CASE STUDY

Clariens Reduces Threat Response Time by 81% with Fortinet Cloud Security Solutions

Grupo Clariens is a Brazilian holding company that owns multiple educational institutions specializing in medical training. It has approximately 5,000 medical students and employs 1,200 staff members across its five education institutions, including Zarns, Imepac, and UnesulBahia. Headquartered in São Paulo, Clariens also has its own clinics, serving patients across the states of Bahia, Goiás, and Minas Gerais.

Founded in 2022, Clariens has grown through a series of major acquisitions that significantly expanded its national presence and medical training capacity. The number of medical school seats has doubled since then, and its academic portfolio now includes veterinary medicine, physical therapy, and others.

Complex Environment and Vulnerabilities

Technology and cybersecurity are strategic pillars for the company. Clariens' critical operations require the protection of sensitive data of students, faculty, employees, and patients. It must also safeguard academic and financial records, which are sometimes targeted by phishing, ransomware, and social engineering attacks. Meeting these demands requires a secure infrastructure, strong policies, regulatory compliance, and a culture of awareness and accountability.

Clariens also has a distinctive operating model that shapes its security challenges. The organization has been cloud-native from day one, with all applications running in Azure. In this environment, access to information is distributed across personal devices and shared among multiple stakeholders. "In our Azure environment, everything happens on cell phones and laptops, while several stakeholders can access any type of information at any time," says Thiago Menezes, infrastructure and security manager at Grupo Clariens.

The decision to be 100% cloud-based was both technical and strategic. Working in the cloud allows Clariens to keep all its geographically dispersed premises fully integrated and to build an elastic, expansion-ready operation. It has enabled Clariens to grow rapidly, while introducing new security concerns along the way. "Managing broad, device-agnostic access to sensitive information across a highly connected ecosystem is a challenge. This characteristic significantly increases our exposure to cyberthreats," Menezes shares.

Against this backdrop, it became evident that Clariens required a centralized cybersecurity solution that was not only effective against sophisticated threats but also scalable and capable of providing deep visibility across its operations. Clariens also needed to have complete control over its security infrastructure and reduce incident response time. "We chose Fortinet because it offers great value for our unique needs: scalability, support for a lean IT team, and the cost benefits

Clariens Educação

"FortiCNAPP is fully integrated with FortiAnalyzer and works with our cloud control panel. So, it's continuously monitoring our entire Azure posture, identifying changes that could generate risk as well as providing guidance and flagging software or applications that may have issues, which is very useful for the development team."

Thiago Menezes
Infrastructure and Security Manager, Grupo Clariens

Details

Customer: Grupo Clariens

Industry: Grupo Clariens

Location: Brazil

Business Impact

- Full visibility into Azure cloud posture, identity and access management, and workloads
- Continuous protection for all cloud-hosted academic applications

of consolidating multiple tools into a single vendor, with comprehensive integration and highly efficient security operations," says Camille Miguel, director of technology and innovation at Grupo Clariens.

Achieving Cloud-Ready Performance

To unify protection and secure cloud connectivity across all institutions, Clariens deployed a distributed hybrid mesh firewall architecture based on FortiGate Next-Generation Firewalls (NGFW). The Salvador campus uses a high-availability (HA) pair for uninterrupted uptime, while the remaining campuses and the corporate office each operate a single device. In the cloud, two additional FortiGate VM appliances run in HA to support the organization's Azure infrastructure.

Building on this foundation, Clariens adopted a complete SD-Branch model integrating FortiSwitch Ethernet switches for secure wired access and FortiAP access points for enterprise Wi-Fi, both centrally managed with FortiManager. The company also enabled security analytics through FortiAnalyzer for reporting and critical decision-making.

The additional security solutions immediately delivered significant improvements: They reduced detection time by 98%, cut incident response time by 81%, and lowered alert volume by 82%, even as security events increased by more than 360%, from 63,000 in 2024 to 294,000 in 2025.

With a stable network foundation in place, Clariens extended Secure SD-WAN across seven units and into the cloud on Azure, supported by the FortiGate HA cluster. This upgrade significantly improved performance: "With Secure SD-WAN, our response time and access time to applications improved by around 30%," Menezes says.

Since all major platforms—student, teacher, and administrative portals, plus registrar services, HR, and ERP—run in the cloud, Clariens also deployed FortiWeb. With it, the company could harden its web-application layer and ensure continuous availability across all academic and administrative services.

End-to-End Cloud Security

Even with all these security solutions in place, Clariens felt there were gaps in their strategy. "We still needed to have more visibility, better control, and greater management of everything that happens on our cloud architecture," Menezes says. This analysis led to the deployment of FortiCNAPP, Fortinet's cloud-native application protection platform. "FortiCNAPP is fully integrated with FortiAnalyzer and works with our cloud control panel. So, it's continuously monitoring our entire Azure posture, identifying changes that could generate risks as well as providing guidance and flagging software or applications that may have issues, which is very useful for the development team," he adds.

Business Impact (cont.)

- Standardized security and compliance across all institutions
- 98% reduction in time to detect threats
- 81% reduction in incident response time
- 82% reduction in alert volume
- 30% improvement in response time and access time to applications

Solutions

- Cloud Security
- Network Firewall
- Secure SD-WAN
- SOC Operations
- Secure LAN

Products

- FortiGate Next-Generation Firewall
- FortiCNAPP
- FortiSwitch
- FortiAP
- FortiAnalyzer
- FortiWeb
- FortiManager
- FortiSOAR
- FortiFlex

One area of particular concern is identity and access management (IAM) as roles shift, new systems are added, and units are integrated through the acquisitions. User access permissions can quickly become excessive or misaligned. As part of its comprehensive cloud protection platform capabilities, FortiCNAPP delivers cloud infrastructure entitlement management (CIEM) that allows organizations to easily monitor and address risks with identities and over-provisioning in cloud-native applications and workloads. "With the FortiCNAPP workload protection, we have continuous vulnerability monitoring, something that's essential for an organization growing as fast as ours and needing to deploy changes quickly," Menezes shares.

The change has been significant. Previously, the team had a narrow, vertical view of resources. Now, it has horizontal visibility that spans all units and workloads. This achievement strengthens compliance and enables Clariens to align policies, meet auditing requirements, and standardize access across the organization.

FortiCNAPP has also accelerated threat detection and remediation. "Tasks that previously required hours of manual investigation, such as log searches or event correlation, are now automated and often resolved in real time," explains Menezes.

With FortiCNAPP integrated into FortiSOAR, a solution that is also part of the company's security architecture, this set of alerts, evidence, and indicators is transformed into orchestrated and standardized actions, linking detection, analysis, and response in a continuous flow. This minimizes any impact related to security incidents and reduces response time, which is crucial to keeping Clariens' operations running and its activities flowing.

With automated workflows, each incident is immediately enriched, routed, and handled according to predefined playbooks, from collecting additional data to triggering automatic or semi-automatic responses, ensuring end to end closure.

The combination of these solutions with AI capabilities enhances this process. Even with a lean team, they can prioritize what truly matters, eliminate operational noise, and respond quickly and efficiently to threats. Moreover, adherence to industry frameworks, CIS benchmarks, and cloud best practices further strengthens governance and ensures a consistent security standard across all campuses and cloud assets.

To manage licenses, Clariens chose FortiFlex, which enables the company to dynamically adapt its cloud security stack. The company can scale security services up, down, in or out in response to acquisitions, growth, new workloads, or rapid expansion of medical programs. "One of the great advantages we saw in FortiFlex was the ability to explore different tools and determine which ones truly fit our reality. That flexibility is essential and relevant for us," Menezes highlights.

> "We chose Fortinet because it offers great value for our unique needs: scalability, support for a lean IT team, and the cost benefits of consolidating multiple tools into a single vendor, with comprehensive integration and highly efficient security operations."
>
> **Camille Miguel**
> Director of Technology and Innovation,
> Grupo Clariens

> "One of the great advantages we saw in FortiFlex was the ability to explore different solutions and determine which ones truly fit our reality. That flexibility is essential and relevant for us."
>
> **Thiago Menezes**
> Infrastructure and Security Manager,
> Grupo Clariens

Supporting Growth through Fortinet Cloud Protection

The company is now heavily focused on innovation while advancing an ambitious roadmap of operational efficiency projects. With rapid expansion and new acquisitions underway, the organization is prioritizing AI across medical applications and its internal systems. This plan requires a full review and strengthening of security policies, zero-trust practices, and standardization across all units. As of December 2025, the team had outlined 38 new major initiatives spanning security, infrastructure, and even a complete relocation to a new building.

Clariens also runs a conceptual security awareness program called Clariens Guard, built around multiple engagement initiatives. The program includes a gamified training platform, an internal competition developed with the management team to participate in, and year-end awards. It also features ongoing awareness lectures for employees, students, and teachers, with Fortinet providing significant support as the program continues to evolve.

Looking ahead, Clariens sees Fortinet as a foundational partner. The entire growth strategy, including cloud expansion, M&A integration, and security modernization, already relies on Fortinet technologies. "Fortinet has proven to be far more than a provider; it's a full platform that gives us visibility and consistency, allowing us to scale our operation quickly," says Miguel. "Also, we always have the support of the sales and the engineering teams, which makes a big difference for us."

Clariens has been following a security roadmap jointly defined with Fortinet, progressing from maturity level 2 toward level 4, with the goal of reaching level 5. “In terms of security, we already have a solid foundation,” Miguel concludes. “But we want to evolve more in the autonomous environment. There’s no shortage of improvements and new implementations we can make. And we know we can scale securely with Fortinet.”

March 20, 2026 5:08 PM / CS-141-0-0-EN