



# Network Firewall Solution Toolkit

# Table of Contents

Industry Insights: Integrated Network Firewalls:  
An Essential Solution for Today’s Distributed Enterprise. . . . . 3

Keep Hackers Off Every Edge . . . . . 6

Checklist: Top Six Recommendations to Improve  
User Productivity With a Hybrid Architecture . . . . . 10

Third-Party Validation. . . . . 12

Customer Success Story: Nuvance Health . . . . . 13

Customer Success Story: Nubank . . . . . 14

Customer Success Story: City of Portland. . . . . 15

Customer Success Story: QIAGEN . . . . . 16



# Integrated Network Firewalls: An Essential Solution for Today's Distributed Enterprise

## What Is an Integrated Network Firewall Solution?

Most organizations lack consistent security and visibility across various segments of their distributed networks, and cybercriminals are using that to their advantage. Because the data center, campus, cloud, and branch environments are interconnected, east-west traffic has increased, allowing a successful breach in one part of the network to quickly spread to others. The most effective way to address this challenge is to deploy the same security in every part of the network, thereby enabling centralized threat correlation and coordinated protection for multiple areas of the enterprise simultaneously. However, the complexities and differences between various network ecosystems can make that difficult.

Network firewalls can be deployed to provide critical NGFW functions anywhere across your network—campus, data center, cloud, FWaaS, and SASE environments—with remote unified management. Using the same operating system creates a single, integrated platform that can span, scale, and adapt to today's dynamic and distributed networks. A unified management console can coordinate protection across IT domains, including corporate sites, public and private clouds, and remote workers. This integrated approach allows IT teams to automate threat detection and response, orchestrate configurations, and enforce policies without investing needless manual hours—especially when the cybersecurity skills gap is already constraining resources.

## The Need for Integrated Network Firewalls

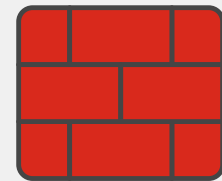
Network firewalls are essential for safeguarding networks from unauthorized access and malicious attacks. They act as digital gatekeepers, monitoring and controlling network traffic to prevent unauthorized access, data breaches, and other security threats. These solutions are designed to address four critical challenges today's IT organizations face:

### 1. IT complexity

Many of today's NGFWs cannot support key capabilities, forcing enterprise IT to purchase separate security solutions for corporate sites, public and private cloud environments, and remote workers. This creates operational inconsistencies, including misconfigurations that can lead to network breaches.

### 2. The cybersecurity skills gap

In addition to complexity, point products add to organizational risk due to their long ramp-up times. Multiple point products increase your cybersecurity IT staff's time learning new features and dashboards. This puts enterprises at even greater risk, as many cybersecurity roles remain unfilled due to the global talent gap.



Fortinet has been recognized as a Leader in the Gartner® Magic Quadrant™ for Network Firewalls for 13 consecutive years and is positioned highest in Ability to Execute in the latest report.<sup>1</sup>

### 3. The rise of advanced threats

Complexity and cybersecurity skills shortages aren't the only factors driving the need for integrated network firewalls. Advanced, sophisticated cyberthreats are rapidly increasing, in many cases thanks to artificial intelligence. These advanced threats are becoming more difficult to detect and are increasingly devastating to businesses. Their attack vectors span the web, applications, content, and devices. Ransomware, for example, continues to disrupt industries across verticals, including operational technology (OT), state and local governments, manufacturing, and healthcare organizations.

### 4. The role of AI/ML and threat intelligence

Complexity, manual oversight, and an expanding threat landscape require coordinated protection. It's not enough that your firewall can span the different areas of your network. They must also contain the artificial intelligence and machine learning (AI/ML) capabilities required to protect against known and unknown threats. Adding AI/ML-powered security to network firewalls enables them to identify and classify applications, web URLs, users, devices, malware, and more, all while automating policy enforcement across domains. AI/ML is at the heart of network firewall automation and can significantly reduce the amount of manual work involved in protecting enterprise IT.

## What to Look for in a Network Firewall Solution for Hybrid Environments

### Centralized and unified management

The most vital benefits of network firewalls are seeing threats, managing policies, and automatically orchestrating responses to threats anywhere across your network using every tool at your disposal.

Unified management coordinates and unifies your domains into a single enterprise IT security solution, enabling simple, automated protection that extends from corporate sites to the cloud and remote workers. Because different organizations have different requirements for managing disparate network firewalls, all form factors must be supported, including appliances, VMs, SaaS, and managed firewall services.

Your network firewall must also bring your network operations center (NOC) and security operations center (SOC) teams together through a single pane of glass to manage and monitor your entire attack surface.

### ASIC-based appliances

Every environment in your network has unique security challenges. Corporate sites require appliances that can scale security functions, ensuring consistent protection without impacting user experience.

Today's performance-hungry organizations need appliances that include enhanced application-specific integrated circuits (ASICs) to increase the speed of critical security services. A security appliance built with a custom ASIC can offload numerous resource-intensive functions, like firewalling, VPN, IPS, and even SSL/TLS or deep packet inspection (DPI). ASICs can significantly enhance the performance of security functions compared to general-purpose processors.

### Cloud-native firewall

Cloud-native firewalls protect public cloud application workloads deployed in IaaS environments as Infrastructure-as-Code. Adding a cloud-native network firewall to your cloud environment also reduces your network security operations workload by expanding visibility while eliminating the need to configure, provision, and maintain a firewall software infrastructure, allowing security teams to focus on policy management.

### Virtual firewall

Virtual firewalls are commonly used to protect virtualized environments in software-defined data centers and multi-cloud environments. Because they are the least expensive and the most portable solution, IT staff can quickly move a virtual firewall from cloud to cloud. The virtual firewalls within a network firewall solution further enable a comprehensive security ecosystem for your software-defined data center, aiding your consolidation process while protecting your environment from threats, using a variety of cybersecurity services beyond stateful firewalling.



### **Firewall-as-a-Service**

Firewall-as-a-Service (FWaaS) is a firewall solution delivered as a cloud-based service. This allows companies to simplify and scale their IT infrastructure. In many ways, FWaaS is much like the hardware firewall you deploy on-premises, providing the full range of NGFW capabilities, like web filtering, advanced threat protection, IPS, and DNS security. A network firewall deployed as an FWaaS solution extends its unique capabilities to distributed users and devices, combining nearly instantaneous scalability with centralized control.

### **A single operating system**


The rapid expansion of network edges has compounded the challenges of vendor and point solution sprawl. Disparate point solutions cannot work together or share information, making consistent security policy, end-to-end visibility, and automation impossible. Trying to maintain and monitor numerous hybrid, hardware, software, and X-as-a-Service solutions also overburdens security teams.

A single operating system consolidates numerous technologies and use cases into a simplified, single policy and management framework. While its unified management console unifies its front-end operations, a single operating system ensures that various deployments, such as appliances, virtual and cloud-native firewalls, and FWaaS agents, can all interoperate on the back end.

## **The Value of Integrated Network Firewalls**

Integrated network firewalls bring enormous benefits to enterprise IT. These include increased IT operational efficiency, simplified cybersecurity operations, reduced organizational risk, relief from the cybersecurity skills gap, resilient protection against known and unknown cyberthreats, automation and coordination via AI/ML, and a lower total cost of ownership.

<sup>1</sup> [A Leader Positioned Highest in Ability to Execute](#), Fortinet, accessed September 13, 2024.

A person wearing a blue hoodie is shown in profile, typing on a keyboard. They are sitting at a desk with multiple computer monitors. The scene is dimly lit with blue and purple ambient lighting. A semi-transparent white box is overlaid on the left side of the image, containing the text 'Keep Hackers Off Every Edge'.

Keep Hackers  
Off Every Edge

## Executive Overview

Today's users need a network that allows them to connect to any resource from any location using any device. At the same time, data center and campus networks must operate in a hybrid IT architecture, working alongside next-generation branch offices, private and public multi-cloud networks, remote workers, and cloud-based Software-as-a-Service (SaaS) solutions. As a result, enterprise security teams are under enormous pressure to provide complete visibility across a moving and distributed network environment to secure and track every user and device accessing data, applications, and workloads. This gives cybercriminals an excellent opportunity to infiltrate your network from the edge. And once they are in, they can wreak havoc.

Unfortunately, most traditional security tools, like legacy firewalls, were not designed for this challenge. They were designed to be static network checkpoints with highly predictable workflows and data. What's needed now is unified network security designed for today's hybrid infrastructure with integrated next-generation firewalls (NGFWs) across the network and form factors, centralized management, and coordinated response to threats. This unification of security needs to protect assets and users located anywhere, converge and consolidate distributed solutions to reduce overhead, simplify management, enable automation, and dynamically scale services and bandwidth to meet your constantly evolving business requirements.

## New Problems

The data center, though essential, is no longer the primary location for corporate applications. Instead, applications can be deployed anywhere. Because a transaction or workflow may span multiple environments and applications, the source, destination, and data path can sometimes change several times, making it impossible to track and secure a transaction end to end.

5G adoption has also left traditional firewalls struggling to keep up, especially when 95% of all traffic is now encrypted.<sup>1</sup> Encrypted traffic, especially secure sockets layer/transport layer security (SSL/TLS) tunnels, is widely used to secure remote access and transactions. However, cybercriminals also use encryption to hide malicious activities, such as stealing company data and secrets and to launch ransomware attacks. Most firewalls cannot decrypt and inspect encrypted traffic without seriously impacting performance and user experience. So, most encrypted traffic, especially data traveling at very high speeds, goes uninspected.

Multi-cloud environments and a hybrid workforce are also rewriting security requirements. The cloud enables agile application development and scale-out/scale-up functionality to accommodate growing application access by remote workers. However, numerous business-critical applications still need to be housed in the on-premises data center for reasons such as compliance, privacy, the need to protect intellectual property, or the need to secure sensitive records. Most traditional firewalls cannot support hybrid data center use cases, including user-to-data center, data center-to-cloud, user-to-cloud, and data center-to-data center interconnect models.

Ultimately, organizations end up creating complex workarounds to get disparate solutions to loosely work together. This is causing the data center infrastructure to become more complex as the number of devices, servers, switches, routers, firewalls, load balancers, and other interconnected components attempt to provide a seamless flow of data between various systems and applications. As the number of devices and the volume of data traffic increases, network complexity also increases, making it more challenging to manage, monitor, and troubleshoot issues.



Though essential, the data center is no longer the primary location for corporate applications. Instead, applications can be deployed anywhere.

## New Solutions

Supporting and securing hybrid architectures requires single-lens visibility across the entire distributed network. This includes knowledge of every user and device on the network and the applications and resources they are accessing. Plus, it's necessary to identify anomalous behavior and malicious activity everywhere. Marshaling all the required security resources to direct a timely, coordinated response is also vital to stopping threats. To support today's expanding networks and their numerous edges, many businesses have begun adopting disparate secure access service edge (SASE), software-defined wide area network (SD-WAN), and zero-trust network access (ZTNA) solutions. This creates complexity while fracturing visibility, compromising user experience, and limiting the ability to respond effectively to attacks.

Integrating NGFWs with these functions can offer both strong defense and network resilience. With centralized management to enforce unified policy in real time, this combination can help mitigate risks from both internal failures and external attacks across all surfaces. Because of its native interoperability, this approach simplifies operations, ensures compliance, reduces complexity, and enables broad automation to increase operational efficiency for today's hybrid business models. It doesn't matter if you have all on-premises firewalls, all cloud firewalls, or a mix of both. The enhanced value lies in centralized and unified management across all firewall deployments.

Fortunately, use cases are remarkably similar regardless of where security needs to be deployed, whether a campus or data center environment, multi-cloud network, branches, or home offices. Addressing them requires breaking down security into three primary functions: protect, converge, and scale. By understanding these three concepts, you can implement a security strategy designed to deliver a seamless user experience and protection aligned with business goals.

## Protect

The main objective is to prevent any threat from entering the network. But if that should happen, the next step is to minimize business disruptions as fast as possible. An NGFW must be aware of the entire application life cycle, including interoperating with tools to accelerate application access and use. This includes providing essential web filtering augmented with advanced image recognition and video content filtering to ensure acceptable use and compliance.

An NGFW solution also needs to provide advanced security solutions, such as an integrated intrusion prevention system (IPS) and anti-malware, to prevent known, zero-day, and unknown attacks. It needs to support constantly shared threat-intelligence feeds from complementary products like email security and sandboxes to detect and prevent the latest threats.

It must also interoperate with other solutions, such as endpoint detection and response (EDR), web application firewalls (WAFs), and other security systems. This combination of native threat protection and integration with other technologies ensures the network is effectively protected against all current and emerging threats.





## Converge

An NGFW should also provide full visibility into sophisticated attacks that hide in secure HTTPS channels to steal data and load ransomware. It should also seamlessly integrate essential networking and security functions into a unified solution, whether delivered directly from an on-premises NGFW or through a cloud-delivered SASE, that combines advanced routing and connectivity functions with dynamic security solutions.

It must also identify any user, device, or application requesting access and automatically assign it to its appropriate network segment. This requires natively integrated proxy services. When a device makes its initial access request, the firewall needs to work with endpoint clients (for users and servers) and network access control (for Internet-of-Things [IoT]/Industrial-Internet-of-Things [IIoT] devices) solutions. It also needs to support multi-factor authentication to determine the role of a user or device, link it to associated policies, and only grant access to the application or segment of the network required to do its job.

For applications and workflows that move from one environment to another, an NGFW must understand, implement, and enforce the same policy everywhere. This consistent orchestration and enforcement approach, built with single-pane-of-glass management, allows security to follow applications, workflows, and other transactions end to end.

For applications and workflows that move from one environment to another, an NGFW must also understand, implement, and enforce the same policy everywhere.

## Scale

Regardless of where a firewall is deployed, one thing remains true: It needs to be fast. And it will need to be even faster tomorrow. Today's data centers generate and process massive amounts of data at transactional speeds, whether it's big data for advanced modeling, low latency for high-speed financial transactions, or hyper-performance for massive multiuser environments.

Speed refers to how quickly a firewall can inspect data and its ability to support automation. An NGFW needs to effectively protect the network from high-speed attacks with advanced and coordinated security and not be bogged down with time-consuming manual provisioning efforts. Manual operations slow things down, and configuration errors can be compromised by ransomware and other attacks.

The challenge is that most traditional firewalls are already running at capacity, which means they can't scale to match growing business demands. That's because they were never designed with hyper-performance in mind. Their biggest problem is they rely on off-the-shelf processors in an age when everything, whether graphics cards, smartphones, or cloud servers, runs on custom chips. Security is a processor-intensive activity. Scaling to meet today's performance demands requires delivering full firewall functionality without sacrificing performance or overwhelming limited IT and security budgets.

## AI-Powered Secure Networking for the Modern World

Firewalls are the first line of defense to keep hackers off the networks. Fortinet's patented security processing unit (SPU), with the industry's only converged security and networking, is a critical component of its AI-powered NGFW architecture, designed to enhance security performance and network efficiency. By leveraging Fortinet's unified security platform, businesses can manage their entire security infrastructure at scale from a single interface, regardless of firewall form factors and deployment locations. This integration approach allows for better coordination and faster threat detection and response across all attack edges.

<sup>1</sup> ["HTTPS encryption on the web,"](#) Google Transparency Report, accessed June 1, 2023.



CHECKLIST

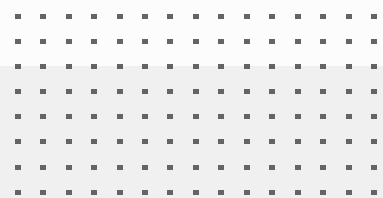
# Top Six Recommendations to Improve User Productivity With a Hybrid Architecture

The speed of business is accelerating the data center’s journey toward digital transformation, requiring new hybrid network architectures that combine on-premise data centers with hybrid clouds. However, to meet the needs of organizations expanding their digital transformation, the underlying enabling technologies must be more reliable, energy-efficient, and secure than ever.

On-premises and virtual data centers are vital pieces in today’s ever-evolving networking puzzle. In this new model, security is essential—not just to protect resources and assets but to enable the network to accelerate and adapt without introducing unknown risks that can jeopardize the enterprise.

Here are six things organizations need to do to position themselves for success.

- 1. Invest in a Flexible Next-Generation Firewall**  
Organizations need to invest in a next-generation firewall that includes technologies like SD-WAN, universal ZTNA, in-line sandbox, and SOC-as-a-Service. These technologies improve WAN connectivity by providing better user experience with direct internet access, while LAN and WLAN provide faster access to local devices and users. In addition, organizations should consider investing in network firewalls that utilize Application-Specific Integrated Circuits (ASICs). They are designed for a specific application or purpose, such as accelerating network security functions beyond general-purpose CPUs.
  
- 2. Deploy Unified Networking and Security**  
Security can’t be an afterthought. When security solutions are not well-integrated with each other or the underlying network, security risks and gaps arise as the attack surface expands and adapts. These blind spots are vulnerable to sophisticated multi-step attacks and are partly responsible for the dramatic rise in successful ransomware attacks. Hence, it is important to look for a unified security framework to deliver automated and reactive security that spans the entire attack surface. Organizations also need to converge their security with networking to protect digital acceleration efforts.
  
- 3. Combining Zero Trust Edge Strategy With Consistent Security and Networking**  
With new network edges being created on-premises and in the cloud, it is critical that the unified convergence of networking and security be available everywhere, combined with ZTNA to enable explicit access for applications and continuous verification of users and devices. This convergence is the heart of a Zero Trust Edge strategy. Also, flexibility in providing this convergence is key in securing digital acceleration for hybrid deployments.
  
- 4. Speed Operations With Centralized and Automated Management**  
The exponential growth of network edges, cloud platforms, and tools can significantly increase operational complexity. Furthermore, poor visibility of and analytics gaps in the network along with tasks performed manually degrade the end-to-end digital experience.  
  
These issues increase the time to configure, manage, and troubleshoot. They also add to operation costs and errors that can cause network outages and reduce flexibility. With centralized and automated management and a dashboard able to span the whole network and security stack, the delivery of network services across their entire life cycle is expedited. Removing manual configuration eliminates a major cause of downtime and security breaches.



## ✓ 5. Increase Visibility With End-to-End Digital Experience Monitoring

Traditional network performance monitoring, IT infrastructure monitoring, and application performance monitoring provide NOC teams with limited visibility. These types of monitoring don't provide the performance insights into critical business applications that customers need. They also severely hinder the visibility that frontline NOC and help desk teams need to resolve issues.

A modern digital experience monitoring platform is required to give your NOC team superior visibility. It allows for the observation of any application, starting from the end-user, across any network, and to the infrastructure the application is hosted on. It can enrich incident management and supply holistic remediation of performance issues.

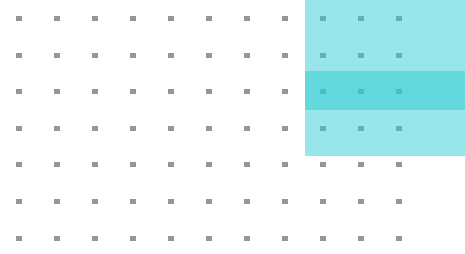
## ✓ 6. Consolidate and Simplify Operations To Provide Instant ROI

Organizations adopting modern networking technologies with integrated security achieve better ROI than point products with limited security. Furthermore, it improves employee productivity with better user experience and simplified operations.

## Conclusion

Many organizations still use a traditional architecture to connect offices to the data center for application access. However, with users working from anywhere and applications distributed across multi-cloud/SaaS environments, this legacy network design is an obstacle for digital acceleration and creates user experience challenges. Organizations that want to have better user productivity and secure network edges need to invest in a modern hybrid network architecture.

Fortinet is the only vendor in the industry to offer an NGFW that includes SD-WAN, universal ZTNA, in-line sandbox, and SOC-as-a-Service that can protect any edge at any scale. Offering the best convergence of networking and security, Fortinet empowers organizations to adopt modern networking technologies essential for digital acceleration. Forrester's [Zero Trust Edge Model](#) validates Fortinet's convergence approach.



**Third-Party Validation**

**September 2023 Gartner® Magic Quadrant™ for SD-WAN**



**Gartner® Magic Quadrant™ for SD-WAN**

Published 27 September 2023

– Jonathan Forest, Naresh Singh, Andrew Lerner, Karen Brown

**March 2024 Gartner® Magic Quadrant™ for Enterprise Wired and Wireless LAN**



**Gartner® Magic Quadrant™ for Enterprise Wired and Wireless LAN Infrastructure**

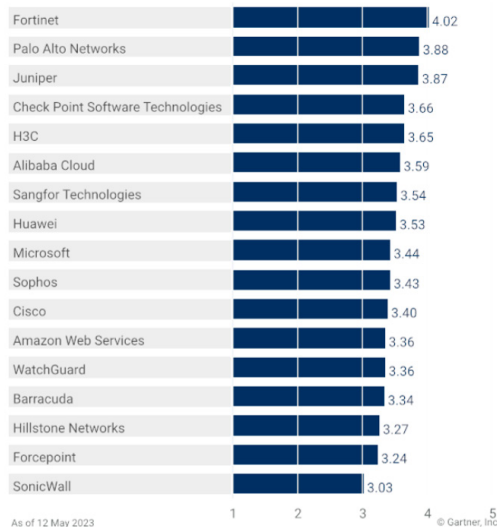
Published 06 March 2024

– Tim Zimmerman, Christian Canales, Nauman Raja, Mike Leibovitz

**Gartner Critical Capabilities**

**Vendors' Product Scores for Enterprise Data Center Use Case**

Product or Service Scores for Enterprise Data Center



As of 12 May 2023

© Gartner, Inc  
**Gartner**

Fortinet is ranked highest for the enterprise data center use case.

**Gartner Peer Insights™ Customers' Choice**



At Fortinet, we strive to put our customers first, and we're very proud to have been named a 2023 Gartner Peer Insights Customers' Choice for Network Firewalls. This distinction, which customers have recognized us for the fourth year in a row, is based on over 500 reviews of our FortiGate Next-Generation Firewalls (NGFWs). In addition to giving FortiGate high ratings, 93% of reviewers are willing to recommend Fortinet NGFWs.

Gartner, Magic Quadrant for Network Firewalls, Rajpreet Kaur, Adam Hills, Tom Lintemuth, 19 December 2022. Gartner, Magic Quadrant for SD-WAN, Jonathan Forrest, Naresh Singh, Andrew Lerner, Karen Brown, 12 September 2022. GARTNER is a registered trademarks and service mark, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved. This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

# Nuvance Health: Fortinet Secures New Hybrid Architecture

## Customer Overview

Nuvance Health re-engineered its network to deploy a secure data center across a hybrid architecture to ensure all information is protected and will deliver a more reliable, energy-efficient, and secure network.

## Challenges

- **Risk management:** reducing exposure to potential attack
- **Cost reduction:** cost-savings requirements after merger
- **Network complexity:** consolidating network management

## Benefits

- Reduced complexity
- Increased visibility
- Increased response speed

## Business Impact

- Saved time for security operations teams with automated processes
- Reduced power usage for operational cost savings
- Improved network management



- A system of award-winning nonprofit hospitals and outpatient healthcare services
- 7 healthcare facilities throughout New York and Connecticut
- 15,000 healthcare professionals
- 13,000 employees

*“Fortinet certainly gives us the ability to reduce the amount of pure network security staff and firewall management staff and allows us to focus other area on other areas [of security] that we have concerns with.”*

**Ben Smith**  
VP, Chief Information Security  
Officer of Nuvance Health

# Nubank Relies on Fortinet Cloud Security Solutions

## Customer Overview

Nubank runs its applications entirely on Amazon Web Services (AWS) and the IT staff is responsible for protecting the customer information residing in the cloud, from both external and internal threats.

## Challenges

- Scale to support growth of company and employees
- Improve internal security
- Protect customer information
- Optimize communication with AWS cloud environment

## Benefits

- Improved network security
- Reduced latency increased time dedicated to higher priority projects
- Improved visibility
- Reduced costs associated with network/security stack

## Business Impact

- Greater reliability and physical security of connected devices
- Better communication with AWS, optimizing the IT team's time
- Improved control over infrastructure, users, and information

## [Read the Case Study](#)



- Largest fintech bank in Latin America, located in Sao Paulo, Brazil
- 6,100 employees
- 90M customers worldwide
- \$1.7B in revenues

*“We were looking for solutions that would support our internal security team and improve communication with our Amazon Web Services cloud environment. In just five months, we managed to reorganize our environment, and we are already thinking about the next steps.”*

**Gabriel Diab**  
Software Engineer,  
Nubank Brazil

# City of Portland Secures Innovative Community Services

## Customer Overview

The City of Portland is pioneering several leading-edge data management initiatives that are designed to better protect its community services against cyberattacks.

## Challenges

- Had inadequate vendor support
- Needed effective protection against DDoS attacks
- Wanted to build a zero-trust network architecture
- Were searching for long-term, strategic partner

## Benefits

- Avoids service disruption with effective, timely protection
- Improved confidence among city leaders that innovative city solutions and services remain secure

## Business Impact

- Built a zero-trust network framework that manages users and application controls for better governance and control
- Simplified operations by automating to avoid manual configurations

## [Read the Case Study](#)



- Oregon's largest city with more than 642,000 residents
- Among the top 30 largest U.S. cities
- Known for being a sustainability-minded city

*"The fewer devices and vendors you use, the fewer passes through the stack where packets could get sidelined. That is why we are all-in with Fortinet."*

**Christopher Paidhrin**  
Senior Information Security  
Officer, City of Portland

# QIAGEN Strengthens Security Across Its Distributed Workforce

## Customer Overview

QIAGEN needed to streamline security and management of its global network and effectively support a more distributed workforce to seamlessly manage and control remote access and endpoint security.

## Challenges

- Needed to replace edge security company-wide
- Required application-aware firewall
- Did not want to “piecemeal security add-ons” to cybersecurity solution
- Wanted to maintain cost structure

## Benefits

- Streamlined management of the Security Fabric
- Reduced latency across the WAN
- Increased network visibility and management
- Integrated a solution of complementary products

## Business Impact

- Minimized brand and competitive risks by protecting crucial intellectual property (IP), financial, and customer data
- Optimized productivity of business users by minimizing latency connecting to the corporate network or internet via VPN

[Read the Case Study](#)



- Molecular diagnostics and applied testing for pharmaceutical research
- 35 offices in more than 25 countries
- 6,000 employees
- \$2.2B in revenues

*“Fortinet has been a fantastic partner, particularly in overcoming the challenges around getting the firewalls installed in certain locations. They went above and beyond in ensuring that we were successful in this major deployment.”*

**Jonathan Martin**  
Director, Global IT Infrastructure,  
QIAGEN



