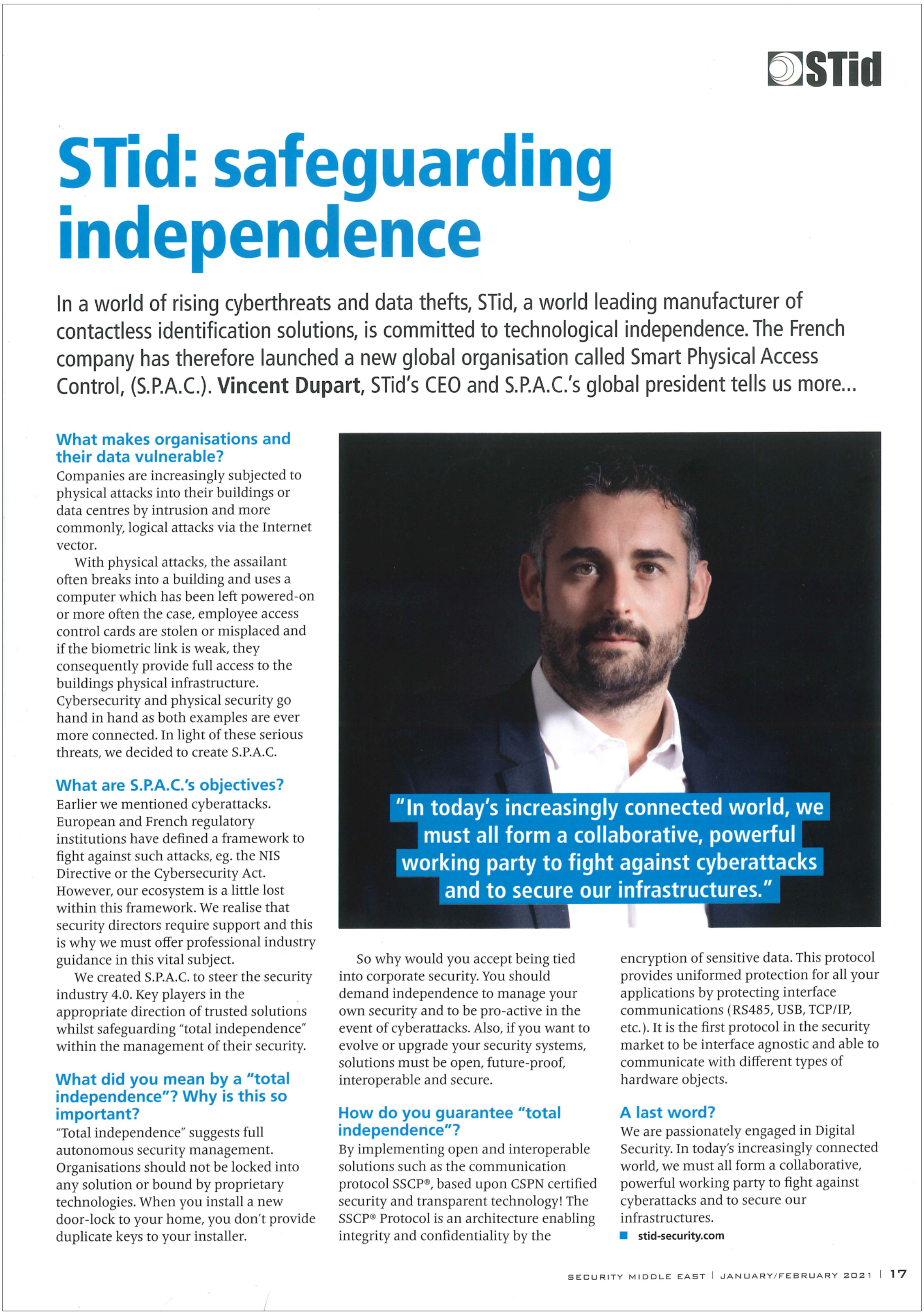
SECURITY
MIDDLE EAST
Protecting your privileges
The growing issue of targeted data breaches

FEBRUARY - 2021

Article
STid: safeguarding independence

Security Middle East - Issue 118 - February 2021



STid

STid: safeguarding independence

In a world of rising cyberthreats and data thefts, STid, a world leading manufacturer of contactless identification solutions, is committed to technological independence. The French company has therefore launched a new global organisation called Smart Physical Access Control, (S.P.A.C.). **Vincent Dupart**, STid's CEO and S.P.A.C.'s global president tells us more...

What makes organisations and their data vulnerable?

Companies are increasingly subjected to physical attacks into their buildings or data centres by intrusion and more commonly, logical attacks via the Internet vector.

With physical attacks, the assailant often breaks into a building and uses a computer which has been left powered-on or more often the case, employee access control cards are stolen or misplaced and if the biometric link is weak, they consequently provide full access to the buildings physical infrastructure. Cybersecurity and physical security go hand in hand as both examples are ever more connected. In light of these serious threats, we decided to create S.P.A.C.

What are S.P.A.C.'s objectives?

Earlier we mentioned cyberattacks. European and French regulatory institutions have defined a framework to fight against such attacks, eg. the NIS Directive or the Cybersecurity Act. However, our ecosystem is a little lost within this framework. We realise that security directors require support and this is why we must offer professional industry guidance in this vital subject.

We created S.P.A.C. to steer the security industry 4.0. Key players in the appropriate direction of trusted solutions whilst safeguarding "total independence" within the management of their security.

What did you mean by a "total independence"? Why is this so important?

"Total independence" suggests full autonomous security management. Organisations should not be locked into any solution or bound by proprietary technologies. When you install a new door-lock to your home, you don't provide duplicate keys to your installer.

So why would you accept being tied into corporate security. You should demand independence to manage your own security and to be pro-active in the event of cyberattacks. Also, if you want to evolve or upgrade your security systems, solutions must be open, future-proof, interoperable and secure.

"In today's increasingly connected world, we must all form a collaborative, powerful working party to fight against cyberattacks and to secure our infrastructures."

How do you guarantee "total independence"?

By implementing open and interoperable solutions such as the communication protocol SSCP®, based upon CSPN certified security and transparent technology! The SSCP® Protocol is an architecture enabling integrity and confidentiality by the encryption of sensitive data. This protocol provides uniformed protection for all your applications by protecting interface communications (RS485, USB, TCP/IP, etc.). It is the first protocol in the security market to be interface agnostic and able to communicate with different types of hardware objects.

A last word?

We are passionately engaged in Digital Security. In today's increasingly connected world, we must all form a collaborative, powerful working party to fight against cyberattacks and to secure our infrastructures.

■ stid-security.com

Press_02_2021_SECURITY_MIDDLE_EAST_ARTICLE_UK