ENTERPRISE
SECURITY

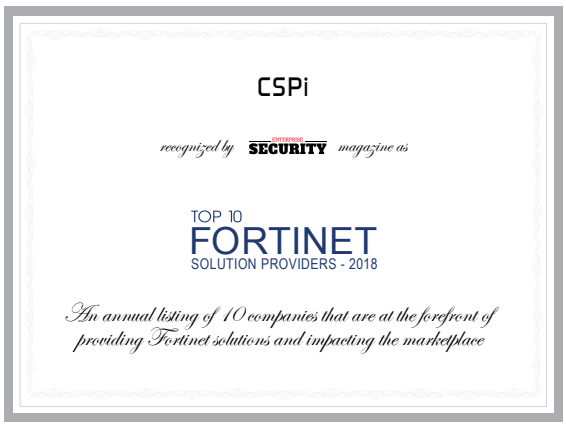
FORTINET SPECIAL APRIL - 15 - 2018 WWW.ENTERPRISESECURITYMAG.COM

Top 10 Fortinet Solution Providers - 2018

Even with all the security measures in place, it is high time for enterprises realize that cybersecurity is not an aspect that should only be confined to cyber specialists. Instead, it has widened to involve personnel at all levels along with new technologies that are emerging. Up-to-date knowledge and awareness of the threat environment and the understanding of the decision makers regarding the cyberspace environment are indispensable factors towards achieving cybersecurity. The vulnerability of cyber attacks have increased exponentially over the last decade with number of companies relying on IT solutions across industries.

In order to counter such threats and to protect customers from losing their valuable and sensitive data, Fortinet solutions provide high-performance network security offerings that can be deployed across any network environment irrespective of the size and nature of the business. For instance, Fortinet's Cloud-based cyber security platform covers end to end solutions along with plethora of product categories such as SD-WAN, Next Generation Firewalls and proactively monitors threats by keeping the perpetrators away. Fortinet has an extensive network of partnership with other organizations to provide security, networking, and management solutions and enhance security deployments.

To counter today's security issues, both large organizations and SMBs should shift their focus from corrective to preventive measures. For this, indentifying the right solution provider capable of leveraging Fortinet's powerful stack to deliver customized solutions is imperative. In response to such needs and demands for cybersecurity, a distinguished panel comprising of CEOs, CIOs, VCs, and analysts including Enterprise Security Magazine's editorial board reviewed the top solution providers in the domain, and shortlisted the ones that are at the helm of tackling the dynamic challenges of cybersecurity for the enterprise security markets industry. We present to you the "Top 10 Fortinet Solution Providers – 2018," offering a glance at tailor-made and efficient solutions for cybersecurity.



Company:
CSPi

Description:
Help customers meet some of computing's most demanding performance, compliance and security challenges

Key Person:
Gary Southwell,
General Manager,
Cybersecurity Division

Website:
cspi.com

CSPi

True PII Breach Detection

The cure to any ailment begins with proper diagnosis, be it in medicine or cybersecurity. The 1,400 reported breaches in the U.S. last year are grim reminders of the sad state of affairs in properly protecting PII. In most cases, it takes over two months for organizations to figure out that they have been breached—let alone which PII/PHI data records were actually exposed. The right diagnosis then is what helps victims uncover the underlying ailment; this is where CSPi has positioned its unique value proposition.


Gary Southwell

Why does detecting a PII breach present such a challenge? Daily the average organization, according to industry reports, is faced with over 5,000 cyber threat incidents, making the task of identifying actual breach incidents daunting. Quickly understanding and pinpointing the aftermath of an identified PII data breach is especially important, as companies that have lost valuable customer records must pay fines if they don't report the incident to the relevant authorities within strict deadlines, including naming the citizens whose records were exposed.

> "We actively utilize the Fortinet API, which allows our system to identify breached PII records in our client systems"

CSPi takes a different approach to diagnosing a breach—"we actively record all data going to and from databases and file shares storing PII data. If those systems have been breached, organizations can search the conversations and locate the exact exposed records. To automate the process, CSPi works with Fortinet's FortiGate ingesting the firewalls and IPS's threat alerts. We actively utilize the Fortinet API, allowing our system to access FortiManager to pull relevant alerts into our solution and run automated searches of bad actors communicating with the monitored and recorded assets," states Gary Southwell, GM at CSPi. In the event of a verified breach, CSPi automatically extracts a file, or detailed report, from the recording, presenting the entire conversation the bad actor is having with the database, and identifies the actual records that were exposed. This provides the vital forensic evidence required to properly report the breach. Another benefit is the recoded data can be replayed through the application to prove if the records were effectively protected by encryption. If so, breach notification is not required, but the extraction files must be saved as evidence.

Here is a real-life use case, a metro healthcare center with 19 clinics was breached. They brought in a third-party incident response company who couldn't narrow down the actual records exposed, after billing $180,000. CPS, however, instructed that by adding a FortiGate IPS coupled with CSPi's Myricom appliance, would provide an effective means to detect the details of a breach, for under $90,000 and pays for itself on the first breach. In this case—recreating the breach circumstances with the Fortigate and CSPi solution—took a total of ten hours to get the extraction files, review it all, and pinpoint which records were exposed, all while the customer was shown how to use the system.

CSPi has subsequently introduced the ARIA Software Define Security (SDS) platform, which automatically encrypts data at the application level. CSPi inserts an agent inside the application making it easy to add encryption during the development process. Addressing another prevalent issue, CSPi has invented an intelligent network adapter with the processing power to run encryption functions within the NIC, this offloads these intensive process from running on server cores thereby allowing encryption to be effectively deployed on any installed legacy system. ES