

FOR ZENETH TECHNOLOGY PARTNERS, THE SIEM APPROACH IS THE RIGHT APPROACH



"I have had hands-on experience with the best-known SIEMs over an extended period of time, and the FortiSIEM clearly stood above all of the other solutions."

*– Peter Clay, principal and founder,
Zeneth Technology Partners*



DETAILS

CUSTOMER: Zeneth Technology Partners

INDUSTRY: IT Security Services

LOCATION: Virginia, United States

BUSINESS IMPACT

- Efficiency and effectiveness create happy clients and enthusiastic prospects
- Ability to embrace even the most diverse client environment
- Enhanced time-to-value through ease of use and flexibility
- Combined NOC/SOC capability increases value to customers
- Heightened efficiency of support teams – more effective and more profitable
- Unique IT/OT/IoT capability provides pivotal business opportunity

SOLUTIONS

- FortiSIEM

Based in Arlington, VA, Zeneth Technology Partners provides information security, critical program management, and application-focused services and solutions to federal and commercial clients. Since being launched in 2005, notable customers have included the Department of Defense, and several federal civilian agencies. The company also serves mid-sized organizations in the private sector with average annual sales typically between \$100M - \$1B. Zeneth has continually prevailed in competitive situations against the largest consulting organizations in the country.

MANAGED SECURITY SERVICES EXPANSION

To further complement its growing portfolio of managed security services, Zeneth identified the opportunity to offer clients the capabilities of a full-featured security information and event management (SIEM) platform. A well designed SIEM tool is a solution able to consolidate disparate security-related technologies – such as firewalls, intrusion prevention, endpoint protection, etc. – into a single, integrated view across a company's overall IT security infrastructure.

Members of the Zeneth team conducted an in-depth analysis of the SIEM marketplace and refined its shortlist of candidates down to two contenders. Zeneth Technology Partners' founder and industry veteran, Peter Clay, recalled, "I have had extensive hands-on and implementation experience with the best-known SIEMs over an extended period of time and the FortiSIEM clearly stood above all of the other solutions. We were able to configure everything we needed for three thousand endpoints at less than half the cost of the nearest competing product."

He continued, "During our testing we found the FortiSIEM to be very simple to install and it has the broadest selection of fully-functional prebuilt connectors that I have seen. Other vendors claim to have working connectors but they don't function as advertised. This is a key reason why FortiSIEM is such a valued element of the Zeneth managed service solutions."

NOT ALL CONNECTORS ARE CREATED EQUAL

The large variety of working connectors equips Zeneth with the ability to rapidly deploy FortiSIEM capabilities into the most diverse client environments without requiring time-consuming customizations. “I can swiftly tie a FortiSIEM solution into wherever my customer’s data is located and however they’re consuming it, to immediately provide effective protection,” noted Clay. “The speed of implementation and ability to quickly become operational make a strong contribution to our ability to differentiate ourselves in a highly competitive marketplace.”

“With information security problems, it’s a myth to think there is a single indicator of something going wrong,” mused Clay. “But because FortiSIEM is able to take input from so many diverse sources and then rapidly create a context within which to correlate the information, it’s far more accurate and insightful than its competitors.”

INTUITIVE AND EFFECTIVE

With the widely acknowledged global shortage of security professionals, training and retaining skilled resources has become very challenging. “The FortiSIEM is extremely intuitive and easy to learn,” commented Clay. “We have people operationally proficient with a week of formal training and a week of shadowing. The cost benefit to us is enormous.”

The level of detail from FortiSIEM – and the speed with which it is made available – positively benefits productivity because Tier 1 team members can start the hunt process very early in the cycle. “When we do have to escalate a case to our Tier 2 personnel – the guys whose time we have to guard even more closely – a lot of the data-gathering work typically needed to take decisive action already has been done. This provides both job satisfaction and efficiency,” affirmed Clay.

BREAKING DOWN TRADITIONAL BARRIERS

Another key feature that sets FortiSIEM apart from its counterparts is the ability to manage functions typically handled by network operations centers (NOCs). Combined with its own rich security operations center (SOC) functionality, the “NOC/SOC” pairing provides significant value for Zeneth and its customers. “Our clients have a surprising amount of what traditionally might be considered as the responsibility of a network team – endpoint management, patching, etc. – but we are very comfortable taking on the dual role because of the FortiSIEM’s ability to consolidate both sets of functionalities under a single pane of glass,” Clay emphasized.

The FortiSIEM toolkit helps Zeneth create customized rules for its customers. “Each customer has a unique set of circumstances and we can tailor the FortiSIEM to accurately address any necessary internal or external mandates,” Clay stated. “FortiSIEM enables us to tell clients very quickly when they are straying from any applicable federal or industry requirements.”

IT, OT AND IOT – IT’S ALL THE SAME TO FORTISIEM

The flexibility of FortiSIEM applies beyond the traditional boundaries of an information technology infrastructure and is enabling Zeneth to push into new areas of potential business. “We’re starting to get traction in the operational technology [OT] domain too,” Clay noted. “FortiSIEM is capable of integrating industrial control systems and IoT technologies with more conventional IT environments. Being able to utilize FortiSIEM to manage the security of IT, OT and IOT components under a single unifying pane of glass is extremely exciting for us.”

SIMPLE BUT SOPHISTICATED

Clay concluded, “I’ve been incredibly impressed to see what Fortinet has done with the FortiSIEM solution and I’m stunned how well it’s integrated across the entire Fortinet Security Fabric. We are making our name by offering robust, end-to-end solutions and FortiSIEM is a big part of what we deliver.”



GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990