SOFTWARE-DEFINED SECURITY

/ **Businesses are faced with a never-ending barrage of cyber threats. Hackers and the threats they create are becoming increasingly sophisticated, widespread and damaging.** Emerging trends like the Internet of things and machine learning as well as more established sources of risk like virtualization and BYOD only exacerbate the problem, serving as enticing targets for those looking to inflict harm.

/ **Any breach can compromise your network, data and your business.** Companies that succumb to threats can suffer dire consequences. But fending off security threats is no simple matter. A cohesive security strategy requires a robust combination of sophisticated technology and security expertise.

SAFEGUARD YOUR NETWORK

A critical step in maintaining a safe network environment is implementing a next-generation security solution capable of keeping up with the ever-changing threat landscape. Using Nitel's integrated SD-Security and Unified Threat Management along with SD-WAN protects your network from the most sophisticated threats.

Delivered on the same hardware as Nitel's SD-WAN solution and with the ability to recognize over 2,600 applications out of the box, deployment and management are simple. Nitel's SD-Security receives updates in near real time to ensure it can prevent against the ever-growing list of threats.

Through the same centralized management portal as your SD-WAN environment, you will safely enable applications, users and content while preventing external threats and protecting your company's data.

INTEGRATED SECURITY STREAMLINES DESIGN AND LOWERS COST

Through Nitel's virtualized network and security platform, every one of your sites—branches, headquarter locations, data centers and others—are protected. Without deploying additional premise equipment specifically for security, you reduce cost and complexity, remove points of potential failure and avoid integration issues with other network components.

Simple Management:
With single-pane-of-glass visibility into your network performance and security environments, Nitel takes the mystery out of ensuring your business is getting the most out of its wide area network.

Service Experience:
With a dedicated team of empowered experts behind you at every step of your journey, you're always a phone call away from finding answers. We'll manage every process with a microscope so you don't have to, and offer a flexible approach to keeping you informed.

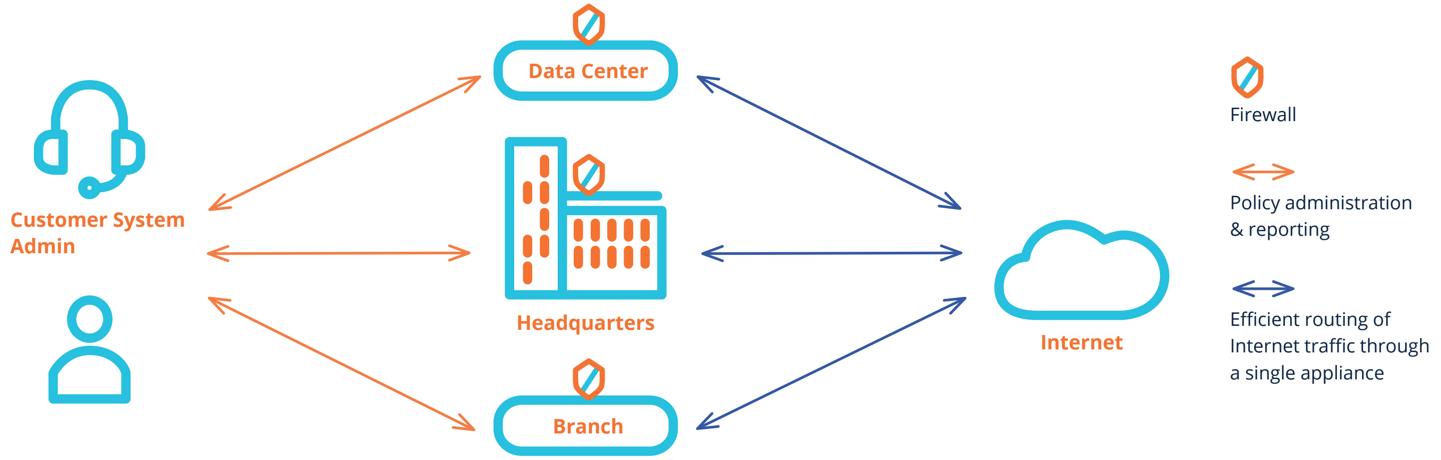
Smarter technology made **simple**

nitel

DE-CENTRALIZE SECURITY TO ELIMINATE BOTTLENECKS

Networks are commonly designed to route all Internet traffic through a common firewall to reduce network complexity and simplify administration and reporting. However, as companies continue to adopt cloud-based applications and resources, more and more traffic is destined for the Internet. Where companies employ a centralized firewall, this can cause a bottleneck, which affects performance and user experience.

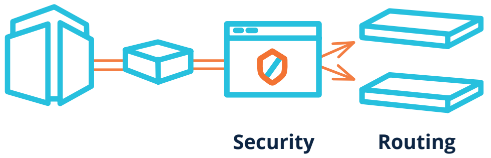
Separating the control plane and data plane in Nitel's SD-Security solution allows security policies to be created and managed from a centralized location but carried out at each individual location. This provides a path to the Internet at each location, alleviating bottlenecks and enabling the most efficient routing of all traffic.


Data Center
Customer System Admin
Headquarters
Internet
Branch
Firewall
Policy administration & reporting
Efficient routing of Internet traffic through a single appliance

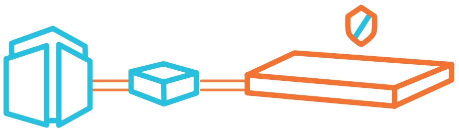
Centralized policy administration and reporting simplifies management of the security environment and alleviates traffic bottlenecks caused by routing Internet traffic through a hub.

SIMPLIFY NETWORK DESIGN

Without Nitel SD-WAN



Nitel SD-WAN with Integrated Security



Best-available routing, next-generation security and unified threat management

With a Nitel SD-WAN solution with integrated next-generation firewall and UTM, you improve network performance, resiliency and security while simplifying network design and reducing the number of appliances you need to manage.

HIGHLIGHTED NEXT-GENERATION FIREWALL FEATURES

Application Control:
Create policies to allow, deny or restrict access to applications or entire categories of applications.

User and Group Definition and Control:
Enable policies to be carried out across specific groups that you create.

SSL Inspection:
Check for expired certificates; untrusted issuers; unsupported ciphers, key lengths or version; restrict certificate extensions.

IP, URL and DNS Filtering:
Filter traffic based on the reputation and geographic location of the source and/or destination IP addresses, URL and DNS. Supports user-defined black and white lists.

HIGHLIGHTED UNIFIED THREAT MANAGEMENT FEATURES

Intrusion Detection and Prevention (IDS/IPS):
Real-time protection via vulnerability signatures and anomaly detection engine. Supports custom user-defined vulnerability signatures.

Multi-layered Anti-virus and Anti-malware Protection:
Detection includes heuristics, emulation and signatures across http, ftp, smtp, pop3, imap and mapi protocols.

File Reputation and Filtering:
Signature-based file type identification and application, file type, direction and size-based filtering. Supports user-defined black and white lists.

SSL Decryption:
Obtain traffic visibility by decrypting outbound & inbound SSL traffic, inspecting decrypted traffic for threats and re-encrypting to both client and server.