FORTINET.

Address: 899 Kifer Road
Phone: +1-408-235-7700
Email: securehealth@fortinet.com
Website: **www.fortinet.com/healthcare**
Twitter: @FortinetHealth
LinkedIn: **Fortinet**

Ryan Witt, Vice President and Managing Director, Healthcare Industry Practice, WEDI Privacy and Security Workgroup co-chair, provided the following responses for this WEDI Member Spotlight.

Please share some history about your organization. How did it begin?

Fortinet was founded in 2000 by Ken Xie, the visionary founder and former president and CEO of NetScreen -- an Internet security company acquired by Juniper Networks for more than $4 billion. Also known as the "Father of UTM," Xie has led Fortinet to become the largest network security appliance vendor, per unit share, in the world, according to IDC. Fortinet is an acknowledged market leader in unified threat management, internal segmentation firewall, and enterprise firewall solutions arena.

Fortinet products and subscription services provide cost-effective, broad, integrated and high--performance protection against dynamic security threats, including to databases and applications – from endpoints, to the perimeter and the core. More than 247,000 customers, including some of the largest brands in the world, trust Fortinet to secure their most valuable assets. Headquartered in Sunnyvale, California, Fortinet has offices and support centers around the world.

What is your primary solution/service/product?

Fortinet offers a complete ecosystem of network security solutions that can meet the patient data protection needs of the smallest physician office to the largest health insurer data center.

Next Generation Distributed Healthcare – With the threat of cyberterrorism, and evolving mobile healthcare technology, the ability to secure a diverse and distributed network is essential. Fortinet's flagship FortiGate security appliances deliver ASIC-accelerated performance

and integrated multiple layers of security designed to help protect against application and network threats. These next-generation firewalls are ideally suited for hospital data center and clinical deployments. At the other end of the spectrum, easy-to-use unified threat management (UTM) appliances and secure wireless access points can safely connect distributed offices to hospitals, insurers, and other providers simply and cost-effectively.

Advanced Threat Protection – Fortinet offers a complete advanced threat protection (ATP) framework that gives health IT a powerful, unified cybersecurity ecosystem to prevent, detect, and mitigate threats to protected health information and valuable intellectual property. ATP begins with multilayered prevention. Fortinet offers a full range of top-rated products that serve at the front lines of network (FortiGate), email (FortiMail) and endpoint (FortiClient) protection to quickly and effectively block threats. Fortinet threat protection stands vigilant against malicious phishing campaigns, recognizable malware, popular exploit techniques, common evasion tactics, and compromised websites.

Because cyberattacks are becoming more sophisticated, it is critical to also have intrusion detection in place. Our FortiSandbox solution provides contained environments to observe the runtime behavior of suspicious files, payloads and URLs. When FortiSandbox identifies malicious or high-risk payloads, integrated products and security staff are immediately alerted for mitigating action. Plus, when information is shared with FortiGuard Labs – Fortinet's large in-house global threat research arm – expert researchers turn threat data into protection updates that are quickly fed back into the ATP framework.

How does your solution/service/product help improve the healthcare system?

The top ten reported breaches to date in 2015 compromised more than 110 million healthcare records as a result of network servers or emails being hacked. The industry is clearly under siege and healthcare organizations require an end-to-end global cybersecurity network platform with faster performance, better security and more control. Fortinet offers a reliable, cost-effective integrated network security solution to protect the healthcare industry – whether it's a physician practice, retail clinic, or large health system data center.

Who are your customers?

Fortinet customers include enterprises, service providers, and government entities worldwide, including the majority of the 2014 Fortune Global 100 and seven of the top 10 largest U.S. health systems and global life sciences organizations.

What differentiates your organization from others?

Hardware-Accelerated Network Performance - FortiASIC custom processors accelerate performance more than five to 10 times faster than the competition, by offloading the compute-intensive security related tasks required to successfully protect the network. This

radical increase in performance allows customers' security to keep up with growing bandwidth requirements and provides a better user experience, particularly in a clinical setting.

Better Security – Today's healthcare cybersecurity threats are more sophisticated and damaging than ever, requiring more advanced technologies and timely threat intelligence to combat them effectively. FortiGuard Labs delivers complete threat intelligence and coordinated updates across a rich array of proprietary security technologies in real-time, 24x7x365. FortiGuard gives customers the dynamic and instant protection and support they need to stay ahead of a constantly evolving threat landscape and an ever-changing network environment.

More Control - Our custom operating system and highly scalable platform allow for true security consolidation. They provide greater visibility and control over users, offer greater performance applications and data at lower cost, and a more robust and rapid response to threats. Customers have the flexibility to deploy what they need, where they need it, simplifying the IT security infrastructure and making it easier to maintain.

What major projects is your organization currently working on?

A large area of focus for Fortinet is internal network segmentation. Besides external threats, healthcare networks are subject to an extraordinary number of internal threats. And once attackers are inside the network, they often find them flat and ripe to move laterally among resources, all while hiding from traditional defenses focused on the perimeter, rather than vulnerable internal servers, devices and data.

Fortinet internal segmentation firewalls (ISFWs) are specially adapted to the performance needs inside a network and closer to the data center cores, providing intelligent segmentation and additional layers of security. As the name suggests, ISFWs move far beyond the notion of quarantines and instead segment networks dramatically. Internal segmentation firewalls, improve the visibility of possible attacks and provide complete internal segregation of data and resources to both comply with regulatory requirements and to better meet the complex security needs of healthcare organizations.

Why did you become a WEDI member?

We value WEDI's important role within the healthcare industry, and feel our partnership with such a valued leader validates the quality and relevance of our solutions in healthcare. Fortinet typically opts to let third-party and customer testing and endorsement speak to the quality of our solutions, and allows FortiGuard Lab results to speak to our threat research and intelligence expertise. Like WEDI, Fortinet strives to educate the industry on important cybersecurity initiatives and best practices. We appreciate WEDI's recognition of Fortinet as a trusted fellow leader in cybersecurity solutions.

What do you find to be the most beneficial part of your membership?

Fortinet values the opportunity to participate in the many and diverse WEDI events, the Privacy and Security Workgroup, and thought leadership initiatives like [Perspectives in Cybersecurity in Healthcare](#) designed to better protect patient data and optimize care delivery.

What are some emerging trends you see in the overall industry that your organization provides thought leadership on?

Cybersecurity continues to be a top priority for the U.S. healthcare industry because of the prevalence of cyberattacks. Customers tell us they see up to 1,000 potential threats a day, with some seeing up to 100 serious attacks a day, 10 of which would warrant a call to the authorities. World-renown security strategists at our FortiGuard Labs and industry experts from our dedicated Fortinet Healthcare vertical provide thought leadership on understanding patient data vulnerabilities, how cyber criminals target an attack, and how to mitigate against these risks using industry best practices.