#2



STORMSHIELD

Businesses' digital transformation:

The start of a new cycle?

Survey of businesses' digital transformation, conducted in partnership with L'Usine Digitale
2019 edition

When the first Stormshield/L'Usine Digitale cybersecurity survey was published in December 2018, we gave you our thoughts on the security aspects of businesses' digital transformation.

One year on, where do things stand? Is digital transformation still a current topic?
For over a decade, people have tried to use the term "digital transformation" to describe the changes taking place in our societies, and, as a result, in our businesses. It's a lifetime in the age of the internet, which has turned our relationship with time on its head.

Before drawing a line – perhaps too hastily – under the expression, let's take a look back at it as a phenomenon.

Did the promised metamorphosis – the one that was supposed to bring businesses improved performance and better collaboration through digital technology – ever take place?

As is often the case, this white paper will show that the answer is "it depends": while significant disparities remain, companies are continuing to invest in digitalising their business and their offerings.

But they aren't the only ones to be gaining virtual ground: cyberattackers are undergoing a transformation of their own, and the consequences are all too real.

Ever more targeted and more sophisticated, ransom demands, data breaches, denial of service attacks and other forms of cyberattacks are becoming more and more common.

Half (48%) of the IT and digital departments we interviewed for this survey had been subject to one or more attacks over the previous 12 months. That's 13% more than the previous year – a figure that highlights the growing pressure that is being placed on IT ecosystems' security.

In this context, how are **businesses tackling their digital projects as 2020 approaches?** We've focused in particular on the ever more strategic issue of cybersecurity.

We hope you enjoy reading this white paper.

Contents

04 **Introduction: can we still talk about “digital transformation”?**

07 **The question of maturity**

13 **How can digital transformation and security be reconciled?**

22 **Preparing for tomorrow – today**

27 **Conclusion**

Can we still talk about "digital transformation"?

According to the figures from the 2019 edition of our survey, businesses' digital transformation is generally an ongoing process.

A growing proportion of interviewees even stated that this transformation has had little impact on the security of their IT systems and their data (16% compared to 5% in 2018).

Should we take from this that the biggest changes are behind us? Do we still need to talk about businesses' digital transformation?

For Frédéric Leblond, Head of IT Security for the port of Boulogne-Calais, it's a phenomenon that's alive and well

"For us, digital transformation is still an ongoing process. For example, at the end of 2018, we began a significant number of projects linked to infrastructure, messaging and even putting collaborative tools in place. We've made a lot of progress, but it's only the beginning."

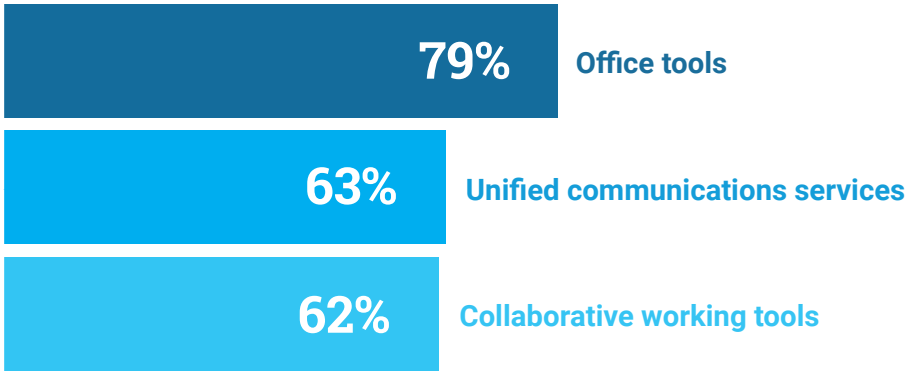
A variety of viewpoints

For Nicolas Arpagian, Strategy and Public Affairs Director at Orange Cyberdefense, it's an endless process of development

"There's never an end point with digital. It goes beyond simply accelerating transformation – it becomes a continuous process instead. That's why I prefer to call it a development or even a split. The real topic isn't that digital is transforming professions, it's that it's creating new activities and new roles."

Key figures for 2019

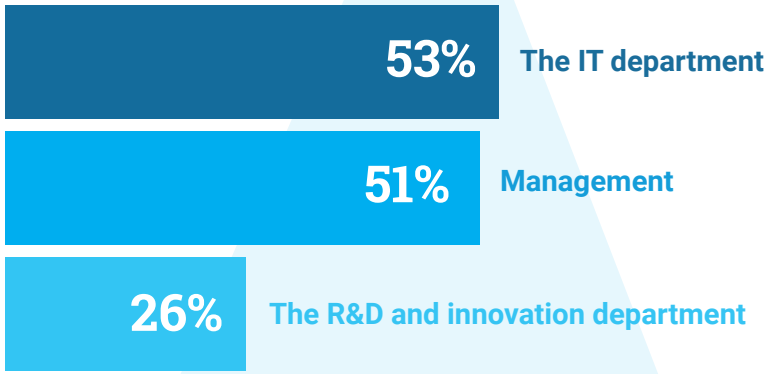
What are the most commonly implemented digital transformation projects?



Big companies leading the way on data

It is clear that big companies are leading the way when it comes to rolling out data transfer and data use projects (32% have plans for such projects, compared to 23% of respondents as a whole).

Who initiates digital projects within companies?

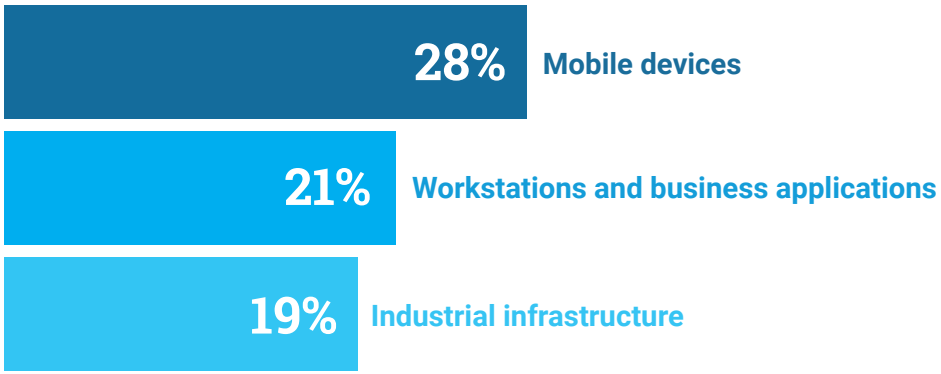


Dedicated departments more widespread within big groups

37% of respondents from big businesses mentioned their digital strategy department (compared to 25% of the total sample).

Key figures for 2019

What are the most vulnerable components in terms of cybersecurity?



Security for mobile devices and document-sharing services is better managed by big companies

81% of respondents who work in big companies reported that their mobile devices were sufficiently secured, compared to just 51% of the total sample. In addition, 88% were satisfied with the security of their document-sharing services (compared to 64% in smaller businesses).

What security solutions are in place within companies?



More than half of all companies have antivirus software, antispam software, network protection and a VPN.



More than a third of companies use an encryption solution, sandboxing software, or a security probe.

X5 Web Application Firewalls (WAFs) and Cloud Access Security Brokers (CASBs) were mentioned around five times more frequently than last year.

Section 1

The question of maturity

Despite these differences in how they perceive their environment, two thirds (64%) of respondents believe that their company made progress in terms of digital transformation in 2018.

So is it possible to say that a certain level of maturity has been reached?

While the global trend seems to indicate that this is the case, the disparity in terms of the realities experienced by those surveyed needs to be taken into account.

Digital transformation progress: the perception gap is growing

48%

of IT and digital departments think they are still behind

Half (48%) of IT and digital departments think that they are still behind (an increase of ten percentage points on last year!), while the proportion of business departments who report being "very far ahead" climbs by eight points to reach 13%.

Should this be taken to mean that IT and digital departments have become more critical?

Frédéric Leblond, Head of IT Security for the port of Boulogne-Calais, believes that above all, they are more realistic: "*faced with the increasing intensity of intrusion attempts and the extremely fast pace at which threats are developing, heads of IT security are on the front lines. This makes it easier for them to monitor the transformation and gauge the company's level of protection.*"

An economic intelligence manager who works at a major energy group recognises this: "*as a business division, we still often offer a user's viewpoint on issues such as these. It's difficult to realise what it represents when you only see part of the picture.*"

Nicolas Arpagian, Strategy and Public Affairs Director at Orange Cyberdefense, believes companies should question the benefit of comparisons between IT and digital departments and business departments: "*comparing yourself to your peers isn't necessarily enough. Digital has created new sources of competition, resulting in new services and offerings that have never existed before. This "unforeseen" competition can be a cause of real weakness.*"

The state of play and shared priorities within business

Despite these differences in how they perceive their environment, two thirds (64%) of respondents believe that their company made progress in terms of digital transformation in 2018.

Data and customer relations in the limelight while mobile apps are losing ground

IT and digital departments agree with their colleagues from other departments on the top three components of digital transformation projects:

Projects that have been deployed	Projects currently being deployed	Projects under consideration
• *collaborative working* • *traditional office software tools* • *unified communications*	• *digitalisation* • *business platforms* • *moving customer relations to digital*	• *using data* • *business platforms* • *digitalisation*

They also agree on another point: 22% of respondents do not plan to invest in rolling out mobile apps – ten percentage points higher than last year. This trend is even more clearly marked in IT and digital departments, where 33% of people report avoiding this kind of project (an increase of 21 percentage points).

Are we moving to security being included in digital projects by default?

6.5/10

the average score respondents gave to their company's level of preparation for the cyber-risks resulting from digital transformation. This figure is stable compared to last year's (6.6/10), but the same difference in perception can be seen between IT and digital departments and business departments: the first group give a score of 6.1, while the second give 6.8/10.

IS THE OPPOSITION OF THE *SECURITY BY DESIGN* AND *BUSINESS FIRST* APPROACHES STILL VALID?

"*The IT Department and the Head of IT Security were involved from the moment we began discussing the development of an in-house information management tool. Even now the tool is in place, it receives regular updates and undergoes regular testing.*"

This comment from an economic intelligence manager in the energy industry demonstrates that some businesses are fully integrating the concept of cyber risks from the design stage of their digital projects: this is the *security by design* approach.

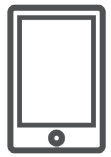
According to the survey results, it appears to be very widespread among businesses, with 85% of respondents reporting that security aspects are incorporated ahead of the project launch.

"*Culturally, this approach resonates strongly with stakeholders in the transport, health and communications sectors as well as with government departments, all of which put security above all else,*" says Rémi Decheron, a sales engineer at Stormshield Data Security. *On the other hand, other stakeholders, such as banks, take a more "business-first" approach: they have long prioritised quality of service, because in their field, information has a shorter lifespan and has therefore required less security. It was a way to avoid productivity drops.*"

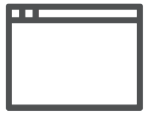
But under the influence of regulations such as the GDPR and faced with the pressure of repeated cyberattacks, the two approaches have tended to converge.

"*Despite differences in culture, priorities and pace, all businesses are now looking for ways to secure their digital transformation. To achieve this, we offer tools that take a "security by design" approach and meet the needs for maximum security expressed by some companies, while also meeting the essential business requirements that others prefer to focus on.*"

From the study, it also emerges that the four most vulnerable components in terms of cybersecurity are:



mobile devices (28%)



business applications (21%)



workstations (21%)



industrial infrastructure (19%)

In this context of partial and varied maturity, how can we continue to digitalise our ways of working and our tools with the best possible level of security?

Section 2

Ensuring a secure digital transformation

37%

the proportion of digital projects led by management in big companies

The survey reveals that management is generally involved in cybersecurity projects, particularly in how they are led (30% of the total sample).

Nicolas Arpagian, Strategy and Public Affairs Director at Orange Cyberdefense, sees this as essential for projects to be a success:

"The incorporation of security aspects into digital projects depends on the management. They need to be involved because it represents an investment by the company. Employees might share what they want to see, but it's up to the manager to give them the resources."

Security as a collective responsibility for the company

Digital security isn't a solitary exercise. On average, respondents had 3.4 stakeholders behind digital projects and 2.2 stakeholders involved in managing them.

In addition, to better take the challenges of cybersecurity into account, 61% of respondents plan to or have put in place organisational changes, such as creating a digital strategy department, for example.

The growing power of digital strategy departments

IT departments still put forward the most cybersecurity projects, and the smaller the company, the closer to the front line they are (59% in SMEs compared to 50% in big companies).

They also remain in the majority when it comes to putting forward digital projects (53%), but this figure is down 16% on the previous year. This can be explained by the fact that many companies have created dedicated departments, often called the "digital strategy department". These new entities are behind one in four digital projects in mid-sized companies, for example, and are behind almost four in ten projects in large firms.

IT departments still put forward the most cybersecurity projects

The legal department: a new player in cybersecurity issues

The European regulatory framework governing cybersecurity has been strengthened, in particular through the adoption of the General Data Protection Regulation (GDPR) and the Cybersecurity Act in 2018 and 2019 respectively.

In addition to increasing awareness of the challenges surrounding cybersecurity, the GDPR has helped to give personal data a "tangible" value, for example by setting a fine of 4% of global turnover for companies found to have failed to protect the data they process. This new regulation has also forced companies to categorise the data they handle and to set out a schedule for compliance.

Faced with these legal developments and with regulations "*that sometimes overlap*," according to Frédéric Leblond, the legal department is increasingly involved in the roll-out of digital projects. 60% of respondents say that they often or even always contact legal, compared to 46% last year. For respondents from IT and digital departments, a similar progression can be seen (57% vs 47% in 2018), and the number of people who never contacted legal fell by ten points.

"The group's policy at this level is fairly recent, but we now have a department responsible for digital transformation and a dedicated cybersecurity staff member in the legal department. Each business department is encouraged to make suggestions, but the decisions are made on a cooperative basis, with advice from the IT department and the information protection team on the technical means available and on compliance."

Economic intelligence manager
at a major energy group

The security department – more of an ally to digital projects than an obstacle

As understanding of cybersecurity issues grows, so does perception of the role of the security department: it is variously described by respondents as an advisor, a “police officer and protector”, and a source of support.

In the same way, taking security issues into account is not seen as an obstacle to the development of digital projects by 82% of those surveyed who work at mid-sized companies, and by 71% of those at big companies. However, it is perceived as such by almost 40% of SMEs surveyed.

Human resources: a key role in cybersecurity

Involvement: a key success factor in raising awareness

Raising awareness of best practices comes top of respondents’ list of drivers needed to face up to the challenges of cybersecurity. 72% of those surveyed reported that initiatives of this kind were in place in their company.

On this topic, Nicolas Arpagian, Strategy and Public Affairs Director at Orange Cyberdefense, highlights the importance of combining theoretical and practical teaching: “*whenever we do work to raise awareness of phishing among staff at one of our clients, we send a phishing campaign before and after the training to measure how effective it was.*”

Involving employees through practical cases that are taken from their daily lives allows everyone to feel like this is an issue that affects them, regardless of their role in the company, and to realise that the company is an “*interconnected social body.*”

However, Frédéric Leblond identifies two obstacles to this type of training activity: the first is the budget, which can be difficult to obtain, and the second is the choice of method. "*Although raising awareness is something that's really important, it's by talking about and demonstrating security that progress will be made in this area.*"

On this second point, a number of initiatives are flourishing, from workshops to newsletters to live demonstrations given by white hats, the ethical hackers who perform intrusion tests, for example, to ensure that systems are secure.

Security aspects also appear to be increasingly incorporated into training on new digital transformation tools (an increase of nine percentage points to 48%).

The specific requirements of cybersecurity recruitment

In addition to raising awareness among all staff, 48% of respondents have already recruited or plan to recruit cybersecurity experts. This figure rises to 67% in large businesses.

For Sylvie Blondel, Director of Human Resources at Stormshield, the first step to attract talented cybersecurity applicants is to publish a job ad that clearly expresses the company's needs in this regard. The challenge is then to make sure that the person has certain "*soft skills*" such as commitment, responsibility and reliability in addition to their technical abilities.

48%

of respondents have already recruited or plan to recruit cybersecurity experts

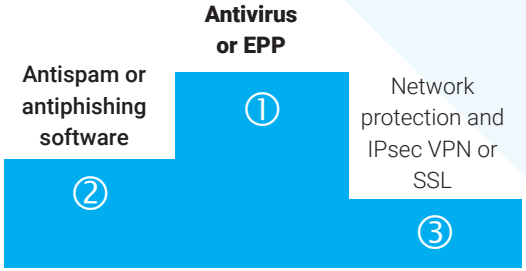
"*It's a collaborative and exhaustive process: there's an interview with HR, but there are also extremely complex technical tests, which are led by managers and which involve the whole team to encourage the new arrival's integration. This job profile has a strong ethical dimension to it, which is why we're looking for people who are both passionate and responsible.*"

Indispensable support from technology

In addition to the organisational developments already mentioned and the measures put in place in terms of awareness-raising and recruitment, there is also a technological aspect to the response to the cybersecurity challenges raised by digital transformation.

The now “traditional” security solutions that are adopted by more than half of companies

In the ranking of the most popular solutions that are in place, antivirus or EPP software takes 1st place (60%), closely followed by antispam or antiphishing software (59%). Network protection and IPsec VPN or SSL share third place (54%).



Almost

75%

of people surveyed mention that new security solutions have been rolled out or that there are plans to do so.

The boom in web applications has boosted WAFs

Among these solutions, Web Application Firewalls (WAFs)[1] have seen significant growth: 41% of respondents report having put such a firewall in place, compared to 8% last year, in the wake of increasing use of web apps such as Google Docs, Office 365, and Gmail. Large companies are particularly keen on them, with 61% reporting that they have implemented a WAF.

"*WAF solutions analyse, for example, the content of web pages or check transfer protocols such as http or https. They also offer protection against attacks such as SQL injection or cross-site scripting (XSS) that specifically target web apps. Finally, they can also check data to ensure it complies with the security policy,*" says Stéphane Prévost, Product Marketing Manager at Stormshield.

[1] Compared to a traditional firewall, WAFs specifically control access to web apps and ensure they remain protected.

An extremely varied range of solutions depending on company type

According to the results of the survey, e-mail encryption is a reality in half of all big companies, compared to a third of SMEs and mid-sized firms. Similarly, 52% of respondents from big companies report using two-factor authentication (2FA), compared to fewer than 20% of SMEs and mid-sized companies. Another example is the use of SOAR (Security Orchestration, Automation and Response) solutions, which are in place at a third of large companies but fewer than 10% of mid-sized businesses and SMEs.

CASB

CASBs' popularity in big companies

Cloud Access Security Brokers (CASBs) are solutions that control access to the cloud. In 2019, almost 20% of respondents report having deployed such a solution in their companies, compared to 4% in 2018. This growth is primarily driven by big groups, 41% of whom have implemented a CASB, compared to 18% of mid-sized companies and 7% of SMEs.

Why are so many big companies using CASBs?

"*This solution is in keeping with the current trend among companies and in the IT world of using cloud services to avoid having to maintain in-house services,*" explains Stéphane Prévost, Product Marketing Manager at Stormshield.

"*Firstly, a CASB allows access to an app to be managed on a user-type basis. It also secures data by using tokens, and it protects the cloud area from threats because it controls what is uploaded and by whom. "Finally, a CASB can partly tackle the problem posed by shadow IT because it gives full visibility regarding who's using what.*"

The budgetary aspect of cybersecurity

As we have seen, a secure digital transformation requires human and material resources – and therefore investment.

"*During the implementation of our collaborative working tools, we decided on a two-stage security process for our project, with a budget of between 1% and 10% of the total project amount on each occasion,*" says Frédéric Leblond, Head of IT Security for the port of Boulogne-Calais.

This figure of 1-10% of the budget for a digital project being allocated to security seems to broadly reflect a standard, as almost half of respondents reported spending this amount. Only 20% of them would spend more. Asked about this, almost a quarter of IT and digital departments report spending more than 10% on digital project security – an increase of six percentage points in a year.

It should nonetheless be pointed out that more than 40% of the sample said they were unable to answer this question due to lack of information, which clearly indicates that the topic remains sensitive or even confidential, even within companies.

It therefore seems unlikely that average budgets are very high. But less than a third (27%) of respondents said they were concerned by the lack of financial resources to prevent risks in the future. The public sector is an exception on this point, however, as the figure rises to 45%.

Paradoxically, across the entire sample, only 10% give financial resources as an area for improvement in terms of cybersecurity in their company.

Section 3

Preparing for tomorrow – today

The lack of financial resources is therefore not the primary concern for survey respondents. Nor is the difficulty of defining the role each party has to play in security efforts, as this was mentioned by just 27% of the sample, down 15 points on last year.

But, then, what are the cybersecurity challenges that businesses will face in the coming years?

With geopolitical issues that interfere with technological choices, automation, increasing attack surfaces as previously closed environments are opened to the internet, sharing of information via the cloud, and increasingly intense regulation, there are certainly plenty of areas of concern as 2020 approaches.

Mobility and the cloud are on everybody's minds

Topping the list of future cybersecurity challenges, almost half (45%) of respondents mentioned employees' increasing mobility, ahead of lack of user knowledge. Using the cloud took third place with the rapid pace of change of IT systems.

~1 in 2

respondents list employees' increasing mobility as the biggest challenge

According to the economic intelligence manager in the energy sector, *"the cloud raises real questions from the information security viewpoint. The issue is how to share data with people who are authorised to have access to it while protecting it from human error and from malicious acts."*

Whether for projects linked to industry 4.0 or to more general digital transformation projects, there is increasing demand for sharing information via the cloud. And the need to protect sensitive and/or personal data is increasing with it.

Big groups are thinking about Big Data and the Internet of Things (IoT)

Big companies take more of an interest in the challenges posed by the development of Big Data (52%) and the IoT (49%) than mid-sized companies (22% and 16% respectively) and SMEs (35% and 26%). However, along with mid-sized companies, they share greater levels of concern than SMEs about the development of artificial intelligence (44% vs 40%).

According to Stéphane Prévost, because connected objects are "*developed by companies that are not cybersecurity specialists, their products don't have cybersecurity built into them. Hacking these objects to carry out Distributed Denial of Service (DDoS) attacks, for example, is a real area of concern. That's why the Cybersecurity Act, adopted in June 2019, includes plans for European certification so companies can purchase devices from certified manufacturers.*"

Strengthening regulations are more of a concern for SMEs

Overall, 41% of SMEs list the regulatory framework as one of the "cyber challenges" of the future, compared to 28% of mid-sized companies and 34% of large companies.

41%

of respondents include the regulatory framework as one of the "cyber challenges" of the future

According to Nicolas Arpagian, "*2020 will be the year in which a certain number of legislation-related commitments come into effect. For many companies, this means continuing to ensure compliance with the GDPR. For others that have been designated "operators of essential services" (OSEs) following the definition of this status in the European NIS directive, it also means applying the security rules for which they are responsible. But all companies need to remember that they are living structures and should strive to maintain this compliance as the organisation develops and grows.*"

Automation as a response to lack of cybersecurity skills?

Lack of user awareness about cybersecurity issues came second among businesses' concerns (42%). We have already mentioned recruitment and upskilling teams to remedy this situation. However, many businesses are tempted to automate security, entrusting it to protection and detection technology. This may be to avoid certain human errors or to free up IT staff's time for tasks that bring greater added value.

Cyber security **2nd** place in the list of companies' concerns

Whatever the case, automation – made possible by the development of APIs and open connectors – is one of the potential approaches for greater security and simpler system administration.

Moving towards greater focus on user experience?

24% mentioned improvements to the user experience of security solutions

Among the challenges of the future, 24% of respondents mentioned improvements to the user experience of security solutions. Very often, when an employee chooses to use a tool other than the one recommended by the company's IT department, this is because the recommended tool does not meet one or more usability[1] criteria: useful, usable, navigable, accessible and/or understandable.

"*How can users be encouraged to adopt cybersecurity and its tools? This is a challenge that will grow in scale over the coming years, because it determines whether the solution put in place will succeed or fail,*" says Rémi Decheron, a sales engineer at Stormshield Data Security.

Because cybersecurity is everyone's business, there needs to be a trend towards developing the usability of cybersecurity tools to encourage everyone to adopt them.

[1] Usability is "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use".

Why are big companies particularly attracted to EDRs and Next-Gen EPPs?

IT and digital departments at big businesses seem to have been won over by Endpoint Detection and Response (EDR) solutions, which promise to offer full visibility in the event that an attack is under way.

"*In the case of sophisticated attacks, hackers try to remain "under the radar" for as long as possible to explore the infrastructure they have penetrated at their leisure. To do this, they launch other commands that indicate that an attack is in progress,* " says Stéphane Prévost, Product Marketing Manager at Stormshield.

It is these weak signals that EDR tools detect. They can also give tips on how to remedy the situation.

As for next-generation endpoint protection platforms, or Next-Gen EPPs, they combine an EDR's detection abilities with the blocking capabilities of a traditional EPP (antivirus, anti-malware, etc.). They are mainly intended for companies that can invest in cyber teams that have the expertise needed to analyse the signals highlighted by the EDR.

What will the flagship security solutions of 2020 be?

24% of IT and digital departments report that they are planning to deploy a Privileged Access Management (PAM) tool over the coming year, and 18% mentioned implementing a sandboxing solution.

Once again, projects vary greatly from one company type to another: while one in five mid-sized companies is considering deploying an Identity and Access Management (IAM) tool, SMEs have a greater tendency (27%) to invest in email encryption, while big groups are focusing on EDRs and Next-Gen EPPs (38%).

Conclusion

A new age for cybersecurity within companies

Maturity is “the final step in a process of growth”. Would a company that has reached maturity on the issues of digital transformation and cybersecurity therefore have digitalised its entire offering and processes and put in place all the tools needed to secure them?

That would be forgetting the new order that is an inherent part of this new environment: with coding, nothing is set in stone.

Change is the new constant. Transformation is no longer a linear road but a way of working. As for the threats of the future, they haven’t been invented yet – so how can companies make plans to protect themselves from them here and now?

A number of companies have reached a key milestone, moving from awareness to action to secure their digital transformation. But maturity is probably not the best term to describe the stage we are entering.

Nicolas Arpagian, Strategy and Public Affairs Director at Orange Cyberdefense, prefers to talk about a “sequence of responsibility”. “*In the past, the people who were aware of the risk put security measures in place. Then, awareness of this risk became more widespread, and as the threat became tangible, more and more players sought to protect themselves. We are now entering a third stage of development in which we are also protecting ourselves to avoid being found liable in light of the new legislation. In the same way, financial agents, insurance companies, investors, and ratings agencies are beginning to ask for accounts on this basis – this is a new phenomenon.*”

Whether we are in the age of maturity or of liability, three fundamental attitudes are essential for companies that don't want to jump on the bandwagon:

Develop a security reflex

Faced with ever more present threats, businesses have to continue investing in cyberprotection and threat detection solutions. The security-by-design approach and automation must not ignore the human aspect of cybersecurity.

Accept the risk

The determined nature of cyberattackers, who are motivated by colossal stakes, makes attacks inevitable: sooner or later, every company might be a victim, regardless of how much they have invested. However, it is possible to pre-emptively improve an organisation's cyber-resilience, helping it to minimise the impact.

Think of the company as an ecosystem

Yes, all companies are affected. Today's hackers target any link in the logistics chain to reach their target. This means that it is essential that companies have a global vision of their digital ecosystem, including service providers, suppliers, customers and all of the company's contacts. **Cybersecurity has become a collective responsibility for private and public organisations alike.**

Sources and references

2019 cybersecurity survey, Stormshield/L'Usine Digitale

Methodology:

Self-administered online questionnaire, completed between 1 July and 26 August 2019 by 233 decision-makers from IT/digital departments and from business departments, from all business sectors and companies of all sizes.



STORMSHIELD

Europe's leading cybersecurity firm and a wholly-owned subsidiary of Airbus CyberSecurity, Stormshield offers trusted solutions that are approved and certified at the highest level. The software publisher offers the broadest range of protection of all the holders of security visas issued by ANSSI (the French national agency for IT system security).

www.stormshield.com