

BT deploys Fortinet firewalls for MSS

Combines BT's service with Fortinet's Security Fabric



↑ Hughes says partnership seeks to help customers protect themselves against today's evolving threats without slowdown.

BT and Fortinet have announced an agreement that will integrate Fortinet's FortiGate enterprise firewalls into BT's global portfolio of managed security services.

The agreement confirms BT's worldwide status as a Fortinet Managed Security Services Provider (MSSP) Platinum Partner. BT customers will benefit from the protection provided by Fortinet's Security Fabric architecture and BT's global reach and expertise in managed security services.

Integrated into BT's managed security services, Fortinet FortiGate enterprise firewalls will provide next-generation firewall, application control, intrusion prevention, web content filtering, Virtual Private Networking (VPN), spyware prevention and malware defence.

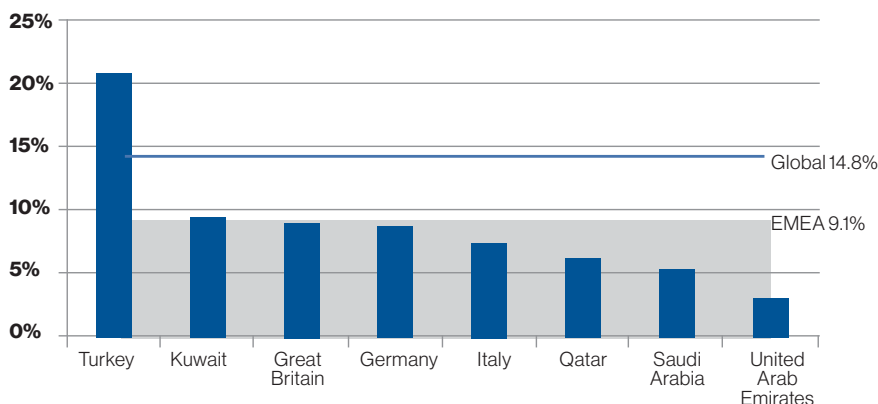
Fortinet's Security Fabric brings traditionally autonomous systems together into an integrated, collaborative, and adaptive architecture designed to deliver distributed security for various types of environments, from Internet of Things (IoT) to the cloud.

Mark Hughes, chief executive officer, BT Security, said: "We are committed to supporting our customers with solutions that can help them stay secure and support their journeys into the digital world.

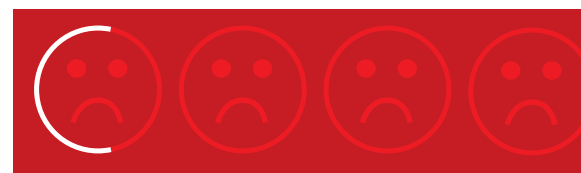
"Together with Fortinet, we provide them with security solutions to protect themselves against today's evolving threat landscape without additional complexity or slowing down their networks," he added.

REGIONAL ADVANCED THREAT REPORT, EMEA, 2H2015: FIREEYE

Advanced targeted threat exposure by EMEA country



→ MSS avails top professionals to look into information security, says Zeineldin.



QUOTED



Given current security climate, all companies should have multi-factor authentication activated by default for all online accounts."

Sebastien Pavie, regional director MENA, Gemalto

eHDF launches cyber defence centre

Over a third of respondents in a survey to invest in MSS in 2016

eHosting DataFort (eHDF), regional provider of managed hosting and cloud infrastructure services, has launched a UAE-based Cyber Defence Centre (CDC).

The Cyber Defence Centre will offer customers a portfolio of managed security services (MSS) along with remote managed SIEM Services. The announcement was made at a seminar hosted along with Necture and LogRhythm in Dubai.

Titled 'Detect & Respond Quickly to High Impact Threats', the seminar covered a range of topics and highlighted the most pressing issues connected to cyber security. The seminar discussed growing popularity of managed security services which covers Advanced Threat Protection, Incident Management and Response, DDoS Protection, Endpoint Security Management, etc. The importance of

MSS and how customers can benefit from end-to-end security lifecycle management was also outlined.

The seminar included talks on threat landscape, the role of MSS in the modern day context and the importance of modernising threat detection & response. The seminar also saw LogRhythm conduct a demo on their SIEM solution.

"At a time when data breaches and hacking are on the rise, it is crucial for organisations to be prepared to combat these attacks," says Yasser Zeineldin, CEO, eHosting DataFort.

"With the need for specialised skills required to tackle security issues, managed security services can help curtail budgets. It will also have professionals look into the highly specialised areas of information security," he added.

Gartner identifies five key areas of focus for successfully addressing cybersecurity in digital businesses

Leadership and governance —

Improving leadership and governance is arguably more important than developing technology tools and skills when addressing cybersecurity and technology risk in digital business.

The evolving threat environment —

IT risk and security leaders must move from trying to prevent every threat and acknowledge that perfect protection is not achievable.

Cybersecurity at the speed of digital business —

Digital business moves at a faster pace than traditional business, and traditional security approaches designed for maximum control will no longer work in the new era of digital innovation.

Cybersecurity at the new edge —

It used to be easy to protect data because it resided in the data centre. The new edge has pushed far beyond the data centre into operational technology, cloud, mobile, software as a service and things.

People and process: cultural change-

With the acceleration of digital business and the power technology gives individuals, it is now critical to address behaviour change and engagement.

12%

Percentage of compromises in EMEA detected by an external source.

Source: Mandiant M-Trends EMEA report



"xDedic (underground marketplace) confirms that cybercrime-as-a-service is expanding through the addition of trading platforms."

Costin Raiu, director, GReAT, Kaspersky Lab



"If left unaddressed, DDoS attacks costs will include lost business, time-to-service restoration and a decline in customer satisfaction."

Raj Jalan, chief technology officer, A10 Networks