

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security

PUBLIC/UN-SPONSORED

T-Systems Targets UK Security Market

- Expanding into other markets like the UK is key to T-Systems' goal of becoming Europe's largest cyber security services provider.
- T-Systems is delivering managed security services with managed SOC, cloud security, Internet protection and other services delivered from its own cloud.
- The company has substantial cyber security assets but the UK business is being selective in the portfolio it offers local business customers.
- Effective from the first half of 2020, both the security and IoT businesses will be spun out as separate GmbH units, albeit they will remain part of T-Systems.

T-Systems wants to be Europe's largest provider of information security services within three to four years.

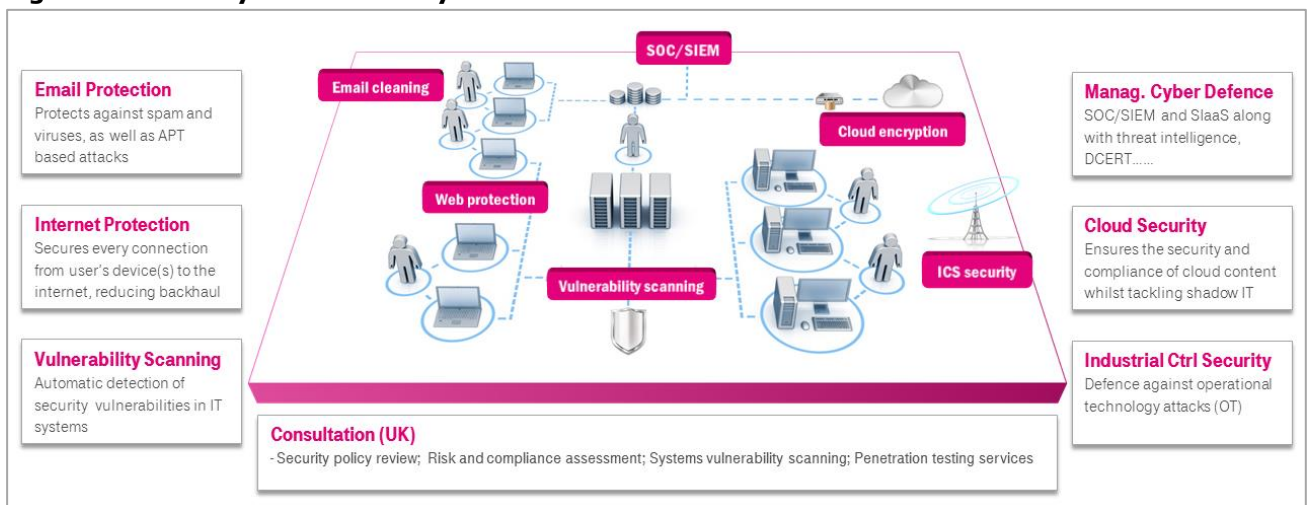
Succeeding in the UK is critical to T-Systems' stated goal of becoming Europe's largest provider of information security services within three to four years. Had it not been for the preoccupation of Deutsche Telekom, its parent company, with the Sprint merger over the last couple of years, T-Systems might already have made some in-country cyber security acquisitions in key European markets. That kind of M&A activity is still likely in the UK and elsewhere in Europe but for now the company's UK strategy is dependent on organic growth.

Around three hundred employees in the UK

T-Systems employs around 300 people in the UK. Security currently accounts for about 5% of total revenues. The single largest top line contributor to the UK business as of today is Cloud & Infrastructure services, which includes classical hosting as well as public, private and hybrid cloud infrastructure for businesses.

Courtesy of the company's German roots, T-Systems is also a leader in SAP deployments and is currently seeing strong traction migrating UK customers to SAP's new Hana platforms. The second largest revenue generator is Connectivity services, providing a range of business communications services to UK companies.

Figure 1: The T-Systems Security Portfolio for the UK



Source: T-Systems

Almost every security product offered in the UK is delivered as a managed service from the T-Systems cloud.

In common with many telcos and their affiliates, historically T-Systems bundled its security offerings together with its telecom services. With effect from January 2019, a new go to-market approach in the UK has driven the formation of a Future Growth division. This comprises the company's security, digital services and Internet of Things (IoT) businesses. These emerging markets have a higher growth potential than the more stable revenue outlook for the core Infrastructure & Cloud and Connectivity businesses.

Some aspects of this change will be phased in over time rather than immediately. For example, because of the tight coupling with telecom services, security offerings such as Next Generation Firewall (NGFW) still reside within the Connectivity business, whilst micro-segmentation and zero trust initiatives fall within the security business. There will inevitably continue to be overlaps between these two closely tied businesses. Effective from the first half of 2020, the security and IoT businesses will each be spun out as separate GmbH businesses, albeit they will still remain part of T-Systems.

T-Systems is investing heavily in the cyber security business

To meet its goals in the UK, T-Systems is leveraging the substantial resources that its' parent company is investing with a view to becoming Europe's cyber security leader. Like any large telco, Deutsche Telekom has unique visibility into the threat landscape via its position in the ICT ecosystem. The dedicated Telekom Security business unit within T-Systems has a headcount of more than 1,500 cyber security professionals.

In addition to the new state-of-the-art Security Operations Centre (SOC) opened in Bonn in 2018, T-Systems has other SOCs in South Africa, Mexico, Brazil, Hungary and Slovakia. The Telekom Security portfolio now comprises products and services from around fifty different vendor partners. Germany's reputation as a European and world leader in data protection can also be a significant differentiator.

As a relatively small player in the UK security sector, T-Systems needs to be disciplined in terms of the customer segments it targets. The segments it is pursuing in the security space include manufacturing, retail, and energy, where it is already seeing initial traction. The company is targeting the public as well as the private sector but that primarily means local government organizations. The cycle times for central government tend to be prohibitive for new players.

Nowadays a high-end enterprise security sale doesn't start with product, still less with a box-oriented sell. The T-Systems approach starts with a consultation around risk assessment, potentially supported by a vulnerability scan. This helps customers allocate limited security budgets to mitigate the highest levels of security risk to their organization. Whereas in Germany, the legacy installed base and expectations of an incumbent telco demand that T-Systems has to continue supporting hardware-based, cloud delivered software as well as managed security services, almost every security product offered in the UK is delivered as a managed service from the T-Systems cloud.

The T-Systems security portfolio for the UK is centered around six core offerings:

- **Managed Cyber Defence (SOC/SIEM).** This is the company's premium service, a SOC offering driven off IBM Security's QRadar platform. It accounts for the largest share of security revenues.
- **Internet Protect Pro:** Leveraging vendor solutions from Zscaler and Symantec, this ensures that employees are able to access the Internet securely from any device, and independent of their location, whether they be at a coffee shop, airport, at home or on campus.
- **Cloud Protect Pro:** Based on Symantec, this protects enterprise access to data once users are connected to the cloud. It enables the setting, monitoring and enforcement of policies that help organizations curtail or eliminate 'shadow IT' practices, and control how content is stored, accessed and shared.

- **Email Protect:** This provides protection against phishing and whaling attacks, which are still the most common threat vector.
- **Vulnerability scanning:** This uses the Qualys platform to audit and identify vulnerabilities in an enterprise's infrastructure. It ranks them in order of the severity of the risk posed and enables different fixes to be prioritized.
- **Industrial Control Security (ICS).** Tailored to the Operational technology (OT) environment, this Cyber-X based vulnerability solution can be deployed autonomously or in conjunction with Qualys. The latter use case serves the increasingly common example where organizations want to synchronize security across their IT and OT environments to protect against threats where attackers move laterally across both domains.

It wouldn't be at all surprising to see T-Systems acquire at least one UK-based cyber security provider or MSP to accelerate sales.

The above six are the core services for which the UK business has identified the highest local demand but there are many other offerings from broader T-Systems security portfolio that it can draw upon. Targeting the managed security services market, there may be some scope for partnering high profile integrators in the medium term but there's no evidence of this just yet. That said, it's unlikely that T-Systems can achieve its goals via organic growth alone. For that reason it wouldn't be at all surprising to see the company acquire at least one cyber security provider or security-savvy Managed Service Provider (MSP) with a strong security pedigree to accelerate sales.

There is an unfilled vacancy for the role of Europe's leader

The UK is pivotal to the contest to be the leader in the European cyber security services market. Given how fragmented the market is – at a national level, let alone at a pan-European level – this is a vacancy that's best thought of as unfilled at this time.

T-Systems and the cyber security divisions of other telcos and IT services companies all covet this position. The world's biggest and best MSSPs such as IBM Security, Secureworks and Verizon all generate more than two thirds of their revenues from North America. Their presence in Europe is significant but not big enough for them to be the region's leader in their own right. How fast T-Systems and others can grow in the UK in the next two or three years will be key in determining which of these players emerges as Europe's leader ■

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a well-known voice in telecom and enterprise security, a leader in custom cyber security research, and a leading publisher of cyber security reports and White Papers. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, ETSI and TM Forum. To learn more visit www.hardenstance.com. Register here for [free email notifications](#) whenever new IT and telecom security content is made available by HardenStance.

HardenStance Ltd Disclaimer of Warranty and Liability

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action

taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same. The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.