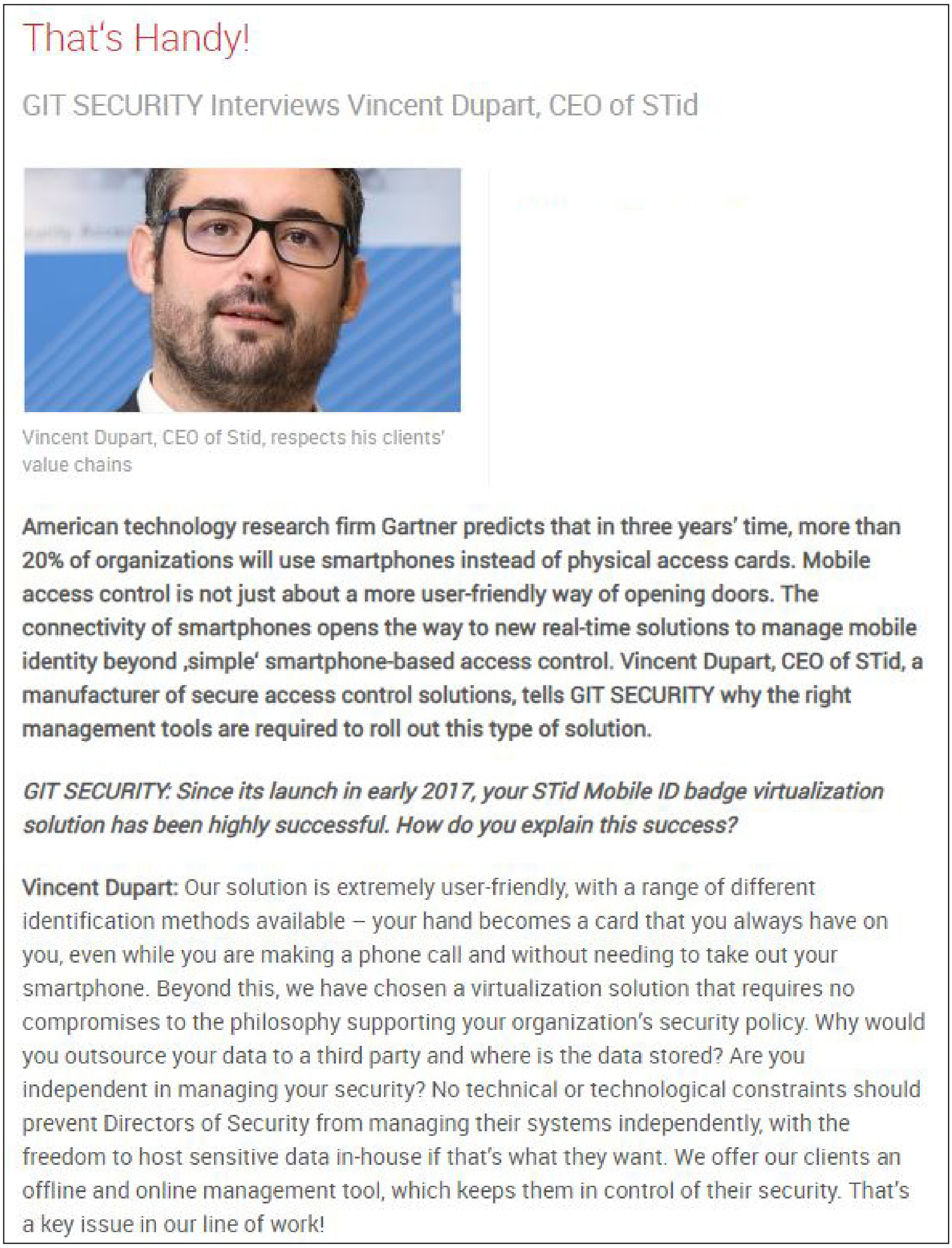
Article - That's Handy!

GIT SECURITY - August 2018

GIT SECURITY
MAGAZINE FOR SAFETY AND SECURITY
EMEA



That's Handy!

GIT SECURITY Interviews Vincent Dupart, CEO of STid

Vincent Dupart, CEO of Stid, respects his clients' value chains

American technology research firm Gartner predicts that in three years' time, more than 20% of organizations will use smartphones instead of physical access cards. Mobile access control is not just about a more user-friendly way of opening doors. The connectivity of smartphones opens the way to new real-time solutions to manage mobile identity beyond ‚simple' smartphone-based access control. Vincent Dupart, CEO of STid, a manufacturer of secure access control solutions, tells GIT SECURITY why the right management tools are required to roll out this type of solution.

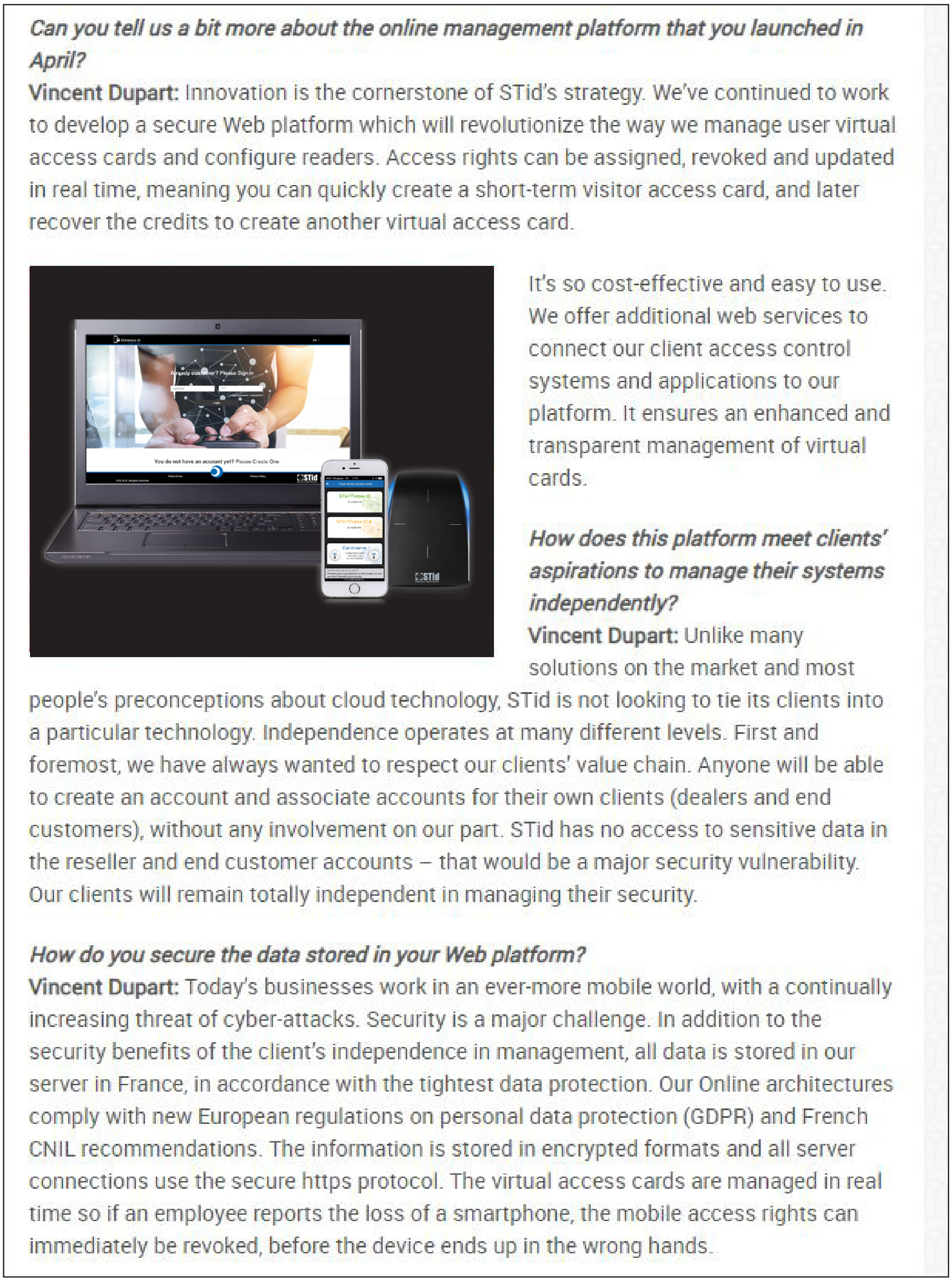
GIT SECURITY: Since its launch in early 2017, your STid Mobile ID badge virtualization solution has been highly successful. How do you explain this success?

Vincent Dupart: Our solution is extremely user-friendly, with a range of different identification methods available – your hand becomes a card that you always have on you, even while you are making a phone call and without needing to take out your smartphone. Beyond this, we have chosen a virtualization solution that requires no compromises to the philosophy supporting your organization's security policy. Why would you outsource your data to a third party and where is the data stored? Are you independent in managing your security? No technical or technological constraints should prevent Directors of Security from managing their systems independently, with the freedom to host sensitive data in-house if that's what they want. We offer our clients an offline and online management tool, which keeps them in control of their security. That's a key issue in our line of work!

Article - That's Handy!

GIT SECURITY - August 2018

MAGAZINE FOR SAFETY AND SECURITY
GIT SECURITY
EMEA



Can you tell us a bit more about the online management platform that you launched in April?

Vincent Dupart: Innovation is the cornerstone of STid's strategy. We've continued to work to develop a secure Web platform which will revolutionize the way we manage user virtual access cards and configure readers. Access rights can be assigned, revoked and updated in real time, meaning you can quickly create a short-term visitor access card, and later recover the credits to create another virtual access card.

It's so cost-effective and easy to use. We offer additional web services to connect our client access control systems and applications to our platform. It ensures an enhanced and transparent management of virtual cards.

How does this platform meet clients' aspirations to manage their systems independently?

Vincent Dupart: Unlike many solutions on the market and most people's preconceptions about cloud technology, STid is not looking to tie its clients into a particular technology. Independence operates at many different levels. First and foremost, we have always wanted to respect our clients' value chain. Anyone will be able to create an account and associate accounts for their own clients (dealers and end customers), without any involvement on our part. STid has no access to sensitive data in the reseller and end customer accounts – that would be a major security vulnerability. Our clients will remain totally independent in managing their security.

How do you secure the data stored in your Web platform?

Vincent Dupart: Today's businesses work in an ever-more mobile world, with a continually increasing threat of cyber-attacks. Security is a major challenge. In addition to the security benefits of the client's independence in management, all data is stored in our server in France, in accordance with the tightest data protection. Our Online architectures comply with new European regulations on personal data protection (GDPR) and French CNIL recommendations. The information is stored in encrypted formats and all server connections use the secure https protocol. The virtual access cards are managed in real time so if an employee reports the loss of a smartphone, the mobile access rights can immediately be revoked, before the device ends up in the wrong hands.