INTERNATIONAL MSSP LEVERAGES BEST-IN-CLASS FORTINET AND SENTINELONE SOLUTIONS TO DELIVER COMPELLING SERVICES TO WORLDWIDE CLIENT BASE

"Fortinet is refreshingly open in enabling best-in-class solutions from other providers to be cohesively assimilated into a single security stack. This has enabled us to deliver maximum value to our customers in a highly efficient manner."

– Mark Oakton,
Founder and Director of Security,
Infosec Partners

InfosecPartners
CYBERSECURITY

London-based Infosec Partners is a managed security services provider (MSSP) that takes a pragmatic, business-centric approach to delivering its solutions and services. The company has an extensive portfolio of offerings that range from strategic, board-level cyber-consulting to indication of compromise and penetration testing, emergency incident response and 24/7 management of complex security infrastructures. Clients include some of the world's largest and best-known businesses as well as high net worth individuals and their families.

Infosec Partners' security consultants are put through a highly structured training program and are required to attain formal business, technical, and vendor-specific credentials before being permitted to engage with clients. The company has assembled a network of trusted partners – with Fortinet and SentinelOne prominent among the select group – to create a world-class portfolio of solutions and services to complement its own in-house expertise.

EARLY ADOPTERS

Infosec Partners was the first British company to be awarded the coveted "Partner of Excellence" classification by Fortinet and are one of the inaugural inductees into the Fortinet Security Fabric Expert Program. Mark Oakton, security industry veteran and Infosec Partners' founder, expounded, "We actually have a policy of being vendor-agnostic but over the years you gain a feel for what works, whom to trust and which companies provide actual risk reduction. Based on years of experience, we felt very confident that the value of partnering with Fortinet and our subsequent achievements together have more than validated this premise."

Infosec Partners began its relationship with Fortinet just a few years after the cybersecurity giant was founded. "Even in the early days, Fortinet was doing some amazing things," recalled Oakton.

Due to the evolving threat landscape, Infosec Partners conducted extensive testing to locate a signatureless endpoint solution that would both deliver maximum efficacy and management efficiency. SentinelOne emerged as the top of the pack: "It's one of the best

DETAILS

CUSTOMER: Infosec Partners

INDUSTRY: Cybersecurity Services

LOCATION: London, England (Headquarters)

PARTNER

- SentinelOne

SOLUTIONS

- FortiSIEM
- FortiGate
- FortiWeb
- FortiClient
- SentinelOne Fortinet Connector

endpoint agents for EPP and EDR on the market today across Windows, Mac, and Linux," observed Oakton. "Coupled with FortiClient to supply VPN and web-filtering capabilities, we believe endpoint surface risks can be materially minimized."

TIMING IS EVERYTHING

Fast forward several years and seeing a trend in the large number of companies that were struggling to effectively manage their security measures, Oakton used the opportunity to expand his company's capabilities to become a managed security services provider. "We knew that we wanted to construct our MSSP services portfolio around a security information and event management [SIEM] hub. However, today – with over a decade of experience with traditional SIEMs – it's obvious that the majority just don't work," he stated. "They're hugely expensive, they're enormously complex, take months if not years to roll out, and there's a vast operational overhead for managing, monitoring, and tweaking them."

Oakton continued, "This is why we were very excited to hear that Fortinet was releasing its own SIEM, and it turns out that Fortinet FortiSIEM has proven to be absolutely the best solution for our clients and for us as an MSSP." The early integration of SentinelOne with FortiSIEM was pivotal for Infosec Partners in managing customers' endpoint and network security environments.

FORTISIEM DELIVERS COMPELLING VALUE

Mirroring the same easy-to-deploy and simple-to-manage philosophies of other Fortinet solutions, FortiSIEM enables Infosec Partners to operationalize customers in an extremely short period of time. "Frequently a new client will approach us with an urgent need to address specific issues with their security and they are astounded to learn that we can get them up and running within three hours," commented Oakton. "The competition can take many, many months to bring their SIEMs online, so being able to dramatically minimize a client's window of vulnerability is extremely compelling for everyone. FortiSIEM enables us to immediately deliver value."

For the majority of its clients, Infosec Partners deploys multiple Fortinet solutions to protect the organization's entire attack surface, complemented by a set of real-time threat intelligence and digital forensics services centered around the capabilities of FortiSIEM. All the components are unified by the unique architecture of the Fortinet Security Fabric; together delivering comprehensive protection, enterprise-wide visibility, and management from a single console.

The use of open APIs and connectors supports the integration of an almost infinite number of third-party products, enabling customers to derive even more value from their security deployments. The ecosystem of complementary technologies and services provided by third-party products helps customers gain better security and enables lower total cost of ownership.

OPEN FOR PARTNERING

"We've been a big proponent of the SentinelOne endpoint protection solution, and the beauty of the Fortinet Security Fabric is that we can also seamlessly incorporate the world-class capabilities of SentinelOne into any deployment we undertake," enthused Oakton. "This is actually a great testimony to Fortinet: The company is refreshingly open in enabling best-in-class solutions from other providers to be cohesively assimilated into a single security stack. This has enabled us to deliver maximum value to our customers in a highly efficient manner."

BUSINESS IMPACT

- Ability to offer broad visibility and protection across network and endpoint attack surfaces at all phases of the threat lifecycle

- Security architecture enables seamless integration of best-in-class solutions into unified security stack

- Rapid deployment capabilities minimize window of vulnerability and threat exposure for clients

- Pre-validated integrated solution saves time and resources, lowering total cost of ownership

Headquartered in Mountain View, California, SentinelOne has repeatedly been recognized as a "Visionary" by leading research and advisory company, Gartner, and has earned NSS Labs' highest rating of "Recommended" for multiple years in a row. The SentinelOne Endpoint Protection Platform uses static and behavioral AI and automated remediation to automatically eliminate threats in real time. "We've found SentinelOne to be an excellent endpoint protection solution," Oakton affirmed. "The accuracy is amazing: We've yet to see a false-positive."

MULTINATIONAL, MULTI-INDUSTRY

Infosec Partners has amassed a highly diverse set of clients since its inception. Oakton recounted, "One of the global utility providers that we work with has operations in almost 50 countries. We were brought in following a breach and deployed our favored combination of Fortinet and SentinelOne solutions to protect the hybrid IT and OT [operational technology] infrastructure from further compromises."

Infosec Partners' extensive experiences with Fortinet and SentinelOne in IT/OT environments has made it the MSSP of choice for clients across a wide number of industries, including airports, power generators and distributors, and critical infrastructure assets, systems and networks. "Traditionally companies have paid double to separately cover their IT and OT infrastructures: We're able to provide unified protection of both environments, with standardized security controls: This is just a colossal win for our clients."

> **TRADITIONALLY COMPANIES HAVE PAID DOUBLE TO SEPARATELY COVER THEIR IT AND OT INFRASTRUCTURES: WE'RE ABLE TO PROVIDE UNIFIED PROTECTION OF BOTH ENVIRONMENTS, WITH STANDARDIZED SECURITY CONTROLS: THIS IS JUST A COLOSSAL WIN FOR OUR CLIENTS.**

With other customers in sectors such as financial services, insurance, hospitality, media and retail, Infosec Partners protects deployments of a few hundred devices through to tens of thousands of endpoints. "We use Fortinet and SentinelOne to secure on-prem, public and private clouds, and hybrid environments.

Invariably clients have existing security products that we need to accommodate but the flexibility and speed of implementation we can offer is just unrivalled. It's rapidly becoming a game-changer for us," enthused Oakton.

He continued, "Because of the tight integration across the entire Fortinet Security Fabric and the instant, on-demand capability of our managed platform, I can drop ship a pre-staged cluster of Fortinet solutions into even the most inhospitable of locations, including ships at sea. I'm also able to immediately provision virtual firewalls, WAFs, SIEMs and endpoints in a hybrid, cloud or multi-cloud environment. I can then complete the configuration and manage everything remotely from a single console. As Sentinel One is all cloud-based, bringing it online is equally straightforward."

BUILDING A FOUNDATION FOR INNOVATION

Leveraging the Fortinet Security Fabric, Infosec Partners has developed a powerful solution known as FortiSecured. Oakton described, "Building on the multi-tenant capabilities of FortiSIEM, FortiSecured combines the strengths of several industry-leading solutions – including the FortiGate next-generation firewall, the FortiWeb web application firewall, and the SentinelOne Endpoint Protection Platform – to create a highly elastic 'instant on' Security as a Service offering for our clients. Enhanced intelligence and forensic insights from Fortinet and SentinelOne are shared across the entire infrastructure to provide protection at every stage of the threat lifecycle."

Oakton concluded, "What really impresses me is that Fortinet has defined a core set of solutions that are all great individually and they come together to deliver massive value. The architecture of the Fabric enables best-in-class partners, like SentinelOne, to be integrated into the Fortinet stack to create something that is totally compelling."

F⊡RTINET®

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