CASE STUDY

International MSSP Leverages Fortinet to Deliver Expect Cyber Protection Services to Worldwide Client Base

London-based Infosec Partners is a managed security service providers (MSSP) that takes a pragmatic, business-metric 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, high net worth individuals and their families, as well as high risk environments such as film sets and superyachts.

Infosec Partners' security consultants are put through a highly structured training program and are requred 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—to create a world-class portfolio of solutions and services to complement its own in-house cyber 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 Oarton, security industry veteran and Infosec Partners' founder, expounded, "We actually have a policy of being a vendor-agnostic but over the years, you gain a feel of what works, whom to trust, and which companies provide actual risk protection. 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 from its inception, with Mark Oakton and his team being the first to deploy Fortinet technology in the UK, shortly after the cybersecurity giant was founded. "Even in the early days, Fortinet was doing some amazing things," recalled Oakton.

Infosec Partners realised that the integration of security controls was key to elevated protection levels and needed and endpoint protection platform to seamlessly shared intelligence with core firewalls and security information and event management (SIEM) platforms.

FortiEDR was chosen: "It's one of the best endpoint agents for EPP and EDR on the market today and the uplift in visibility gained from an integrated platform is a game changer," observed Oakton. "Coupled with FortiInsight providing insider threat protection and behavioral analysis, and Forticlient to supply virtual private network (VPN) and web-filtering capabilities, we believe endpoint surface risks can be materially minimized.

InfosecPartners
CYBERSECURITY

"Fortinet is refreshingly open in enabling other providers to connect via API to all core products. The Fortinet fabric has matured quickly providing a cohesive platform of control, the inclusion of FortiEDR, FortiInsights, and FortiSOAR means, we have advanced control in our Fortinet managed service without any reliance on other vendors."

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

Details

Customer: Infosec Partners
Industry: Cybersecurity Services
Location: London, England (Headquarters)

Business Impact

- Ability to offer broad visibility and protection across network and endpoint attack surfaces at all phases of threat lifecycle
- Security architecture enables seamless integration of best-in-class solutions into unified security stack

Timing Is Everything

Fast forward several years and seeing a trend in the large number of companies that were struggling effectively manage their security measures, Oakton used the opportunity to expand his company's capabilities to become a managed security service provider. "We knew that we wanted to construct our MSSP services portfolio around a SIEM hub.However, today—with over a decade of experience with traditional SIEMs—it's obvious that 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 all core fabric controls 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 TCO.

Business Impact (contd.)

- 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 (TCO)

Solutions

- FortiSIEM
- FortiEDR
- FortiWeb
- FortiInsight
- FortiSOAR

"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."

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

Open for Partnership

"We've been a big proponent of the Fortinet Fabric and the beauty is that we can seamlessly extend it, many of our clients have several Fortinet components as an integrated fabric of baseline control for their environement but then we layer in technologies from other vendors to further enhance threat protection and incident response capability 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 attack. This has enabled us to deliver maximum value to our customers in a highly efficient manner."

"Most clients' Cyber maturity level progresses quickly as they feel confident in the integrated fabric approach and we integrate vulnerability management, external threat intelligence and decoy, and deception systems for example. The combination of

tightly integrated suite of Fortinet controls and simple extension to include external providers systems through the FortiSIEM and FortiSOAR integration processes is unrivalled in the market, the staffing, and recurring costs of security operations with a Fortinet platform is far lower than other vendor offerings and the benefits will increase as we enhance this partnerships."

Multinational, Multi-industry

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

Infosec Partners' extensive experiences with Fortinet controls 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 and assets, systems, and networks. "Traditionally companies have paid double to separately cover their IT and OT infrastructure: We're able to provide unified protection of both environments, with standardized security controls: This is just a colossal win for our clients."

With our customers in sectors such as financial services, insurance, hospitality, media, and retail, Infosec Partners protects deployments of a few hundreds devices through to tens of thousands of endpoints. "We use Fortinet to secure on-premises, 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, web application firewalls (WAFs), SIEMs, and endpoint controls in a hybrid, cloud or multi-cloud environments. I can then complete the configuration and manage everything remotely from a single console. Adding layers of protection from FortiEDR, FortiInsight, and FortiSOAR allows us to achieve advanced visibility and control without any of the complexity that usually accompanies expert systems."

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 (NGFW) integrated with advanced endpoint ecurity controls focusing on insider threat, EDR, and forensics—to create a highly elastic 'instant on' Security as a Service (SECaaS) offering for our clients. Threat intelligence and forensically sound evidence from the Fortinet Fabric are shared across the entire infrastructure to provide protection at every single stage of the threat lifecycle."

Oakton included, " 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 a massive value. The architecture of the Fortinet Fabric enables best-in-class partners, like Infosec Partners, to integrate incident response and remediation capability into the Fortinet stack to create a cohesive protection platform that is very compelling.

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

March 19, 2021 4:52 AM

D:\Fortinet\2021Rebrandedtemplates\MarketingorCommsRequest\March\BrandingRefresh\907004-InfoSecPartners\cs-international-mssp-leverages-best-in-class-solutions-3192021\cs-international-mssp-leverages-best-in-class-solutions-3192021

232638-A-0-EN