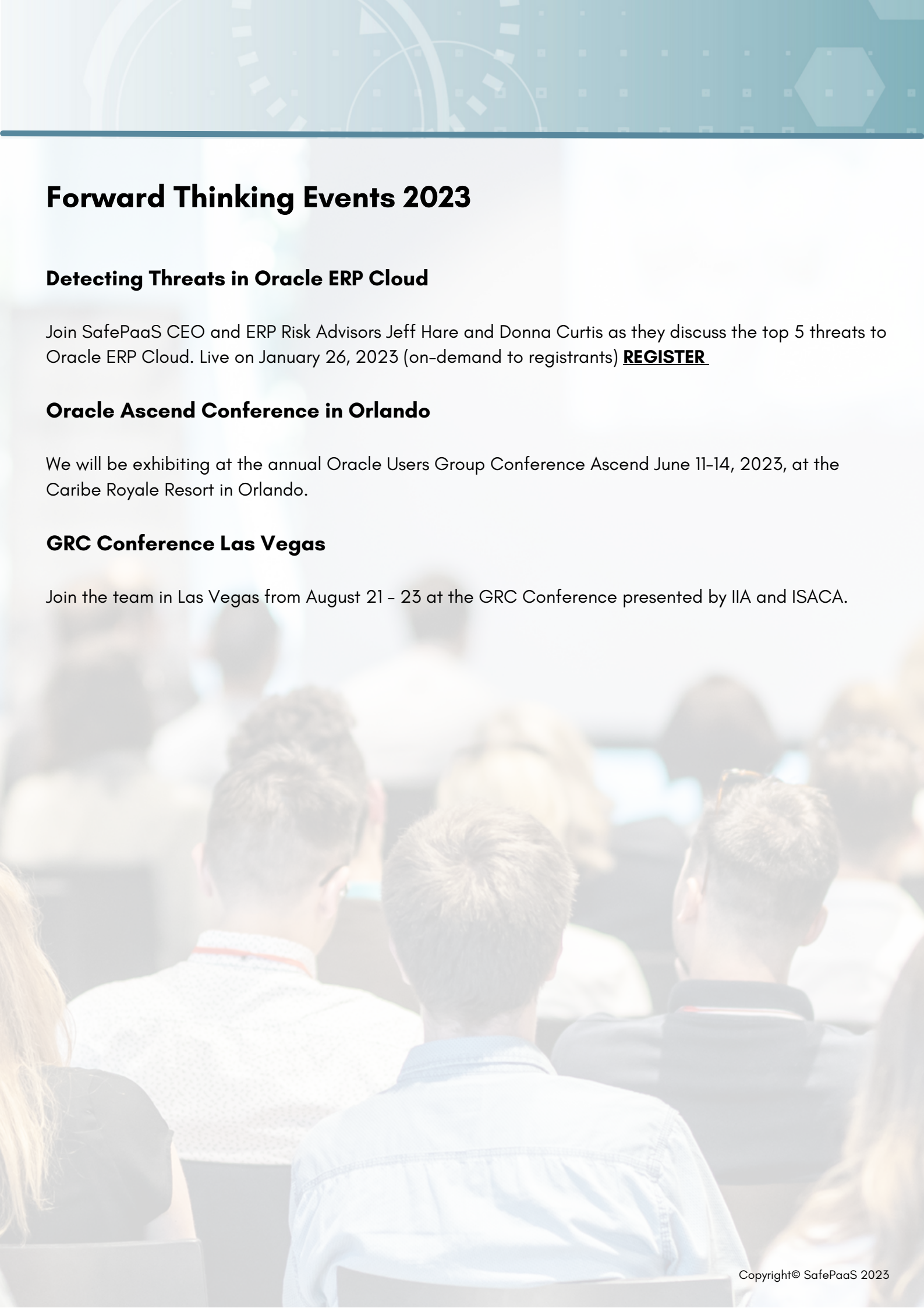
Join SafePaaS CEO and ERP Risk Advisors Jeff Hare and Donna Curtis as they discuss the top 5 threats to Oracle ERP Cloud. Live on January 26, 2023 (on-demand to registrants) **REGISTER**

Oracle Ascend Conference in Orlando

We will be exhibiting at the annual Oracle Users Group Conference Ascend June 11-14, 2023, at the Caribe Royale Resort in Orlando.

GRC Conference Las Vegas

Join the team in Las Vegas from August 21 - 23 at the GRC Conference presented by IIA and ISACA.



RELEASE SUMMARY

Time stamp	Release Issue Key	Component	Release Note
16-Dec-2022 12:00AM	SFP-515	Administration > Company Settings > SafePaaS User Listing	Enhanced SafePaaS User Listing to provide the Role Assignment Start Date and End Date
14-Dec-2022 12:00AM	MTP-233	Inbox - Workflow	Enhanced Incident workflow to enable Requestor to review the changes based on user ID in the change record and provide Incident number from ITSM and justification before sending to Approver
14-Dec-2022 12:00AM	MTP-282	MTP > Incidents notification to the Requestor	Enhanced Incident reports to display the Approver and Reviewer Action status in separate columns
14-Dec-2022 12:00AM	MTP-294	MTP > Analytics > Change Tracker Report	Enhanced Change Tracker report to download a single zip file split based on the split size setting under Company Administration for all monitors
07-Dec-2022 12:00AM	SFP-452	Administration > Company Settings > SafePaaS User Listing	Enhanced SafePaaS User Listing report to provide line item details of roles assigned to users by application

RELEASE SUMMARY CONTINUED

26-Nov-2022 12:00AM	SFP-467	Java/UI Upgrade	Upgraded Java/UI to introduce new capabilities for workflow administration
21-Nov-2022 12:00AM	EAM-346	EAM > Detect Violations > Manage Violations	Enhanced EAM to do Mass Update Exception under Detect Violations
02-Nov-2022 12:00AM	ERM-33	EAM > Roles Manager > Manage Roles	Enhanced role simulation workflow so that violations are detected before the approval workflow is submitted for approval
31-Oct-2022 12:00AM	SFP-432	MTP > Analytics > Change Tracker Report	Enhanced change tracker report to be generated using the scheduler
27-Oct-2022 12:00AM	EIA-72	Administration > Company Settings > Manage Company	Enhanced the company page to disable email notification for the users when the EIA request is approved or rejected
26-Oct-2022 12:00AM	MTP-254	MTP > Monitors > Manage Monitors > Add/Edit Monitors	Enhanced Manage Monitors page to view the occurrences or change trackers under the snapshot tab by selecting the radio button
13-Oct-2022 12:00AM	SFP-439	Administration > Company Settings > SafePaaS user Listing	Enhanced SafePaaS User Listing report to show roles by Applications in separate rows along start and end dates