

Grupo Argos Strengthens Security and Reduces Complexity across Data Center and Cloud with Idaptive



Grupo Argos is a conglomerate with sustainable investments in infrastructure headquartered in Medellin, Colombia and registered on the Colombia Stock Exchange. Its presence is throughout Latin America and North America, through its affiliates and subsidiaries including Argos (cement), Celsia (energy) and Odinsa (road and airport concessions). Grupo Argos, parent of the business group, has strategic investments in companies listed on the stock exchange and private companies, as well as a solid investment portfolio.

THE CHALLENGE

Increase visibility into outsourced IT activity for more efficient management, as well as SOX compliance due to US-based holdings. Increase security and reduce strain on the help desk due to password reset requests, by providing employees with single sign-on (SSO) to key company apps and joining Macs to Active Directory.

With more than 400 employees of the parent company, password expirations and resets at Grupo Argos had become a significant strain on IT resources. "Traveling was another challenge for our staff. Logging into SAP and other apps from outside the office was difficult, and that was impacting productivity," says Paula Jaramillo, IT Coordinator at Grupo Argos. "Compounding the issue was the fact that users frequently had different passwords for each SAP app, so having three or four SAP passwords wasn't unusual."

Employees across the organization also had an additional password for each of their cloud apps including Office 365, Ariba and Success Factors. Managing passwords for both privileged users and end users had become cumbersome, and concerns were also raised about security because users were re-using passwords, or keeping their passwords in unsafe locations in an effort to alleviate password overwhelm.

According to Jaramillo, Macs presented the company with an entirely different set of issues. "Macs were completely independent, and managed locally with users having local accounts without IT oversight. Configurations on our Mac devices seemed to just disappear," she says.

But forgotten passwords and Mac devices weren't the only issues for Grupo Argos. "We use third-party service providers for the administration of our SAP and Windows servers," she says. "They handle all our server needs, which is beneficial, but it also leaves us with limited visibility into what happens inside those servers."

Grupo Argos is subject to Sarbanes Oxley (SOX) compliance regulations due to its U.S. holdings. The ability to effectively audit access and activity to determine what actions had been taken on their servers was a fundamental requirement for an identity management platform.

All too frequently, the SAP servers would shut down and the company had no visibility into the cause. "We have a great degree of trust in our server administration company, but we still needed to know what was happening on those servers both to meet SOX compliance, troubleshoot the outages and to help make informed decisions. Ultimately, we're responsible for everything that transpires inside our environment," says Jaramillo.

To address these issues and reduce cyber-attack surface across the organization, Grupo Argos needed to provide employees in the office and on the road with single sign-on (SSO) to SAP and other key apps, to more effectively manage Mac devices, and to gain significantly more visibility into administrative activities on servers.

THE SOLUTION

Idaptive provided the visibility and comprehensive auditing required for SOX compliance, SSO to key cloud applications including Office 365 and Success Factors, and a single login for Mac users.

The IT team at Grupo Argos began its search for a solution by evaluating materials from analyst firms Gartner and Forrester Research. Once they'd narrowed the field, they took a deeper look at the top providers.

Idaptive was the only provider to offer single sign-on, auditing and management of both privileged users and end users across both the enterprise data center and the organization's growing dependence on cloud apps.

A live demo helped the team to better understand how Idaptive could help them to audit the activities performed on their servers, and how they might be able to reproduce administrator sessions. "We wanted to see how we could replay entire sessions and analyze exactly what actions had been taken, when they were taken and who executed them," says Jaramillo.

This ability to do session replay was crucial to meet Grupo Argos' goal to gain visibility into exactly what was happening on its servers managed by third-party service providers.

Early on, after initially implementing Server Suite across its SAP servers, the organization experienced an unexpected illustration of the value of its in-depth audit capabilities including session replay. "When we went home for the weekend, our SAP servers were working fine," says Jaramillo. "When we returned on Monday, they weren't operational. With the help of the Idaptive team, we ran an audit and found that over the weekend a change had been made to one of the servers.

"Rather than having to go through the usual process of contacting our services company, scheduling a meeting, gaining access to our servers and then ascertaining what had happened, we worked out the issue in real time. Using Idaptive, we used session replay to understand everything that had happened, identified the problem, and quickly had our SAP environment back up and running with a minimal loss of productivity. We knew we'd made the right choice," she said.

THE RESULTS

Increased visibility into outsourced IT activities. End users are more productive and effective due to SSO, and helpdesk calls have dramatically been reduced.

After experiencing firsthand how Idaptive would help them to directly address such server issues in the future, Grupo Argos moved forward with an expansion of the implementation. "We were so impressed with Idaptive's ability to audit and replay activities across our SAP environment that we immediately extended it across our Windows Server environment as well. Now, we have complete visibility across the entire enterprise – including data center and cloud," says Jaramillo.

"And it's not just visibility that the Idaptive audit feature provides – it's valuable information that can be leveraged to make informed decisions about the server environment," says Jaramillo. "Now, we can perform our own investigation to see exactly what transpired when something goes wrong. We can then take the actions necessary to reverse or correct the situation."

As part of the implementation, the company also installed Identity Service to provide single sign-on for SAP apps. "Today, everybody has one-password access to all the modules inside the SAP system, which means many people went from four passwords to single sign-on," she says. "After that, we implemented single sign-on for our other critical apps like SuccessFactors, Ariba and Office 365, so users today only have to remember one password for access to everything they need through a single portal, where they can see all of their apps and just click on an icon to gain access.

"Not only has pressure been taken off the help desk, but we've reduced our risk of security breach dramatically. Because every user needs just one password, we've eliminated password sharing and the tendency to store them in insecure places – and that goes for server access as well," she says. "And our Macs are now managed. We no longer get calls from frustrated users unable to access apps from their Mac devices. The entire program has been a great success."

Idaptive delivers Next-Gen Access, protecting organizations from data breaches through a Zero Trust approach. Idaptive secures access to applications and endpoints by verifying every user, validating their devices, and intelligently limiting their access. Idaptive Next-Gen Access is the only industry-recognized solution that uniquely converges single sign-on (SSO), adaptive multi-factor authentication (MFA), enterprise mobility management (EMM) and user behavior analytics (UBA). With Idaptive, organizations experience secure access everywhere, reduced complexity and have newfound confidence to drive new business models and deliver kick-ass customer experiences. Over 2,000 organizations worldwide trust Idaptive to proactively secure their businesses. To learn more visit www.idaptive.com.

Ready to learn more?

Please contact us at
hello@idaptive.com