



Capitalizing on Palo Alto Networks for assured cloud visibility, user access, and security



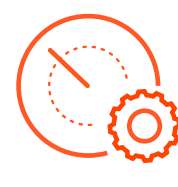
RESULTS Enabling consistent cloud security and secure remote access.

90%

reduction in disparate tools

0

High-priority incidents compared to 1,000 in 2020



Turnaround time (TAT) for generation of compliance reports reduced

Darwinbox is a new-age, agile Human Capital Management (HCM) Suite that enables enterprises and growing businesses to automate their day-to-day human resources (HR) processes, deliver actionable insights, and build better workplaces. The company serves over 850 organizations and 2.2M employees across 116+ countries, including large conglomerates and fast-growing tech companies. With a lean security team, no real-time monitoring, and open-source tools to manage their cloud and runtime security, Darwinbox's enterprise customers were immensely concerned about their cybersecurity posture and strategy.



CUSTOMER

Darwinbox



INDUSTRY

End-to-end enterprise HR software



COUNTRY

India



PRODUCTS

Prisma® Access

Prisma® Cloud

CHALLENGE

Open-source tools and Open VPN expose internal tools to security threats

- Prior to 2020, numerous open-source tools to secure their cloud-based Human Resources Management Software (HRMS), lack of consistent application security across virtual machines (VMs), hosts, containers, and Kubernetes.
- Use of open VPN that resulted in lags and latencies, exposing the internal tools to the internet.
- The solution needed to provide them with comprehensive cloud security posture management (CSPM) and ensure cloud workload protection (CWP) with container access control to monitor their cloud accounts and protect the entire application stack.
- Required secure VPN access to prevent internal tools from being exposed to the internet.



We selected Prisma Cloud from Palo Alto Networks, as it was best-suited to our needs and could be deployed across all servers. We gained the benefit of single pane of cloud visibility across multiple cloud environments, while also facilitating integration."

Vinodh Kumar Basavani, Senior Engineering Manager, Darwinbox

SOLUTION

Comprehensive cloud visibility, network security, and secure remote access

Darwinbox began as a cloud-based HRMS, SaaS multitenant application, designed to be agile and flexible. The company needed robust CSPM to secure multiple cloud service providers (CSPs) across six regions: Mumbai, Singapore, Frankfurt, Jakarta, North Virginia, and Eurasia. The security monitoring capabilities of the CSPs were also limited. Collecting logs from 10–15 separate CloudTrail logs and moving it to a centralized location to write alert rules manually was proving to be tedious and cumbersome. Basavani elaborates this further, "We wanted a solution that could immediately integrate all of our cloud accounts, analyze logs in real time and generate all required alerts. With several open source tools, we were mired in tool sprawl and overlapping technologies, making management complicated."

To address the challenge of latencies on account of open VPN, Darwinbox opted for Palo Alto Networks Prisma Access so that different cloud providers could access their internal tools without any risks of security breaches. Basavani explains, "We wanted to have a lot of restrictions for secure access, especially with respect to developer missions and with Prisma Access, we were able to gain protection through the security service layer, in real time, allowing the security operations center or SOC to fix any detected vulnerabilities immediately." Basavani also highlights that Prisma Access deployment was done seamlessly, despite the pandemic. Palo Alto Networks has also ensured that Darwinbox meets with the compliance and regulatory requirements across the six regions where they are present.

90% reduction in tool sprawl

Darwinbox had deployed around 10 different tools such as AWS GuardDuty, AWS CloudTrail with CloudWatch Logs group, CloudWatch Logs metrics and rules, Wazuh, Elastic Search, etc. They have replaced all of these tools with a single tool from Palo Alto Networks, bringing down the tool sprawl by 90%.

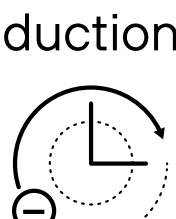
On top of the reduction in tool sprawl, Prisma Cloud has helped Darwinbox improve on their service-level agreements (SLAs)—pertaining to their response and resolution time—that they have with their customers. Darwinbox has also improved their incident management because of the wide range of integrations provided by Palo Alto Networks. As such, there has been an increase in efficiency and productivity as the team is now able to have a consolidated view of their security and security tools.

High-priority incidents reduced to zero

In 2020, Darwinbox had to contend with a high number of high priority incidents: ~1,000, which would require the teams to prioritize and resolve them in a timely manner. Since Palo Alto Networks, this has been drastically reduced to zero.

Compliance reports TAT cut to 30 minutes

Prior to deploying the Palo Alto Networks solution, the generation of compliance reports took between 3–5 days. This has been reduced considerably to 30 minutes and can be easily shared with their customers (upon request). Additionally, there is now greater trust from Darwinbox's customers as they are confident in Palo Alto Networks reputation as a trusted leader in cybersecurity.

Reduction in  Response time **1 min** (from 10 mins on average)

Resolution time **30 mins** (from 1 hour)

Utilized best practice suggestions to reduce alerts from **5,000** → **100** 

Compliance reports generated in **30 mins** (from 3–5 days)

CONCLUSION

Darwinbox had 50 internal tools whose endpoints were on the internet with IP restrictions, prior to Palo Alto Networks. With Prisma Access, they can now deploy all 50 internal tools on their private network, with seamless access through VPN with a complete audit log. They are now also able to secure proprietary code with many customized rules in VPN and are able to integrate different cloud environments. Besides the tangible benefits realized by Darwinbox with Palo Alto Networks solutions, Basavani highlights, "We have witnessed a significant uptick in trust across our customers, because they know that we are utilizing Palo Alto Networks best-of-breed solutions. Our customers know that we now have the best security protocols in place that can keep them fortified."

Find out more about [Prisma Access](#) and [Prisma Cloud](#).



We have witnessed a significant uptick in trust across our customers, because they know that we are utilizing Palo Alto Networks best-of-breed solutions. Our customers know that we now have the best security protocols in place that can keep them fortified."

Vinodh Kumar Basavani
Senior Engineering Manager
Darwinbox

