NGINX
Part of F5

NGINX
How its open-source roots feed into enterprise cyber defense.

With so many malicious agents out breaching corporate networks and stealing data, information security departments have risen to become one of the most critical branches in IT. Vendors are doing their best to keep up with the threat of cybercrime, however as these security companies move forward and create more advanced protective solutions, the hostile technologies that threaten corporate networks continue to evolve at pace.

To counter the ongoing threat of cybercrime, global security specialist, Exclusive Networks, and its cloud-native subsidiary, Nuaware, helps customers build bundled solutions to defend networks from today's and tomorrow's ever-evolving attacks. Partnerships with other security vendors are the foundation of Exclusive Networks' services and having the right partners and products on-hand gives Exclusive Networks the leverage it needs to produce the best security solutions possible.

Recently, Exclusive Networks, announced its new partnership with F5, a leader in enterprise cloud, and application security and delivery services, who through its own subsidiary, NGINX, is taking on the role as a premiere cybersecurity vendor sitting in the security landscape.

Let's take a closer look at what the Exclusive Networks/Nuaware and F5/NGINX partnership can offer.

f5

EXCLUSIVE
NETWORKS

NGINX, the most used web server on the internet today, surpassed its past and present competition by being more scalable and lightweight. Originally developed to deal with the “C10K Problem”, NGINX was the first server of its kind that could handle thousands of users on a single node. Along with hosting features, NGINX is also used for web proxy services and sits in a middleman role between user endpoints and the server-based services users rely on. Other notable uses for NGINX include load balancing, reverse proxy, mail proxy, and caching services. Eventually becoming its own company, NGINX grew and added other products to its lineup, including the NGINX Unit web application server and the NGINX Controller API management solution.

Now an F5 company, NGINX continues to offer its own catalog of services, adding NGINX App Protect, NGINX Ingress Controller, and NGINX Service Mesh to its product list. The NGINX gives F5 a tried-and-true resource it can integrate into its own products, while also infusing its own F5 capabilities into the NGINX line-up. That same lightweight, yet versatile web server that made such a large impact on the internet now contributes its ability to provide its renowned performance and concurrency to F5’s products, while also adding an architecture that today’s cloud-native businesses could rely on for their web-scale applications. The improvements generated from the acquisition will ultimately include better application delivery services, API management, and security, three pillars that DevSecOps teams need to thrive as businesses continue to move forward to multi-cloud architecture.

For security, F5’s NGINX Controller platform helps DevSecOps watch over and manage APIs. Using workflows and it’s API Management module, Controller helps protect apps from malicious agents by protecting critical touchpoints, such as authenticating and authorizing API clients with API Keys and JSON web tokens, applying rate limit policies, and taking advantage of HTTPS to help protect traffic between the defined group of application servers.

NGINX Ingress Controller protects Kubernetes-based applications from external threats by acting as a gateway that helps protect and manage a cluster’s containers. By using methods like SSL termination, layer 7 routing and load balancing, Ingress Controller can help route traffic from an entry point to the appropriate containers. If scaling within the cluster is needed and the number of containers is changed, Ingress Controller will update the NGINX web server so that the new containers are available to incoming traffic. Additionally, NGINX Plus customers get JWT authentication for single sign-on, session persistence for stateful applications, fast reloads and active health checks of their application environment.

> “**NGINX** is the most used web server on the internet today.”

For mitigating app vulnerabilities in DevSecOps environments, NGINX App Protect integrates critical security controls into application development processes and frameworks. Deployed at scale, the App Protect web application firewall (WAF) provides app-centric security designed to help improve availability while also providing developers the technical security guidelines needed to achieve their goals. App Protect also provides application environments with several protective measures against DoS attacks and can notify DevSecOps of potential usage spikes.

NGINX Service Mesh is a lightweight infrastructure layer that uses the NGINX web server to manage and optimize container traffic in Kubernetes environments. Aside from helping coordinate traffic between the Kubernetes control and data planes, Service Mesh adds an additional security role by ensuring all data on the wire is mTLS-encrypted, protecting sensitive information from hackers. Service Mesh also enables DevSecOps with policy-driven rules that help control traffic flow and inter-service communication.

In a cloud-aware, app-driven world, customers need to find the right cybersecurity products to protect their environments. Now that Exclusive Networks and Nuaware are partnering with F5, these same customers can benefit from the time-proven performance and scalability of F5's NGINX catalog of security products, including Controller, Ingress Controller, App Protect and Service Mesh, as well as from Exclusive Networks and Nuaware's own cybersecurity expertise and resources. To find out how you can better protect your cloud, multi-cloud, app and DevSecOps environments, contact Exclusive Networks.

Contact

Exclusive Networks

distribution_us@exclusive-networks.com