

# MANAGED NEXT-GENERATION SECURITY SOLUTIONS

## / WHAT KEEPS LEADERS UP AT NIGHT

For business leaders everywhere, a data breach is on par with the most damaging things that could happen to an organization. The thought of being the next company to make headlines keeps leaders up at night while IT organizations fight to keep the bad guys out. As threats become increasingly widespread, sophisticated and dangerous, companies look to develop security strategies that protect their environment while staying within budgets that seem to get tighter every year.

## / CUSTOMIZED MANAGED FIREWALL SOLUTIONS

Your business is unique, with its own set of needs and priorities. That's why we offer a suite of security solutions that offers multiple ways for you to protect your business. Whether your business is big or small, whether you value distributed architecture or centralized, you'll find a solution that fits how you prefer to manage your environment.

### ENTERPRISE GRADE PROTECTION

- Safely enable applications, users and content by classifying all traffic, determining the business use case and assigning policies to allow and protect access to relevant applications.
- Prevent threats by eliminating unwanted applications to reduce your threat footprint and apply targeted security policies to block known vulnerability exploits, viruses, spyware, botnets and unknown malware (APTs).
- Protect your data centers through the validation of applications, isolation of data, control over rogue applications and high-speed threat prevention.
- Secure public and private cloud computing environments with increased visibility and control; deploy, enforce and maintain security policies at the same pace as your virtual machines.
- Embrace safe mobile computing by extending the enterprise security platform to users and devices no matter where they are located.

### DISTRIBUTED ARCHITECTURE, CENTRALIZED CONTROL

With Nitel's software-defined security (SD-Security) platform, customers with distributed networks avoid traffic bottlenecks at hub locations. 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 site. This provides a path to the Internet at each location, alleviating bottlenecks and enabling the most efficient routing of all traffic.

### ROCK SOLID PROTECTION FOR SMB

Our customized solutions deliver next-generation security for every size and type of business. Gain full control and visibility of application traffic passing through your network, even for encrypted traffic, thanks to application detection, user-identity awareness, SSL interception and built-in live reporting.

You benefit from the same critical next-generation security features that large enterprises receive—but sized appropriately for your business. Your business will fend off threats with included next-gen features that take place directly in the data path, including:

- Firewalling
- Intrusion detection and prevention (IDS/IPS)
- URL filtering
- Dual anti-virus
- Application control

**Includes unlimited site-to-site and client-to-site VPN capability.**

#### Enabling Your Move to the Cloud

Seamless integration with the following infrastructures:

- Microsoft Azure
- Amazon AWS
- Google Cloud Platform
- VMware vCloud Air



## / SECURITY EXPERTISE ON YOUR SIDE

Nitel has partnered with Gartner Magic Quadrant leader Trustwave to complement our managed next-generation firewall service with a suite of security management services. This 1-2 punch creates a comprehensive managed security solution to reduce your business risk and give you peace of mind. With Nitel overseeing your network health, performance and security, you have a single partner working on your behalf to ensure your business operates optimally and safely.

### SECURITY INFORMATION EVENT MANAGEMENT

Achieve more effective identification and mitigation of security threats. You'll reduce your burden with around-the-clock support from 10 global security operations centers staffed with experts who have in-depth knowledge and experience working with complex network environments for highly distributed organizations.

Our SIEM service collects, analyzes and stores logs from networks, hosts and critical applications. It extends visibility beyond the network perimeter to the application layer, helping you achieve more effective identification and mitigation of security threats, and compliance validation with numerous regulatory and industry standards.

#### Advantages:

- SpiderLabs security research utilizing global event data to identify current and emerging threats
- Industry-leading compliance expertise
- Solutions tailored to the specific needs of healthcare, financial, retail and more
- Collects and reviews over 1 billion events per day

### MANAGED SECURITY TESTING

Reveal potential vulnerabilities in your environment with thorough penetration testing. Expert "ethical hackers," armed with the same techniques as today's cybercriminals, attempt to hack into your network or application to help you identify network-connected assets, learn how those assets are vulnerable to attack and understand what could happen if those assets were compromised.

Need to maintain compliance with PCI, DDS, HIPAA, SOX, FISMA, GLBA/FFIEC? Let Nitel help. We'll help you fulfill your requirements for vulnerability scanning, penetration testing and ongoing evaluation of your environments and applications.

#### Four Levels of Testing:

As we learn more about your databases, network and applications, Nitel will help you determine an appropriate level of testing to suit your needs.

#### Basic:

Simulates the most common attacks, typically using freely available, automated attack tools.

#### Opportunistic:

Includes opportunistic attacks executed by skilled attackers seeking easy targets, using a mix of automated tools and manual exploitation to penetrate targets.

#### Targeted:

Simulates targeted attacks from a skilled, patient attacker that has targeted a specific organization. Expends significant resources trying to compromise systems.

#### Advanced:

Simulates an advanced attack executed by a highly motivated, well-funded, extremely sophisticated and unrelenting attacker.

Smarter technology made **simple**