New Offerings Make MFA and Encryption Accessible to SMEs as Data Protection Challenges European Organizations

An IDC White Paper
Sponsored by ESET
February 2017

Authors: Alexei Proskura
Mark Child

New Offerings Make MFA and Encryption Accessible to SMEs as Data Protection Challenges European Organizations

An IDC White Paper, Sponsored by ESET

IDC Opinion

There are obvious limitations to the resources that small and medium-sized enterprises (SMEs) can assign to security — it is hard enough for them to deal with IT as it is. At the same time, the market is seeing a shift of focus from infrastructure to data security as the perimeter disappears and data becomes omnipresent. Mobile/multiple devices add to the complexity of both IT and security. These developments are driving the need for SMEs to re-evaluate and update their IT and security strategies.

To resolve data security challenges, two key elements have to be addressed: 1) user access management, which relies on reliable user authentication; and 2) data protection, both for data at rest and data on the move, including in the case of compromise.

1. Of confirmed data breaches, 63% are attributed to stolen or cracked passwords (DBIR, 2016), indicating the critical need for an additional or alternative authentication factor. However, the typically limited IT headcount in most SMEs makes the additional burden of further authentication management duties a barrier to adoption in many such companies. Any proposed solution has to deliver the promised gains with high ease of use and minimal demands on departmental resources.
2. Anonymization of data is one option and encryption is another — both have their pros and cons. Anonymization is a good approach, but it can be defeated by correlation of data from multiple sources. Encryption resolves this drawback, but, at least until recently, it was seen as too complex and expensive for most SMEs. With cloud enablement, this may no longer be the case.

Wider availability of cloud services at affordable prices, the decreasing cost of smart mobile devices, and advances in security technologies are changing the operational landscape for SMEs. It is time to revisit security technologies that were once unattainable due to acquisition and/or maintenance costs and the requirements for support provision.

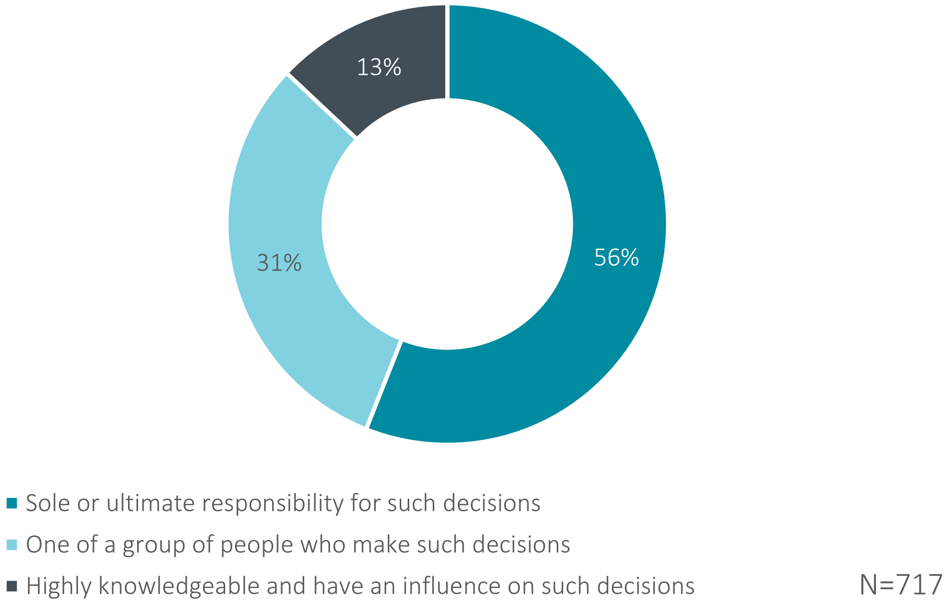
Methodology

IDC's white paper is based upon the findings of extensive fieldwork and surveying of more than 700 organizations across seven European countries: the Czech Republic, Germany, Italy, the Netherlands, Slovakia, Spain, and the United Kingdom. The survey focused on SMEs with 50–499 endpoints to protect across all vertical sectors. Respondents in C-level, security, or IT administrative or management positions were questioned about a range of security-related topics including endpoint protection solutions deployed or desired at their organization, regulations affecting them, measures taken to improve data security, barriers to improving their security stance, attitudes toward using cloud for security, and the impact of any security breaches suffered.

FIGURE 1

Respondent Involvement in IT Security Decisions

Q. Which best describes your involvement in IT security decisions affecting your organization?



Source: IDC, 2017

In This White Paper

The current landscape around information security is becoming more and more challenging for organizations, which must face up to a raft of evolving legislation while at the same time protecting increasingly extensive and dispersed information assets from an ever-growing array of threats. Companies face difficult decisions on how to prioritize their security investments, how best to remain compliant, and how to react when security incidents occur.

This White Paper looks at the information security solutions that European organizations are deploying and the criteria they use to select them, the challenges they face in trying to improve their security stance, and their understanding and awareness of the risks and threats. The study is based on extensive fieldwork across Europe, as well as IDC's existing knowledge and research in the fields of information security, security processes and technologies, the threat landscape, and regulatory frameworks.

Situation Overview

Workforce Change

According to The European Business Review, demographic changes are occurring in the workplace that will increasingly affect more and more organizations. Companies should prepare for the generation that values "multitasking, the role of technology and being connected, work-life integration, and social consciousness." [1] This means that to attract future talent, companies have to be able to satisfy new workforce requirements which, in turn, means mobility, multiple devices, and no perimeter.

Disappearance of the Perimeter

According to Verizon's 2016 Data Breach Investigations Report (DBIR, 2016), 63% of all confirmed data breaches in 2015 involved default, weak, or stolen passwords[2]. In simple terms this means that perimeter defenses are essentially being circumvented. This group of valuable security controls should not be discarded, but is no longer sufficient to protect the enterprise. Identity and access management — covering areas such as advanced authentication, user provisioning, access control, role management, and rights management — is overtaking perimeter defenses in importance.

[1] http://www.europeanbusinessreview.com/demographic-workplace/

[2] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

Data Security Takes Center Stage

Infrastructure is no longer the main target for cybercriminals. While they will certainly use every compromised device, they are now primarily after data, which is easier to monetize. Several factors are making data security significantly more challenging in the current environment:

- State-sponsored threat actors have entered the stage with vast resources. The organization, skills, and strategic approach of state-sponsored groups makes it exceedingly difficult for most organizations to defend themselves against their sophisticated attacks.
- According to the DBIR, the volume of unknown malware remains high, while previously unknown vulnerabilities continue to be discovered. Until signatures and patches for these are created and deployed, organizations will continue to struggle to protect their systems and data against such exploits. Meanwhile, known vulnerabilities are still being exploited and account for a major share of data breaches.
- The availability of automated exploit frameworks continues to increase, enabling even attackers with limited expertise to carry out attacks with increasing frequency, extent, or intensity. More and more organizations can become targets — it is no longer an option for a company to consider itself "not at risk" due to its size or the nature of the organization.

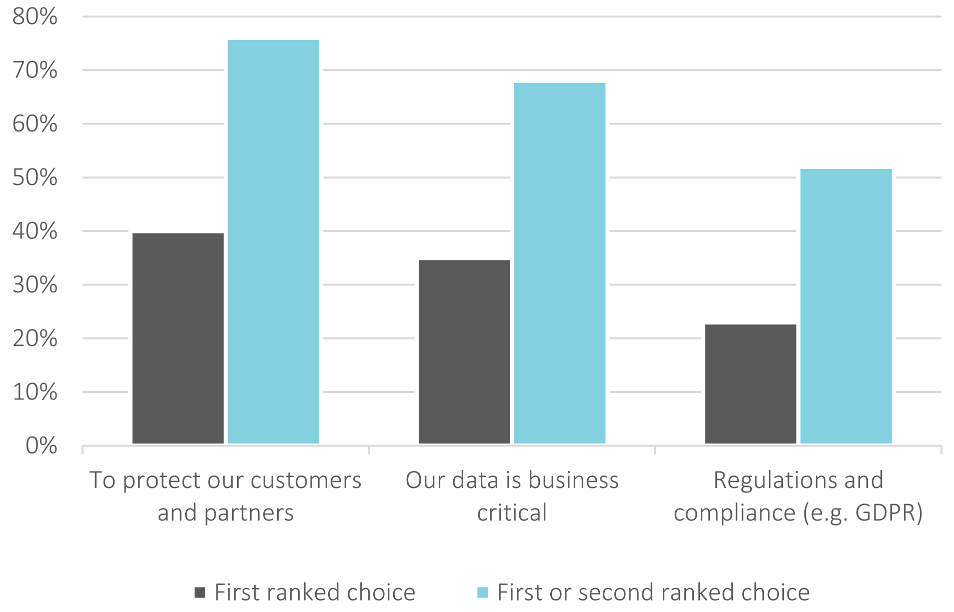
Consequently, if data is sensitive, the pragmatic approach is to assume that the organization's systems could already be compromised or could be compromised at any time. This is where encryption may come to the rescue. Deploying an appropriate encryption solution will benefit any organization, but encryption is complex to manage, especially for SMEs, and expertise is expensive. Encryption is also complex from the user point of view, as it often requires at least basic understanding of the technology. Open-source applications tend to be more secure due to peer review but are not very user friendly, as they are assumed to be adopted by users with extensive knowhow and technical capabilities.

IDC's survey data shows European SMEs making the right noises about protecting their data and the reasons and drivers for them to do so (see Figure 2 below). Protecting customers and partners is of course paramount to the continued success and survival of any entity, but companies also increasingly recognize the business value of their data and are aware of the expanding legislative frameworks they must comply with and the penalties levied for failing to do so.

FIGURE 2

Drivers for Securing Data

Q. What drives your organization to prevent unauthorized access to your data?



Source: IDC, 2017

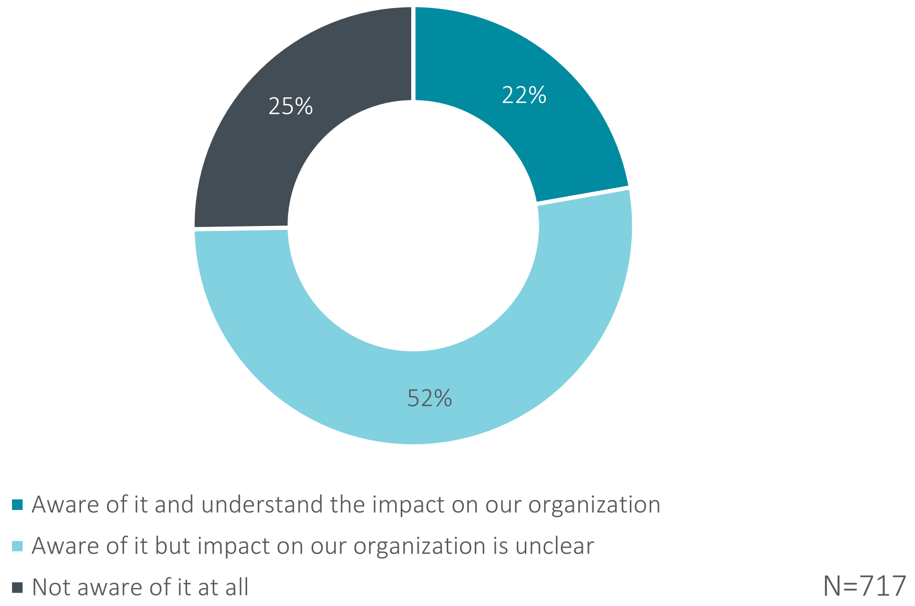
The Regulatory Landscape

While regulations are being put in place to impose more control over how data is handled, they are mostly concerned with private data. The wider availability and increasing affordability of big data technology, particularly cloud-supported offerings, has made it possible for SMEs to provide analytical services to larger customers. These companies should pay closer attention to data protection, as they are also subject to the data privacy protection regulations due to their handling of large volumes of private data. Nevertheless, these companies often lack the appropriate expertise to protect that data.

In terms of regulations, the greatest share of respondents cited the Payment Card Industry (PCI) data security standard as affecting their organization (46%). The EU General Data Protection Regulation (GDPR) and Network Information Security Directive (NISD) followed with 37% and 36%, respectively. GDPR has been heavily covered in the media and through conferences and seminars over the past year, and yet 52% of respondents still say that its impact for their organization is unclear, while a quarter were not aware of it at all (see Figure 3). Of those that are aware of GDPR, 20% claim they are already compliant, 59% say they are working on it, and 21% say they are not prepared at all (see Figure 4).

FIGURE 3

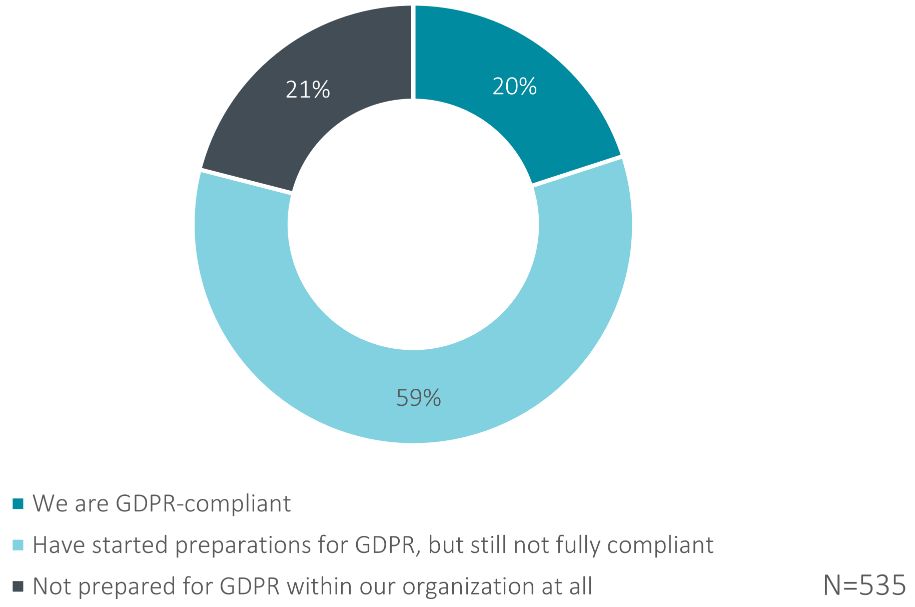
What Is Your Understanding of GDPR?



Source: IDC, 2017

FIGURE 4

Status of Preparations for GDPR Within Organizations



Note: only respondents confirming awareness of GDPR in previous question

Source: IDC, 2017

Data Leak Prevention (DLP) technologies are sometimes seen as a silver bullet for data protection by companies seeking to become compliant. However, this impression can be misleading, as DLP requires underlying technologies such as authentication and data classification to be fully effective. It may seem counterintuitive but, depending on business specifics, stronger authentication (e.g., multi-factor authentication) or encryption may be more cost-effective security controls and also provide additional productivity benefits (e.g., by enabling workforce mobility).

Classical Endpoint Security Is No Longer Sufficient for Data Protection

As one would expect, antivirus and antimalware solutions had the highest penetration rate (84%) across all countries in the survey (see Figure 5 below), followed by host firewall (68%). Nevertheless, many organizations recognize that their existing antimalware software is insufficient in the current threat environment, and half of the respondents cited this as their top area to add to or upgrade. Within the field of antimalware solutions, many vendors are undertaking qualitative improvements to their technologies, while new vendors are entering the market and challenging the established players. Recent malware trends (such as the rise in ransomware attacks) are forcing companies to revisit their antimalware defenses, and many are looking to upgrade or complement their existing solutions. The main concern regarding firewalls is that attackers and exploits utilize the ports that are open due to operational requirements, such as those used to allow web traffic. This drives the need to move defenses deeper into the infrastructure and closer to the data itself.

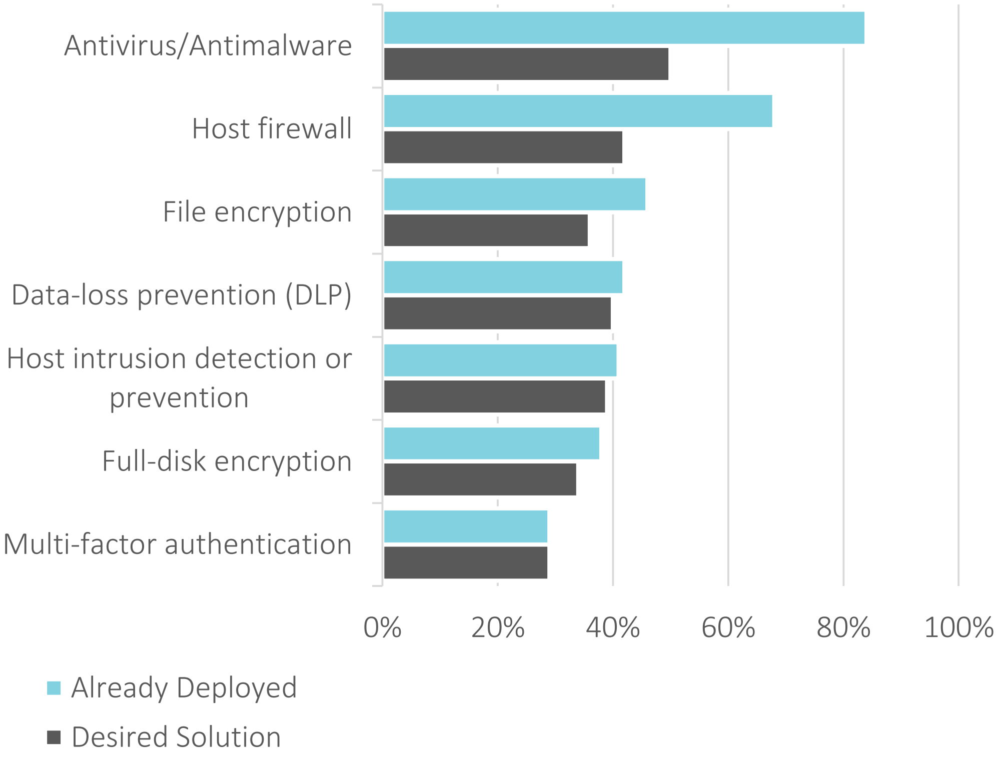
Encryption and access control provide the means by which these challenges can be addressed, although the classical mindset described above continues to dominate security planning.

FIGURE 5

Security Solutions in Place or Desired by Organizations

Q6. What endpoint security solutions are used within your organization?

Q7. If budget approval was guaranteed, what top three security solutions would you deploy or upgrade?



Source: IDC, 2017

This "classical thinking" prevents organizations from taking the necessary next steps to improve their data protection stance, and also occupies a share of the financial resources required to take these steps.

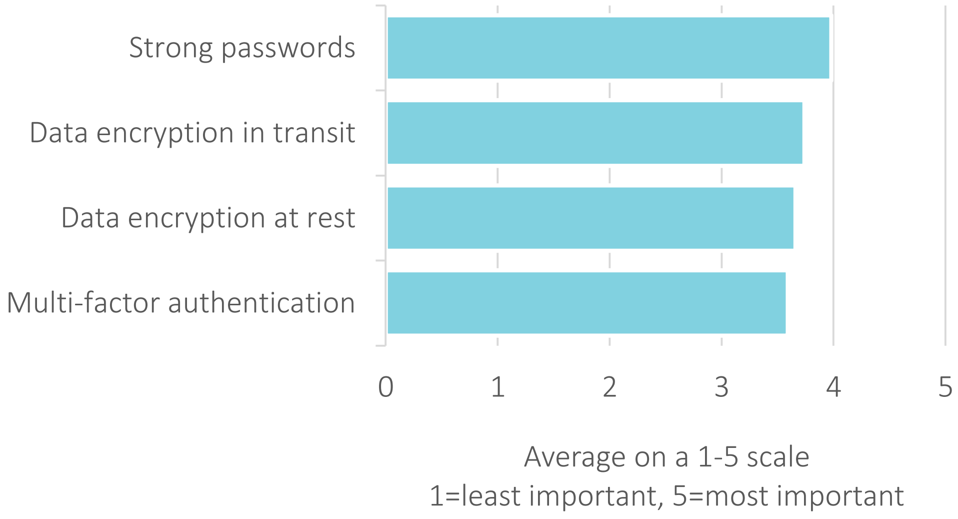
One of the first steps should be the deployment of multi-factor authentication (MFA), which functions as a means to compensate for the weaknesses of password-based protection (such as the requirement for users to memorize significant numbers of strong/complex passwords). MFA makes it more difficult for attackers to compromise user identity (for example, when employing a second device as one of the factors). This serves a dual function, as MFA protects at both the system login level and at the application level, protecting the data therein. As noted earlier in this white paper, compromised passwords account for 63% of data breaches, and MFA therefore holds significant potential for reducing the number of breaches.

One further means of protecting data is to encrypt it, thereby rendering it unreadable to anybody that has stolen it but does not have the means to decrypt it. Encryption keys are often stored as part of the user's identity record which is available only after the user has been successfully authenticated. This further strengthens the case for MFA, as combining these technologies improves the overall level of data protection, adding overlapping layers of defense that reinforce the effectiveness of the individual security controls.

Hence there is clearly market demand for solutions that extend the benefits of encryption and multi-factor authentication to SMEs that do not have the same resources as their large corporate counterparts. However, there are further hurdles to overcome, the first of which is emphasized in Figure 6 below:

FIGURE 6

Importance of Specific Controls for Data Protection



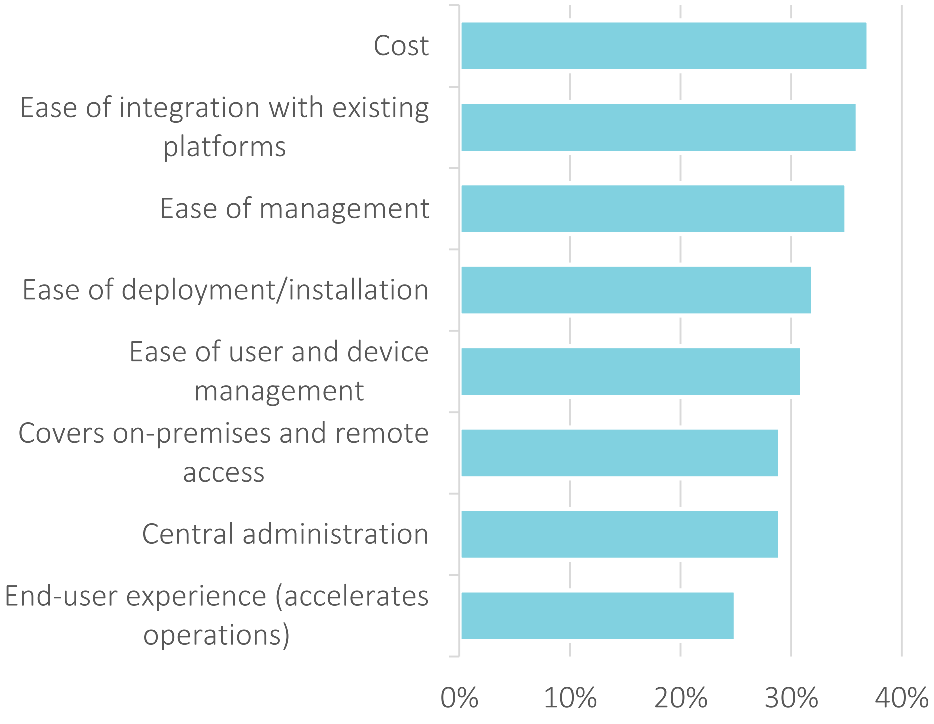
Source: IDC, 2017

Data protection is a complex area and the approach that each company takes to addressing it depends on business considerations specific to the organization. Nevertheless, as Figure 6 indicates, organizations still place a large degree of trust in the password system which, despite best efforts and best practices, does not provide the same level of protection that the combination of MFA and encryption can. Consequently, the sense of urgency or necessity to invest in these solutions is absent, and an educational effort on the part of market players and security experts is required to underline to end users how these technologies can make a significant difference to their security stance. IDC believes that much greater attention should be paid to MFA as a fundamental enabler for improving both data and system security.

According to the survey data, the second hurdle is cost. As can be seen from Figures 7 and 8 below, this is a critical consideration for both MFA and encryption. As noted above, organizations continue to allocate a significant portion of their security budgets to technologies that: 1) they have already deployed, and 2) they are familiar with both in terms of use of the technology and the benefits that it provides. To date, there has been limited market availability of either MFA or encryption solutions that are affordable from the perspective of a typical SME's security budget, as most solutions are targeted at large enterprises. In addition, there are further costs associated with the maintenance of these solutions.

FIGURE 7

Selection Criteria for Multi-Factor Authentication

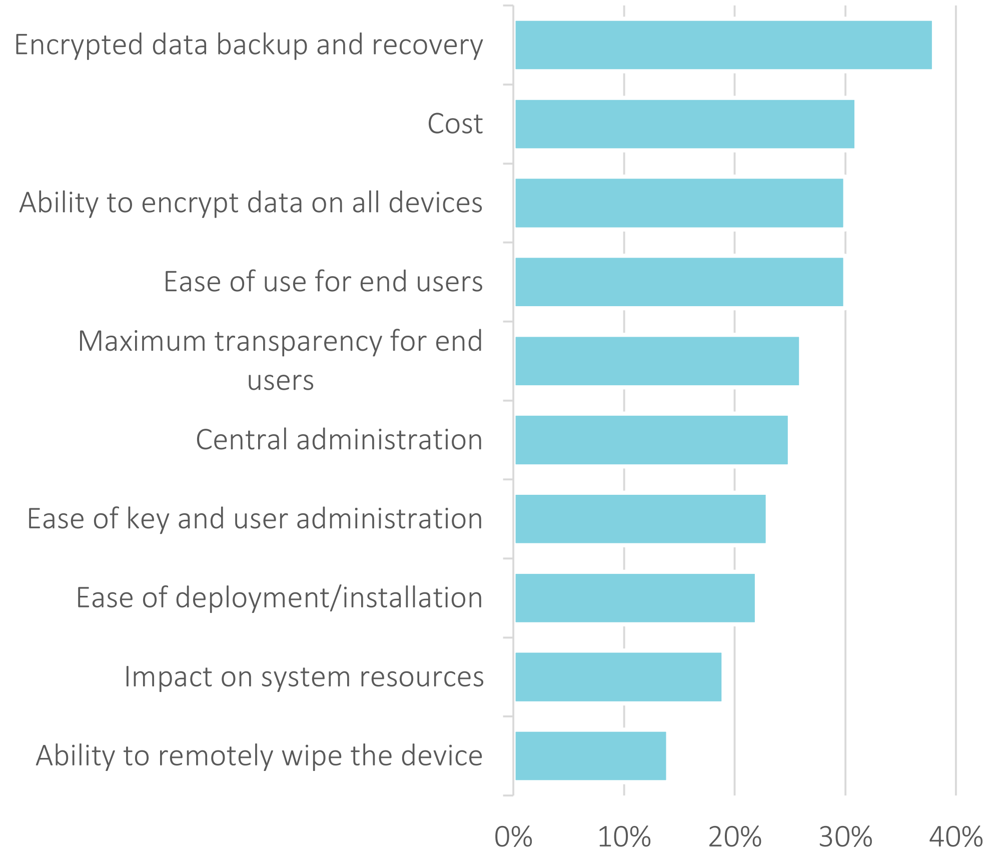


Source: IDC, 2017

The third hurdle associated with multi-factor authentication is ease of use. As with encryption, this is a multifaceted challenge that includes ease of use from both the end-users' and solution administrator's perspective. The selection criteria for MFA and encryption are slightly different, as can be seen from Figures 7 and 8. According to the survey, the MFA priorities are more around solution administration and integration of the solution with platforms already in use. This is easily explainable, as the full benefits of MFA are best realized when the technology is used throughout the whole application stack (i.e., in the system and application layers).

FIGURE 8

Selection Criteria for Encryption



Source: IDC, 2017

A slightly different picture emerges when looking at the selection criteria for encryption. While cost is still one of the most important factors, it takes second place to backup and recovery. Indeed, encrypted data backup and subsequent recovery contains several challenges, the main being key management. A common practice is to assign a key expiration date and, consequently, it is important to either keep the key if it has been used to back up data, or re-encrypt the backup with a new key, which is not always feasible and certainly not very practical. The situation is further complicated by key revocation for any reason, including loss of the device or media containing the key.

The ease-of-use challenge has been firmly attached to cryptography for many years. There is a general user perception that cryptography is one of the more difficult technologies to deploy and maintain. Working with encrypted data assumes that the sender is able to encrypt the data and that the recipient can decrypt it regardless of the device they are operating on and as seamlessly as possible, ideally without any additional user interaction other than the request to encrypt the data. This perception is corroborated by the selection criteria survey responses. It is of ultimate importance to understand that management complexity for any encryption solution consists of several parts, all of which should be addressed by vendors to make their solutions attractive.

If the ease-of-use focus for MFA is on the solution administration side; for encryption, this focus shifts to the user. Transparency and the ability to encrypt the data on all devices are more important for solution adoption, although this does not mean that ease of installation, deployment, and user and key management are unimportant.

The order of selection criteria simply reflects the fact that users will not use encryption if they are unsure whether the recipient is able to decrypt the data or if there are other possibilities for the data being undecipherable. Companies also highlighted the importance of the ability to encrypt data on all devices, which is becoming vital in today's business world where most users utilize at least two devices intensively (PC and smartphone).

ESET Offering

ESET is a Slovak IT security vendor that has become a force in the worldwide market with its endpoint protection suite. The vendor states that its goal is to ensure that everybody from consumers to large enterprises can benefit from the opportunities and protection that technology offers. Like many other antimalware vendors, ESET has recognized that there is significant opportunity to deliver more robust and comprehensive protection to its customers, and has consequently expanded its offerings. The vendor recently acquired two companies (FireID for authentication and DesLock for encryption), and has worked rapidly to integrate them into its offerings. In particular, these acquisitions enable ESET to provide multi-factor authentication and encryption at price points that are attractive to SMEs — a segment that has been largely underserved until now. However, these solutions are also sufficiently scalable to serve large enterprises.

As noted, ESET is an established antimalware player with solutions that cover both endpoint and server protection. Complementing these are now MFA and encryption offerings that significantly improve defense through the addition of further dimensions, as detailed below.

Multi-Factor Authentication

ESET Secure Authentication

ESET's authentication solution incorporates several main principles that properly address the market concerns outlined in the previous section. Designed for easy installation (taking only minutes), the product reduces the number of potential installation issues, not only by verifying system readiness, but also by providing user support if additional components need to be installed. Furthermore, the installation process automatically detects installed applications that are able to benefit from ESET Secure Authentication. This includes web-based productivity, remote access, and cloud services applications, as well as local logins.

ESET Secure Authentication is deployed on-premises and can be directly integrated with existing platforms through the API or through a custom authentication module developed with available SDK support modules developed in Java, PHP, and .NET. Integration possibilities are further expanded by Active Directory Federation Services (ADFS) support, meaning services like Office 365, Google Apps, or any other service supporting ADFS integration can benefit from ESET Secure Authentication.

ESET Secure Authentication favors mobile platforms, on which the required software can be easily installed, and with the ability to deliver one-time passwords (OTPs) via data and SMS services. While adoption of ESET's MFA solution does not require any hardware modules, it provides additional operational flexibility by supporting existing OTP hardware modules.

One feature that deserves special mention is push authentication. Push authentication further improves the usability of MFA by saving users from retyping OTPs (delivered by SMS or generated by a mobile application from their mobile device) into a login prompt. It also addresses out-of-band authentication security concerns voiced with regard to SMS-based over-the-air (OTA) services [3] Push authentication is available as part of the solution's mobile offering and supports Android and iOS devices, as well as wearables.

MFA Challenges

Active Directory integration is a requirement for ESET Security Authentication implementation, with Linux, Mac, and Windows platforms all supported. At the time of writing, the solution does not include a cloud offering: Authentication to the cloud is provided by Active Directory and ESET MFA through the ADFS, although MFA is not yet provided in SaaS form.

Encryption

ESET's DESlock Encryption Solution

ESET's DESlock Encryption solution is specifically designed with SME customers in mind, although the solution can be easily scaled to fit multinational enterprise environments. DESlock provides full backup and recovery capabilities as part of comprehensive remote management that also allows administrators to remotely remove access to the whole system or to specific data. In addition, the solution is able to decide if data should be accessible to administrators or not readable for anyone if the system is, for example, lost forever. The DESlock offering is divided into three editions that gradually increase the ability to apply encryption, from common business objects such as files, folders, archives, and email, to removable media and full disks. The tiered split into editions allows SMEs to choose the version that suits their needs and not overpay for the features they are not using.

[3] https://pages.nist.gov/800-63-3/sp800-63b.html

A mobile offering is also available and can be used in either unmanaged mode (when the device is not managed by policy from ESET's DESlock Enterprise Server) for which only password-based encryption (and not-key based) is available, or managed mode, where key management and policy enforcement is performed by the Enterprise Server. The two DESlock mobile encryption modes allow enterprises to augment their security practices while keeping the software on the mobile device itself, thereby simplifying provisioning. What makes ESET's offer particularly attractive is the fact that the Enterprise Server is free for any company with five or more endpoint licenses.

DESlock Encryption also goes a long way toward addressing end users' ease of use concerns. The software is built in a way that requires as little interaction during key usage as possible. Keys are combined into groups and associated with user groups making key management transparent for the user, while the recovery key that is generated simultaneously with the user key and server-side user key copy ensures key backup and recovery capabilities. Such redundancy makes data decryption possible even in cases when users have lost their keys together with their devices. The user's ability to interact with the key is limited, thus reducing the possibility of human error (e.g., when a user accidentally changes the key). Another usability effort addresses the integration of DESlock Encryption with other business applications. Integration with Microsoft Outlook, for example, is executed in the form of a toolbar, which further contributes to user-side ease of use.

The Enterprise Server requirements on the management side are very standard, necessitating the Microsoft Windows platform that is already used by the majority of ESET's target audience. The web-based management console almost guarantees a reduced learning curve in terms of policy and key management. In addition, the console can be accessed remotely in cases where a full-time on-premises security administrator is not available. The solution has been FIPS 140-2 validated and is capable of using various encryption algorithms, including AES with 128- and 256-bit key length.

Encryption Challenges

Overall, ESETs DESlock Encryption solution is a welcome step toward making security — once available only to larger enterprises — accessible to SMEs. There are, however, several factors that should be considered when evaluating the solution. While DESlock cleverly combines public and symmetric key cryptography to take complexity out of the user experience, there are still traditional challenges associated with the use of cryptography that need to be remembered. Some examples would be ensuring that the key is available to decrypt data from a backup made a long time ago, or minimizing copies of sensitive data and applying encryption to all remaining copies. While these and other best practice principles are not specific to ESET's product and are equally applicable to any encryption solution, users should not lose sight of the fact that practices and processes around encryption are as important as the security of key exchange channels and key storage.

At the time of writing, DESlock mobile encryption is only available on iOS, with an Android version in the works.

Conclusion

Penetration of both multi-factor authentication and data encryption remains low among European SMEs. There appear to be a few reasons for this, with cost high on the list, while there are also concerns about ease of use, ease of management, and ease of integration with existing platforms. In the case of encryption platforms, companies also highlighted the importance of the ability to encrypt data on all devices.

- Organizations claim they are concerned about data protection, yet they cite strong passwords as the most important control ahead of multi-factor authentication and data encryption at rest or in transit.
- Cost is highlighted as a key criterion when choosing an MFA or encryption solution. On the one hand, this presents a challenge, as organizations are still focusing on the bottom line and not on what is best for their organization. On the other hand, it presents an opportunity for any vendor with an affordable offering to claim a hitherto unpenetrated chunk of the market.

ESET's offering, namely the combination of three security technologies supported by a well-established vendor, opens up the possibility for SMEs to significantly improve their security posture, not only in terms of data protection, but also at the broader system infrastructure level. The next step is for the vendor to communicate this development to the market and help organizations realize the necessary steps to integrate these technologies, which ESET has made more accessible, into their infrastructure and business processes.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC CEMA

Male namesti 13
110 00 Praha 1, Czech Republic
+420 2 2142 3140
Twitter: @IDC
idc-community.com
www.idc.com