WE GET NETWORK SECURITY IS JOB SECURITY.

To keep your data and your business safe, you need IT Orchestration by CDW®.

Defending modern IT environments is a complicated task especially as organizations continue to adopt cloud and software-defined technologies that dissolve the network perimeter. Next-generation firewalls inspect all traffic, including all applications, threat and content and tie that traffic to the user, regardless of location or device type.

Next-generation firewalls can help you achieve:

- Intrusion Prevention
- Advanced Threat ProtectionControl
- Application Visibility and Control

Orchestrating the Right Solution

When adopting a NGFW, you should carefully select the product that best meets your organization's security and business requirements, evaluating the following criteria:

Security Functions: to ensure security doesn't impede business results, organizations should not only consider a firewall's key features but also its ability to mitigate risk without slowing down network performance.

- Consideration: Does the solution enhance your network security by safely enabling application and preventing known and unknown threats without getting in the way of business?

Performance: The firewall must scale and adapt to the required throughput of all business needs, both now and in the future.

- Consideration: Will the solution still support throughput requirements if you enable additional security features down the line?
- Consideration: Will you have to compromise on security to maintain or improve performance?

Operations: By opting for a firewall that can automate low-value functions, organizations reduce management responsibilities and free up security staff to focus on high-value activities.

- Consideration: Can the firewall integrate workflow automation, policy automation and security automation to reduce routine tasks?
- Consideration: Does it have the potential to integrate with cloud-native services?

CUSTOMER SUCCESS STORY

Industry: Transportation and Carrier Company

BUSINESS CHALLENGE: A national transportation firm was upgrading the existing internet connections at their primary and secondary data centers. Due to the increase in bandwidth, the customer needed to upgrade their firewalls to ensure secure connections. The customer was having issues with the system updates and user interface of their current solution and was looking for guidance around what other corporations were implementing.

SOLUTION: The customer is implementing Palo Alto Networks 3220 firewalls in both their primary and secondary data center. CDW will provide professional services to support the implementation, configuration and handover of the day-to-day operations.

RESULT: The business results are yet to be determined as we are currently rolling this project out. The customer was very impressed with the consultative approach that CDW took and has engaged with their account team to learn more about our Managed Services practice as their current agreement will expire in a year.

Design
Using tools, data, and years of expertise, we can make specific recommendations for our customers.

Orchestrate
Our expert engineering teams implement the right technology and ensure it works the first time.

Manage
We help customers get the best results from their solution and fully realize the expected value.

CDW PEOPLE WHO GET IT®

WHY CDW

CDW is a trusted adviser that:

- Provides peace of mind through sophisticated hardware, software and services
- Offers a highly skilled security assessment team that can rigorously test customers' cybersecurity, help them understand where and why they're vulnerable, and prioritize their needs
- Consults with customers to create the appropriate strategy, toolset and coverage for their needs
- Delivers proven cybersecurity solutions backed by our experience in thousands of engagements

Solve Business Challenges With NGFWs

Defending modern IT environments is a complicated task especially as organizations continue to adopt cloud and software-defined technologies that dissolve the network perimeter. Next-generation firewalls can help solve business challenges by protecting the extended perimeter and delivering advanced security capabilities.

Business Priority	Solution
Identify Users and Enable Appropriate Access	Your next firewall must be able to pull user identity from multiple sources. Knowing who is using the applications on your network, and who may be transmitting a threat or transferring files, strengthens security policies and improves incident response times.
Safely enable applications and control functions	Your next firewall must classify traffic by application on all ports, all the time. The firewall must provide complete visibility into application usage along with capabilities to understand and control their use.
Detect and Prevent Advanced Threats	Your next firewall must identify evasive techniques and automatically counteract them with advanced threat prevention technologies enabled through a single, unified engine.

CONSIDERATIONS FOR ADOPTION

Before adopting a NGFW solution, organizations should answer the following questions to help determine the best solution for their needs.

1. Does the solution enhance your network security by safely enabling applications and preventing known and unknown threats without getting in the way of business?
2. Will the solution still support throughput requirements if you enable additional security features down the line?
3. Will you have to compromise on security to maintain or improve performance?
4. Can the firewall integrate workflow automation, policy automation and security automation to reduce routine tasks?
5. Does it have the potential to integrate with cloud-native services?

Partners Who Get IT

Check Point SOFTWARE TECHNOLOGIES LTD.

CISCO Partner

FORTINET

paloalto NETWORKS

SONICWALL

To learn more about Next-Gen Firewalls, contact your CDW account manager at 800.800.4239 or visit CDW.com/security.

CDW PEOPLE WHO GET IT