

CYBERSECURITY SOLUTIONS

Identity is the cornerstone of Digital Transformation



30+

At Paynalli Systems we have a strong track record and expertise in **zero trust, identity management, cloud security**, and secure software development. With more than 40 years of combined experience and operations in USA and Mexico, we have improved the cyber security posture for 30+ clients.

Our vision is that **cybersecurity** is a critical component of **digital transformation**, providing protection for digital assets, **mitigating cyber risks**, ensuring compliance, **building trust** with clients, **fostering innovation**, and enhancing overall business resilience. By prioritizing cybersecurity throughout their digital journey, our clients can reap the full benefits of digital transformation while safeguarding their operations, data, and reputation.



OUR ROLE

Overall, our role is to provide our clients with specialized expertise, guidance, and support to enhance their security posture, mitigate risks, and respond effectively to cyber threats. As your trusted advisors, we protect your critical assets and maintain a strong defense against evolving cybersecurity challenges.

- 1. Assessing Security Posture:** Conduct thorough assessments of existing security infrastructure, policies, and practices, identify vulnerabilities, risks, and potential weaknesses in systems, networks, applications, and processes.
- 2. Providing Expert Advice:** Develop effective security strategies, recommend appropriate security controls and technologies, and advise on incident response, disaster recovery, and business continuity measures.
- 3. Designing and Implementing Security Solutions:** Design and implement security solutions tailored to our client specific needs. This includes selecting and configuring identity management, intrusion detection, encryption technologies, access control mechanisms, and other security tools.
- 4. Conducting Security Audits:** We perform comprehensive security audits to assess compliance with regulatory requirements and industry standards.
- 5. Training and Awareness:** Cultivate a security-conscious culture within the organization by raising awareness about potential threats, social engineering attacks, phishing, and other cybersecurity risks.

TOP 10 SOLUTIONS WE PROVIDE TO OUR CLIENTS

1

Identity and Access Management

2

Identity Governance and
Administration

3

Privileged Access Management

4

SIEM and SOAR implementation and
management

5

Cyber Security Assessment and
Consulting

6

Data Loss Prevention

7

Cloud Security

8

Secure Software Development

9

SSO and API Gateway
implementation

10

Blockchain and Smart Contracts
Development



01

GLOBAL FINANCIAL
INSTITUTION

Paynalli Systems established escalable **DevSecOps** practices in the Software Development Lifecycle, thus, increasing productivity and reducing time to market, while maintaining a secure foundation

THE PROBLEM: MIGRATE FROM DEVOPS TO DEVSECOP

Our client, a global financial institution, faced a big challenge when striking the right balance between security and speed of development. Paynalli System established security practices into the **DevOps** workflow, aiming to ensure that security is built into the development process from the beginning.

Here are some of the challenges our client faced when implementing **DevSecOps**:

Cultural Shift: Implementing **DevSecOps** requires a cultural shift towards collaboration, communication, and breaking down silos between development, operations, and security teams.

Legacy Systems and Applications: client reliance on legacy systems and applications, having outdated security practices or limited compatibility with modern **DevSecOps** tools and practices.

Skills and Expertise Gap: Building and sustaining a strong **DevSecOps** team with the requisite skills and expertise.

Tooling and Automation: Selecting, integrating, and configuring the right tools and technologies was a difficult undertaking for our client

OUR CONTRIBUTION: DRIVE DEVSECOPS ADOPTION

Implementing an effective **DevSecOps** program for our client required careful planning and coordination. Here are some steps we recommended and helped implement:

- 1. Gain Leadership Support:** Obtain buy-in from senior leadership and stakeholders within the organization. Communicate the benefits of **DevSecOps** in terms of increased security, faster time-to-market, and improved agility.
- 2. Assess Current State:** Conduct a thorough assessment of the organization's current security practices, development processes, and infrastructure. Identify areas of improvement and potential vulnerabilities. Understand the existing security and compliance requirements specific to the financial industry.
- 3. Define Security Policies and Standards:** Define guidelines for secure coding practices and comprehensive security policies and standards that align with industry best practices and regulatory requirements.
- 4. Foster a Collaborative Culture:** Break down silos and establish cross-functional teams. Foster a culture of shared responsibility for security throughout the development lifecycle.
- 5. Security Integration into Development Lifecycle:** Incorporate security practices into each stage of the development lifecycle. Implement security controls, code reviews, and security testing at every step. Integrate security tools into the continuous integration/continuous delivery (CI/CD) pipeline to automate security checks and ensure early identification of vulnerabilities.

OUR CONTRIBUTION: ADD VALUE TO SDLC WITH DEVSECOPS

6. Automation and Tooling: Leverage automation and tooling to streamline security processes. Implement security testing tools, static code analysis, dynamic application security testing (DAST), and container security scanning. Automate security checks and vulnerability assessments in the CI/CD pipeline to ensure continuous monitoring and rapid feedback.

7. Continuous Monitoring and Improvement: Implement continuous monitoring and real-time threat intelligence to detect and respond to security incidents promptly. Regularly assess and evaluate the effectiveness of the DevSecOps program. Measure key performance indicators (KPIs) related to security, speed, and quality to identify areas for improvement.

8. Compliance and Audit: Ensure that the DevSecOps program adheres to relevant industry regulations and compliance requirements.

9. Collaboration with Third Parties: Engage with external security experts, industry groups, and relevant communities to stay updated on emerging threats and best practices. Collaborate with vendors and partners to ensure secure integration of third-party components and services.

THE TOOLS WE USED AND IMPLEMENTED



Snyk: Secured the entire development lifecycle, static code analysis, dynamic application security testing (DAST), and container security scanning.

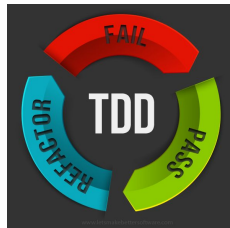


Jenkins

Jenkins: Automate security checks and vulnerability assessments in the CI/CD pipeline for on-premises applications



Argo CD: Automate security checks and vulnerability assessments in the CI/CD pipeline for containerized applications in Kubernetes and the Cloud.



Test-Driven Development: Established for our client Test-driven Development best practices for a improved software quality and reducing time to market while maintaining high software security and quality standards.



02

BLOCKCHAIN IN REAL ESTATE

Paynalli Systems provided a flexible **Blockchain** solution based on **Ethereum Smart Contracts** to a Real Estate Company

THE PROBLEM: REAL ESTATE BLOCKCHAIN ADOPTION

Our client, a construction and real estate development company, identified **blockchain** opportunities in their **business model**. However, they needed to identify a consulting and implementation partner with the right experience building secure software and smart contracts for the **Web3 Ethereum** ecosystem. Our client was concerned about these threats:

1. Security and reliability of the smart contracts.

Development best practices are required to preserve reputation of the business. Software quality control in place that only an experience implementation partner can provide.

2. Understand their unique requirement to address the opportunities they identified.

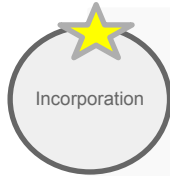
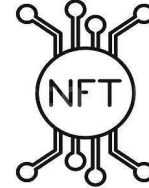
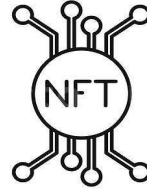
Our client's business model is unique and the blockchain solution required a high level of adaptability to new market opportunities.

3. Cyber-attacks on Smart Contracts are rampant.

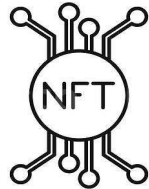
Poorly written and untested Smart Contracts can lead to huge financial losses and penalties.

Examples of vulnerabilities includes: Reentry, Arithmetic Overflows, Race Condition, Entropy Illusion, Tx Origin Authentication and Lack of Access Control List

OUR SOLUTION: FRACTIONAL NFTs



- Notary Service
- Mint NFT



Property as an ERC-721 NFT



Property Shares as ERC-20 Fungible Tokens



Property Shares as ERC-20 Fungible Tokens

THE TOOLS WE USED AND IMPLEMENTED



Nuxt JS: For secure, high performing and SEO-friendly rapid UI development. Deployed in the Edge



Solidity: De Facto Standard for smart contracts development. We developed ERC-20 and ERC 721 compliant smart contracts for our client's solution



Metamask: Integrated the solution with Metamask Wbe3 and Mobile wallets.



Truffle Suite: By using the Truffle suite, we were able to deliver the solution to our client in an agile manner and constantly be able to show progress in a controlled test environment.



03

BUSINESS INFORMATION

RESEARCH COMPANY

Paynalli Systems provided **Zero Trust** Consulting to a Business Information and Research Company

THE PROBLEM: ZERO TRUST ADOPTION

Our client, a corporate information research firm, needs to strengthen security posture in order to enter new markets with more stringent compliance regulations. Modernization of their security tools and procedures was necessary to boost corporate productivity and raise consumer confidence in their digital offerings.

Main concerns from client expressed during our cyber security assessment:

Insider Threats: Our client relied on traditional perimeter-based defense model assuming that users and device within the network were trustworthy. However, insider threats, whether intentional or accidental, can pose significant risks.

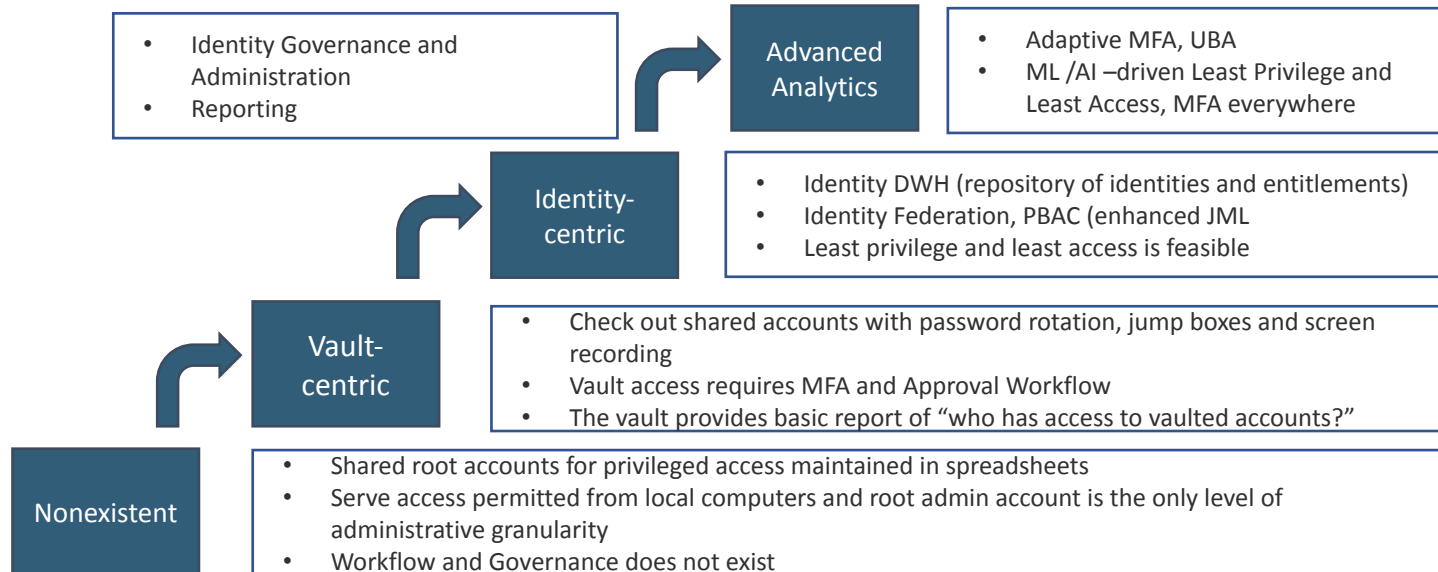
Evolving Threat Landscape: Over-reliance on legacy security models made our client to struggle to keep up with the rapidly evolving threat landscape.

Stringent Compliance Requirements: Our client was unable to enter new markets because of more stringent international compliance standards..

Data Privacy: Given the nature of our client business model, Data Privacy and Data Loss Prevention were essential for preserving business reputation and client trust

OUR SOLUTION: ZERO TRUST MATURITY MODEL

The Zero Trust Maturity model was used to conduct a thorough evaluation for our client and identify opportunities for improvement in the areas of data privacy, data loss prevention, and access governance. With excellent potential to reach level 4, our client was able to reach maturity level 3.



04



REACTIVE IDM OUR FLAGSHIP PRODUCT

Reactive IDM is an Identity Governance and Administration platform, delivering next-generation analytics and second to none scalability

THE PROBLEM: LEGACY IDM PLATFORMS

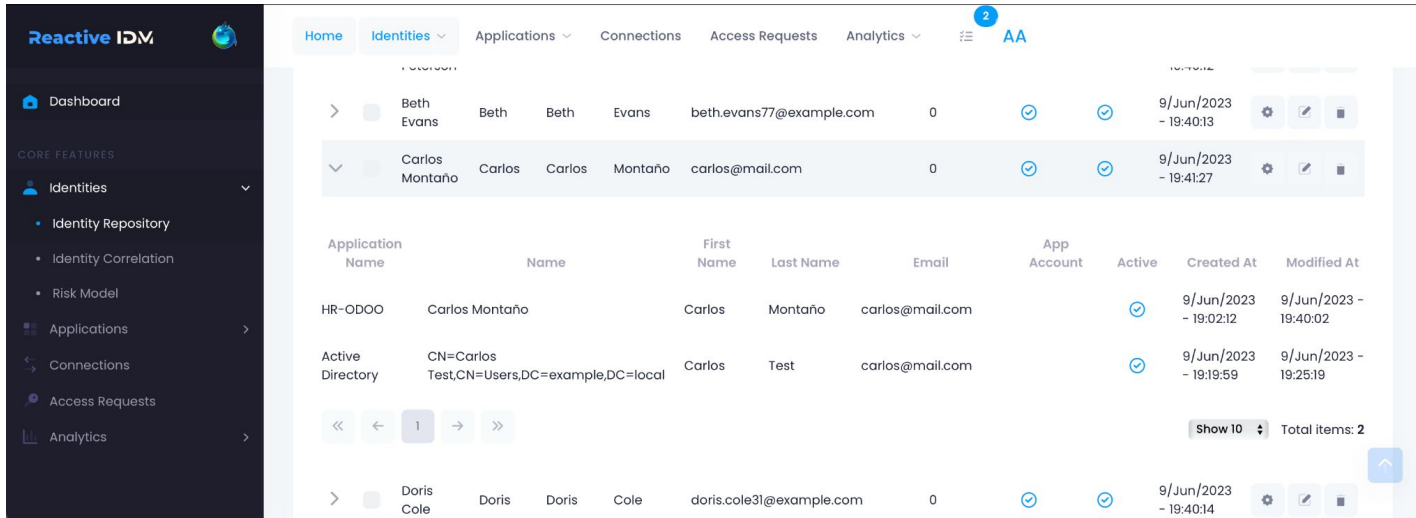
While existing identity management tools offer significant benefits, they can also encounter some challenges. The problems that organizations most often face when using identity management tools:

- 1. Complexity and Deployment:** Identity management tools are complex to implement and deploy. Configuring and integrating these tools with existing systems and applications may require significant effort and expertise.
- 2. Licensing costs.** In addition to implementation and consulting costs, licensing cost can be onerous and prevent many Small and Medium Size Business to adopt an Identity Management Solution.
- 3. Limited Integration with downstream and upstream systems.** Many organizations have legacy systems and applications that may not have native support for modern identity management protocols and standards. Integrating identity management tools with these legacy systems can be challenging and may require custom development or workarounds

OUR SOLUTION: REACTIVE IDM

Paynalli Systems engineered from the ground up an Identity Management Solution with industry best practices

1. Based on standards. Connectors compatible with Sailpoint and ForgeRock
2. Out-of-the-box integration with major players such as Okta, Splunk, Elastic Search
3. Theoretical infinite scalability. Built with Cloud-native and Big Data technologies
4. Built-in Identity Threat Detection and Response (ITDR) and Account Takeover (ATO prevention capabilities)



The screenshot displays the Reactive IDM web interface. On the left is a dark sidebar with navigation options: Dashboard, CORE FEATURES (Identities, Applications, Connections, Access Requests, Analytics), and a search bar. The main content area shows a navigation menu with 'Identities' selected. Below the menu, there are two sections: a list of identities and a table of application connections.

Identities List:

Identity	First Name	Last Name	Email	App Account	Active	Created At	Modified At
Beth Evans	Beth	Evans	beth.evans77@example.com	0	✓	9/Jun/2023 - 19:40:13	
Carlos Montaña	Carlos	Montaña	carlos@mail.com	0	✓	9/Jun/2023 - 19:41:27	

Application Connections Table:

Application Name	Name	First Name	Last Name	Email	App Account	Active	Created At	Modified At
HR-ODOO	Carlos Montaña	Carlos	Montaña	carlos@mail.com		✓	9/Jun/2023 - 19:02:12	9/Jun/2023 - 19:40:02
Active Directory	CN=Carlos Test,CN=Users,DC=example,DC=local	Carlos	Test	carlos@mail.com		✓	9/Jun/2023 - 19:19:59	9/Jun/2023 - 19:25:19

At the bottom of the table, there is a pagination control showing '1' of 2 items and a 'Show 10' dropdown. Total items: 2.

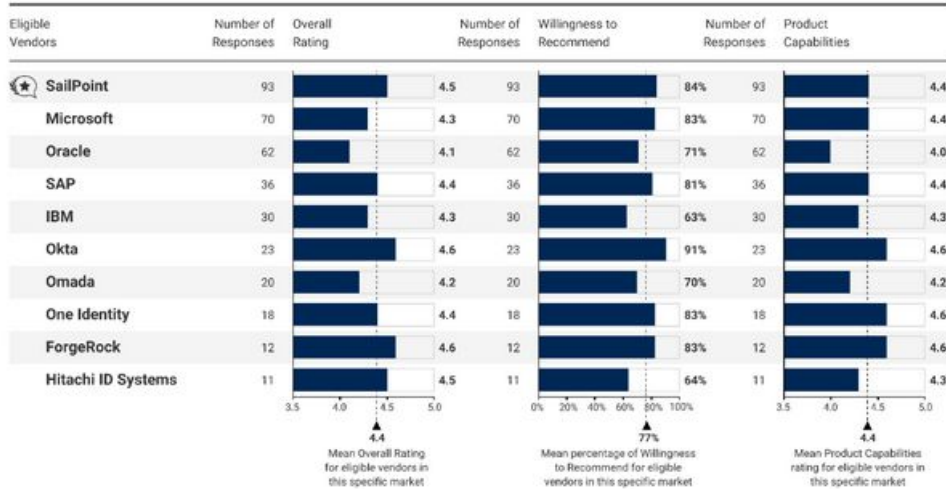
HOW REACTIVE IDM COMPARES WITH OTHER TOOLS

Gartner Peer Insights "Voice of the Customer" Identity Governance and Administration

Vendor Comparison - 1 of 2

As of 31 January 2020

Sorted by overall reviews



Notes: Vendors with greater than or equal to 10 eligible reviews on Gartner Peer Insights in the past one year as of 31 January 2020 are considered eligible vendors. Vendors are listed by overall reviews as displayed in Figure titled "Overall Ratings." In case, two or more vendors have the same number of reviews, then they are listed alphabetically. Gartner Peer Insights Customers' Choice announced on 12 March 2020. Number of reviews and ratings as of 31 January 2020. "Mean Overall Rating" may not match with the "Mean Rating" in the Figure 1 as time frame for the calculation is different. All charts are plotted and labeled to the tenths digit for clarity.

©2020 Gartner, Inc. All rights reserved.

Reactive IDM Competitvity

- Deep Integration with Okta for Identity Governance
- Similar Features as Sailpoint but improved UX, scalability and efficiency
- Binary compatible with ForgeRock.
- Can migrate from Sailpoint and ForgeRock easily

Market Objectives

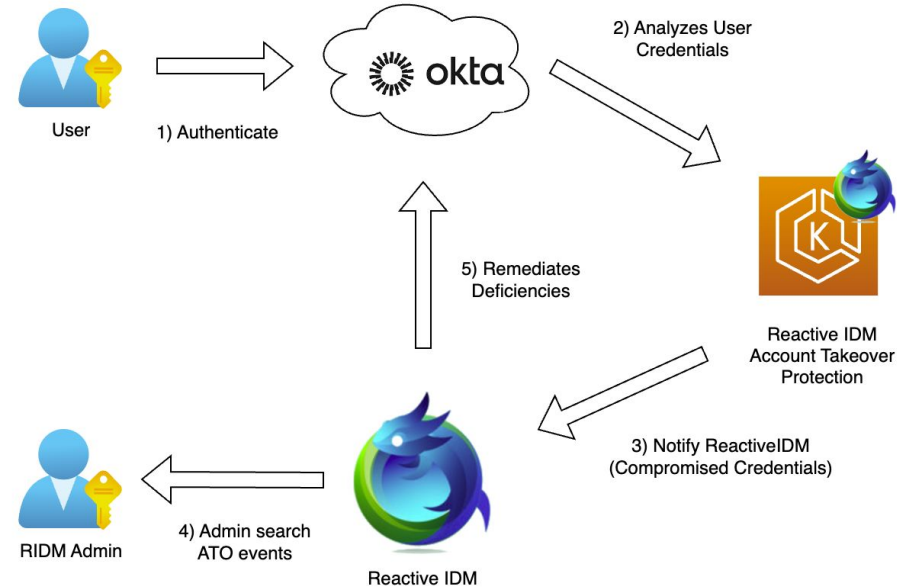
- Enable SMB to adopt Zero Trust Security model
- Lessen costs to existing Sailpoint, Oracle and ForgeRock clients
- Be attractive to LARGE organizations having trouble scaling to million of identities

ACCOUNT TAKEOVER PROTECTION

Paynalli Systems' Reactive IDM offers out-of-the-box integration with **Okta** for implementing **Account Takeover Protection** on common **passwords attacks**.

How Reactive IDM ATO Solution works?

1. Upon user login in Okta, RIDM ATO **analyzes user credentials**
2. If compromised credentials are detected, ATO solution records the event in Reactive IDM
3. Compromised credentials events are visible to the IDM Administrator
4. Reactive IDM **remediates deficiencies** by setting up stricter Password Policies, and enforce MFA enrollments and password resets **automatically!**



THE TOOL WE USED IN REACTIVE IDM



Nuxt JS: For secure, high performing and SEO-friendly rapid UI development. Deployed in the Edge



Kafka: De Facto Standard for data streaming. We use Kafka to aggregate application data, logs and system telemetry



Elastic: For application log analysis and SIEM use cases that Reactive IDM implements out-of-the-box.



Prometheus: Reactive IDM uses Prometheus for system monitoring and alerting, as a time-series database allows to build AI/ML-based alerts and responses

Thank You!



¿ Do you have any question?

raul.caceres@paynalli.com

+52 (999) 163 1083 - México

+1 (973) 637-0435 - USA

<https://paynalli.com>