ENTERPRISE SECURITY | TOP 10 FIREWALL SOLUTION PROVIDERS 2017

From software that secures terminals, to state of the art hardware barriers between local and external networks, the concept of the firewall has broadened over time—in terms of both technology and definition. With cyber-infiltration lurking at every corner it is becoming increasingly important for companies to be as invulnerable as possible. Malware in worm or Trojan forms can squirm their way into servers, as was the case with the recent WannaCry attack, and so with the advent of application layer filtering, deploying deep packet inspection for intrusion prevention, lends unprecedented levels of security to the enterprise class. In the line of hardware, it is important to note that simply fortifying the network at one device isn't enough—the focus must be shifted to formulating a holistic strategy that integrates every device on the network to become a point of defense.

The connected world of today is enclosed by a fabric of networks. Needless to say, avalanches are triggered by single snowflakes, and in establishing market dominance in firewalls, competitors are constantly innovating to define more niche and air-tight solutions around security concerns, striving to avert infiltration.

For this edition of Enterprise Security magazine, a distinguished panel comprising of CEOs, CIOs, analysts and our Editorial Board has reviewed companies with a proven record of expertise in firewall space. In our selection we looked at companies' ability to identify client requirements, develop strategic approach and provide support and customization through their offerings. We present to you the 'Top 10 Firewall Solution Providers 2017.'

Top 10 Firewall Solution Providers 2017

Company	Management	Description
Check Point Software Technologies [NASDAQ:CHKP] San Carlos, CA checkpoint.com	Gil Shwed Founder and CEO	The Check Point Infinity offering effectively knits through the cloud, mobile and network environments to deliver a cyber security strategy that caters to business needs both policy wise and in terms of scalability
F5 Networks Seattle, WA f5.com	François Locoh-Donou President and CEO	The company's Big IP Advance Firewall Manager (AFM) provides attack visibility and intellignece and as well combines with other BIG-IP solutions to strengthen and unify security capabilities
Fortinet [NASDAQ: FTNT] Sunnyvale, CA fortinet.com	Ken Xie Founder, Chairman of the Board, and CEO	FortiGate next generation firewall (NGFW) platforms are powered by dedicated FortiOS and custom Security Processor (SPU) for performance optimised security
IT Solution Singapore itsolution.com.sg	Lawrence Chai Director	The company is committed to easing workloads by providing various IT needs and enhancement solutions in an innovative way
McAfee Santa Clara, CA mcafee.com	Christopher D. Young CEO	McAfee offers a consolidated and integrated platform for endpoint defense that leverages a single agent architecture with deep integration and automation capabilites
Securcloud Hamburg, Germany securcloud.com	Dennis Monner CEO Felix Blank Senior Product Manager	Provides firewall-as-a-service to SMBs and mobile and household networks
Skybox Security San Jose, CA skyboxsecurity.com	Ravid Circus Vice President, Products	Provides automated, next generation firewall management across physical, multi-cloud and industrial networks
WatchGuard Seattle, WA watchguard.com	Prakash Panjwani CEO	The company's approach to network security combines Next Generation Firewall (NGFW) with Unified Threat Management (UTM)
Waterfall Security Solutions (Rosh HaAyin, Israel) Ashburn, VA waterfall-security.com	Lior Frenkel Co-founder and CEO	Provides an evolutionary alternative to firewalls in industrial network environments
Zscaler San Jose, CA zscaler.com	Jay Chaudhry Founder and CEO	The Zscaler Cloud Firewall enables secure local internet breakdowns without appliances. The offering brings next-gen firewall controls across locations, ports and protocols

IT Solution
Comprehensive Infrastructure Security

As vulnerabilities increase and the sophistication of infiltrators grows, even state-of-the-art firewall systems are not adequate. There needs to be a mix of a robust network, flawless backup policy solution, enhanced maintenance, and round-the-clock monitoring to reduce network vulnerabilities. A Singapore-based managed IT services company, IT Solution, is more than just a firewall expert; it is a one-stop IT solution provider that best serves customers through unique security solutions. "With today's evolving threats, a mere firewall is not the go-to solution; organizations need a comprehensive solution," says Lawrence Chai, Director of IT Solution. "We guarantee the highest level of security that will protect any network and system against viruses and ransomware attacks."

IT Solution's offerings protect any user and device, regardless of the location, as long as they are connected to a network. Chai understands that training is essential to keep employees up to speed as well as ensure that businesses stay safe. "We train and empower any organizational staff with the knowledge of cyber security so that they can recognize common cyber threats and warning messages." IT Solution prioritizes applying rules to network traffic to ward off threats that may interfere with systems, from networks to mobile devices. In addition, Chai's team provides the most comprehensive security coverage—which can be tailored to meet specific client needs—with security features that go beyond the capabilities of a firewall.

> We guarantee the highest level of security that will protect any network and system against viruses and ransomware attacks

Chai states that many firms do not really have the knowledge or experience to activate all the firewall features or implement them correctly. To this end, IT Solution provides a broad array of firewall and antivirus solutions to tackle and protect systems against malware, virus, and ransomware, including automating processes and ensuring all of a client's devices are up to date. The company offers expert guidance in installing and setting up a firewall to ensure that networks are well protected.

IT Solution assists clients to install and assume appropriate IT policy and standard operating procedures to reduce the potential risks of cyber attacks. "We encourage clients to engage our full managed services through which we can have complete information on network usage. This ensures our ability to cover all the loopholes that may exist," adds Chai. In an example, a customer had lost all their data during a ransomware attack and was helpless since their previous service provider had not recommended them to set up a backup system. IT Solution's expert team assisted the client in enhancing their firewall and implemented an automating backup solution with on site and off site backup features to prevent the occurrence of data loss in the future.

Daniel Lim   Lawrence Chai

IT Solution strives to provide state-of-the-art security services to clients with latest firewall technologies and help more SMEs with their cost-effective firewall solution that protects clients against any ransomware attack. Moreover, designed to search, detect, identify, and remove malware programs and other types of malicious software like Trojans, worms, and adware, IT Solution's antivirus products offer users superior protection against web related threats. Not following the clichéd route of offering clients a one-size-fits-all solution, the company provides flexible packages that result in the implementation of the right solution that suits customer needs and complexity of the network. "To us, nothing is more important than helping SMEs grow because IT security is one of the top priorities for organizations that want to scale new heights," concludes Chai. ES

CIO Only Until the Next Data Breach

By Bob Fecteau, CIO, SAIC

Bob Fecteau

Today's chief information officers (CIOs) operate in digital environments that are riddled with cyber threats, and they face a daunting new reality: The next cyber-attack against their company, and the public's reaction to it, could make or break their careers.

Hype versus Reality: Cyber security is no doubt a significant global challenge, but I question whether we are expecting too much from our IT professionals and are not properly supporting them. With the public moving toward a zero-fault position, cybersecurity has become an overwhelming focus for CIOs– and increasingly for chief executive officers, chief finance officers, boards of directors, and shareholders. A view is emerging that protecting a company's data from intrusions, breaches, and viruses falls squarely on the CIO and his or her team. Nothing could be further from the truth. It is a total team effort that must become part of an organization's DNA.

During the recent cyber-attack against the U.S. government's Office of Personnel Management's data systems, the public criticized OPM for compromising the data of millions of active and former government, military, and contractor personnel. Critics were quick to point fingers, but failed to recognize the challenges associated with securing this type of data in an increasingly complex digital world.

As the House Oversight Committee grilled OPM Director Ms. Katherine Archuleta over exactly how many records were compromised (ranging between 14 million to 20 million), the complexity of the challenge was missed. The truth is, it does not matter how many records are compromised. A single record breached is too many and CIOs work diligently every day to ensure data is as secure as possible.

The focus should not have been on numbers, but how the breach was dealt with. When security is compromised, CIOs and their teams have to act fast, smart and decisively with prepared and tested remediation plans that safeguard those affected, ensure a resolution, and protect other areas that could also be vulnerable to the now known threat. Leaders at all levels must know these plans and procedures and be ready to execute them in these situations. Ms. Archuleta, who had held her post for 17 months, was not able to do that. Demands for her resignation came quickly, demonstrating how vulnerable leaders are to a cyber-event.

Perfect Storm: Unfortunately, no matter what Archuleta did or how much taxpayer money she dedicated to securing OPM data, she may not have been able to prevent the attacks on these systems. Anything short of disconnecting the systems from outside networks would not have prevented this attack by a sophisticated adversary. The OPM breach occurred over a period of more than a year before it was discovered. If this attack was state-sponsored, as has been alleged, the chances of initial detection a year ago may not have been possible given the state of sensor technology and signature recognition at the time. In this case, some of OPM's legacy systems are so old that just keeping them patched and