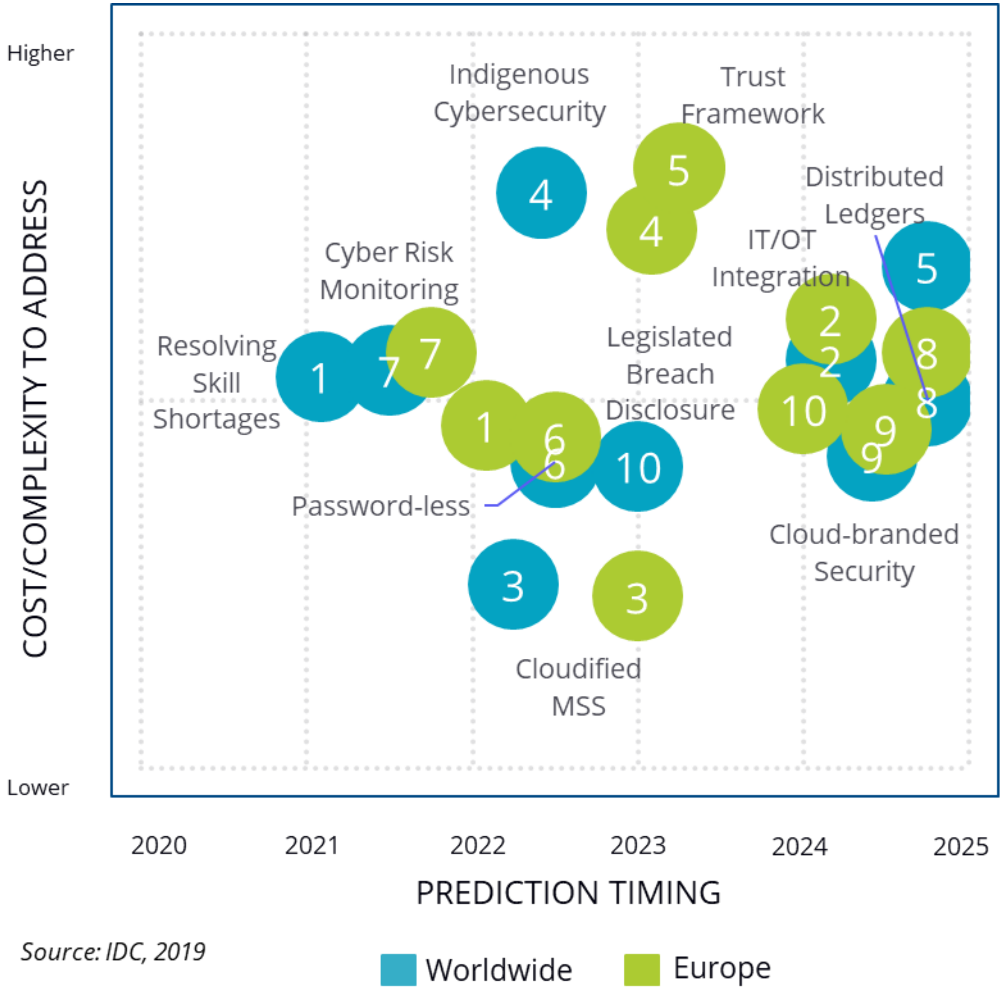
IDC FutureScape: Worldwide Security and Trust 2020 Predictions — European Implications

Mark Child, Research Manager
Romain Fouchereau, Research Manager
Ralf Helkenberg, Research Manager
Konstantin Rychkov, Research Manager
Claudio Stahnke, Senior Analyst
Dominic Trott, Research Director

January 2020

IDC FutureScape:
Security and Trust Worldwide & European Implications



Source: IDC, 2019

1 Regional Prediction 1: Resolving Skill Shortages
Hampered by perpetual security skill shortages, by 2022, 50% of tier 1 security operations center (SOC) analysts in Europe will permanently elevate their productivity and improve operational security metrics by harnessing artificial intelligence (AI) and machine learning (ML).

2 Regional Prediction 2: IT/OT Integration
Advancements in operational technology (OT) visibility tools will propel 66% of major European industrial firms to adopt an IT-OT integrated approach to security monitoring by 2024.

3 Regional Prediction 3: Cloudified MSS
Shifting of workloads to the cloud is shifting consumption of managed security services (MSS), and by 2023, 35% of European MSS customers will be served by cloudified MSS providers.

4 Regional Prediction 4: Indigenous Cybersecurity
Driven by rising aversion to "foreign" technology, 20% of developing markets in Europe will mandate the use of indigenous cybersecurity vendors to secure government and critical infrastructure by 2023.

5 Regional Prediction 5: Trust Framework
With the business criticality of digital trust rising, 55% of European spending on security services will be devoted to developing, implementing, and maintaining a ‘trust framework’ by mid-2023.

6 Regional Prediction 6: Passwordless
Intolerant of trade-offs between superior digital experiences and identity assurance, consumers demand both; by 2022, 30% of consumer online transactions in Europe will be high trust and passwordless.

7 Regional Prediction 7: Cyber-Risk Monitoring
Brand and attentiveness to cyber-risk have become tightly entwined, and by 2021, 75% of large European companies will embed cyber-risk monitoring into their business planning and quarterly reporting.

8 Regional Prediction 8: Distributed Ledgers
Explosions in data and analysis force the adoption of edge computing; to guarantee data provenance and security, 25% of European enterprise data will reside in distributed ledger systems by 2025.

9 Regional Prediction 9: Cloud-Branded Security
Innovation, opportunity, and market demand collide to place hyperscale cloud providers directly and permanently in the security business; by 2025, 9% of their revenue will be attributed to security.

10 Regional Prediction 10: Legislated Breach Disclosure
Effectively combating attacks by nation-states and cybercriminals is data dependent, and by addressing this dependency, 70% of European markets will legislate full cyberbreach disclosure by 2024.

Security and Trust: Worldwide Drivers

The complete list of drivers for all IDC FutureScapes can be found in *Critical External Drivers Shaping Global IT and Business Planning, 2020* (IDC #US45540519, October 2019). Of those drivers, the following seven will have the greatest impact over the next five years in the areas discussed in this document:

- ✓ **The age of innovation**: driving the future enterprise
- ✓ **The platform economy**: competing at hyperscale
- ✓ **Sense, compute, act**: maximizing data value
- ✓ **Crisis of digital trust**: escalating threats mandate strategic responses
- ✓ **Intelligence everywhere**: AI's opportunity and implications
- ✓ **Rising customer expectations**: more convenience, customization, and control
- ✓ **The future of work:** agile, augmented, borderless, and reconfigurable

For additional details on the above drivers, please refer to report *IDC FutureScape: Worldwide Security and Trust 2020 Predictions* (IDC #US45582219, October 2019).

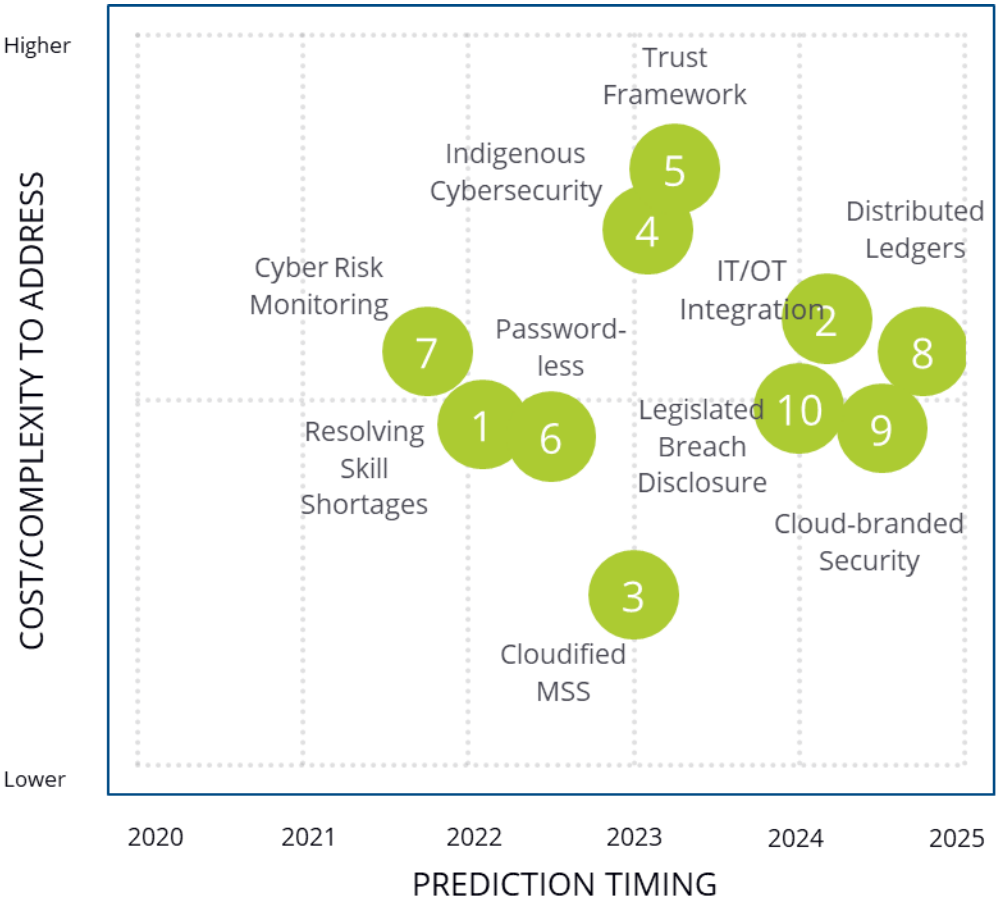
Security and Trust: European Situation Analysis

- **Political uncertainty undermines trust.** The U.K. is racing toward the European Union (EU) exit door, a situation that has also stirred up uncertainty about the futures of Scotland and Northern Ireland within the union. Spain has had four general elections in the past four years as regional, social, and economic differences drive separatist and extreme movements. In Italy, the right-left divide has led to multiple government collapses in the same timeframe. The moderate French president's approval ratings have slid so far that a November poll suggested he would lose to a far-right candidate if France were to have an election "today," while Germany's long-serving leader is stepping down, partially because of the rise of nationalistic and anti-immigrant views that have empowered far-right parties. Central Europe is no stranger to turbulence either, with the governments of Poland, the Czech Republic, Hungary, Slovakia, and Romania all struggling with controversy of one form or another. At the same time, the specter of election interference looms large across the region: Cyberdisruption through infrastructure attacks, hack-and-leak operations, reconnaissance hacking, and identity falsification are all concerns for any state seeking to ensure a secure and fair election. These concerns undermine trust in democratic institutions — even more so as those institutions transition to digital platforms for governing and engaging with both enterprises and citizens.

- **Regulators walking a fine line.** In many ways, the European Union has been the digital vanguard, with legislation such as the General Data Protection Regulation (GDPR) seeking to safeguard the rights and privacy of its citizens without impeding the ability of enterprises to do business. Other areas under consideration for regulation by the EU include increased protection around connected devices and the Internet of Things (IOT), as well as around the use of AI. Cybersecurity risks around both IOT and OT have been widely documented, while the debate is extensive around AI and ethics. These areas are complex and far reaching, and it is important that legislators improve protections while allowing organizations to continue doing business and building the trust required for digital enterprises.

- **Regional differences underscore security maturity.** Although the EU acts as something of a leveler across the 28 (soon to be 27) states within the bloc, differences in maturity, wealth, resources, and transparency impact security markets. The countries of northern and western Europe are considered more economically stable, technologically advanced, politically transparent, and generally more developed than those of the southern and eastern Europe. While major organizations in the west increasingly take a strategic, risk-based, and often governance-structured approach to cybersecurity, many in the east are still focused on operational priorities, lacking the budget and resources to embark on the proactive initiatives they may wish to implement, particularly as they strive for secure digital transformation (DX).

IDC FutureScape:
Security and Trust European Implications



Source: IDC, 2019

1 Regional Prediction 1: Resolving Skill Shortages
Hampered by perpetual security skill shortages, by 2022, 50% of tier 1 security operations center (SOC) analysts in Europe will permanently elevate their productivity and improve operational security metrics by harnessing artificial intelligence (AI) and machine learning (ML).

2 Regional Prediction 2: IT/OT Integration
Advancements in operational technology (OT) visibility tools will propel 66% of major European industrial firms to adopt an IT-OT integrated approach to security monitoring by 2024.

3 Regional Prediction 3: Cloudified MSS
Shifting of workloads to the cloud is shifting consumption of managed security services (MSS), and by 2023, 35% of European MSS customers will be served by cloudified MSS providers.

4 Regional Prediction 4: Indigenous Cybersecurity
Driven by rising aversion to "foreign" technology, 20% of developing markets in Europe will mandate the use of indigenous cybersecurity vendors to secure government and critical infrastructure by 2023.

5 Regional Prediction 5: Trust Framework
With the business criticality of digital trust rising, 55% of European spending on security services will be devoted to developing, implementing, and maintaining a ‘trust framework’ by mid-2023.

6 Regional Prediction 6: Passwordless
Intolerant of trade-offs between superior digital experiences and identity assurance, consumers demand both; by 2022, 30% of consumer online transactions in Europe will be high trust and passwordless.

7 Regional Prediction 7: Cyber-Risk Monitoring
Brand and attentiveness to cyber-risk have become tightly entwined, and by 2021, 75% of large European companies will embed cyber-risk monitoring into their business planning and quarterly reporting.

8 Regional Prediction 8: Distributed Ledgers
Explosions in data and analysis force the adoption of edge computing; to guarantee data provenance and security, 25% of European enterprise data will reside in distributed ledger systems by 2025.

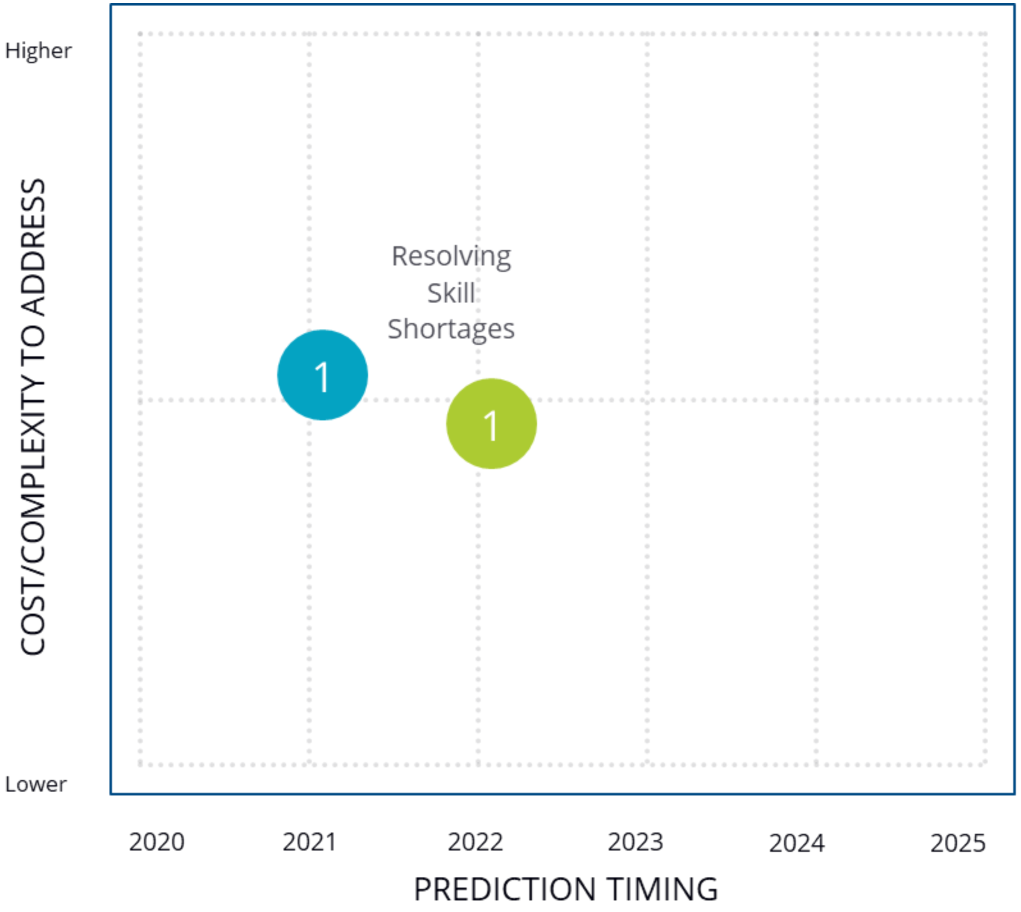
9 Regional Prediction 9: Cloud-Branded Security
Innovation, opportunity, and market demand collide to place hyperscale cloud providers directly and permanently in the security business; by 2025, 9% of their revenue will be attributed to security.

10 Regional Prediction 10: Legislated Breach Disclosure
Effectively combating attacks by nation-states and cybercriminals is data dependent, and by addressing this dependency, 70% of European markets will legislate full cyberbreach disclosure by 2024.

Prediction #1: Resolving Skill Shortages

Hampered by perpetual security skill shortages, by 2022, 50% of tier 1 security operations center (SOC) analysts in Europe will permanently elevate their productivity and improve operational security metrics by harnessing artificial intelligence (AI) and machine learning (ML).

- Enterprise networks have become heterogeneous, incorporating mobile, IOT, public/hybrid clouds, and software-as-a-service (SaaS) applications with internal and remote access by employees.
- With this diverse network footprint, monitoring is heavily human dependent in first-stage SOC functions and is doomed to fail against cyberadversaries that leverage cutting-edge technologies.
- Given these challenges and the difficulties in scaling up in-house talent, 35% of European respondents to IDC's 2019 security survey indicated that they plan to outsource security analytics, intelligence, response, and orchestration (SAIRO), including SOC, in the next couple of years. This will put strain on service providers (SPs), which are struggling to recruit the skills they need as demand grows at a fast pace.
- The multi-faceted nature of the European market, which encompasses diverse polities, languages, and cultures, means service providers have to offer support in local languages — a strong local presence is seen as a differentiator. As a result, resources are replicated across different geographies within the EU, increasing the need for talent.
- But there are positives. User behavioral analytics (UBA), powered by AI and ML, provides a security analytics layer to automatically creates profiles of devices/users from which statistical baselines of normal behaviors are established. AI provides a rich context of these events, prioritizes alerts from multiple sources, guides investigatory steps, and defines and initiates auto-remediation. The adoption of AI-powered tools to deal with the manual activities of lower-tier SOC analysts will enable them to focus on more qualitative higher-level analysis, helping the security workforce to better tackle the most serious threats to the organization.



Source: IDC, 2019

Prediction #1: Resolving Skill Shortages

Hampered by perpetual security skill shortages, by 2022, 50% of tier 1 security operations center (SOC) analysts in Europe will permanently elevate their productivity and improve operational security metrics by harnessing artificial intelligence (AI) and machine learning (ML).

IT impact

- Enterprise networks must integrate IT and security architecture. In practice, securing platforms and applications as changes or additions are being evaluated must become a standard operating practice.
- Workflows, especially the generation of IT tickets, must be considered a joint venture between security and IT.
- SOC managers must introduce processes that measure efficacy and lead to no-touch automation in as many instances as possible.
- AI-based tools will automate the most repetitive tasks, freeing up resources that service providers will be able to dedicate to creating a more tailored service for their end-users, improving their vertical expertise and geographical presence in Europe.

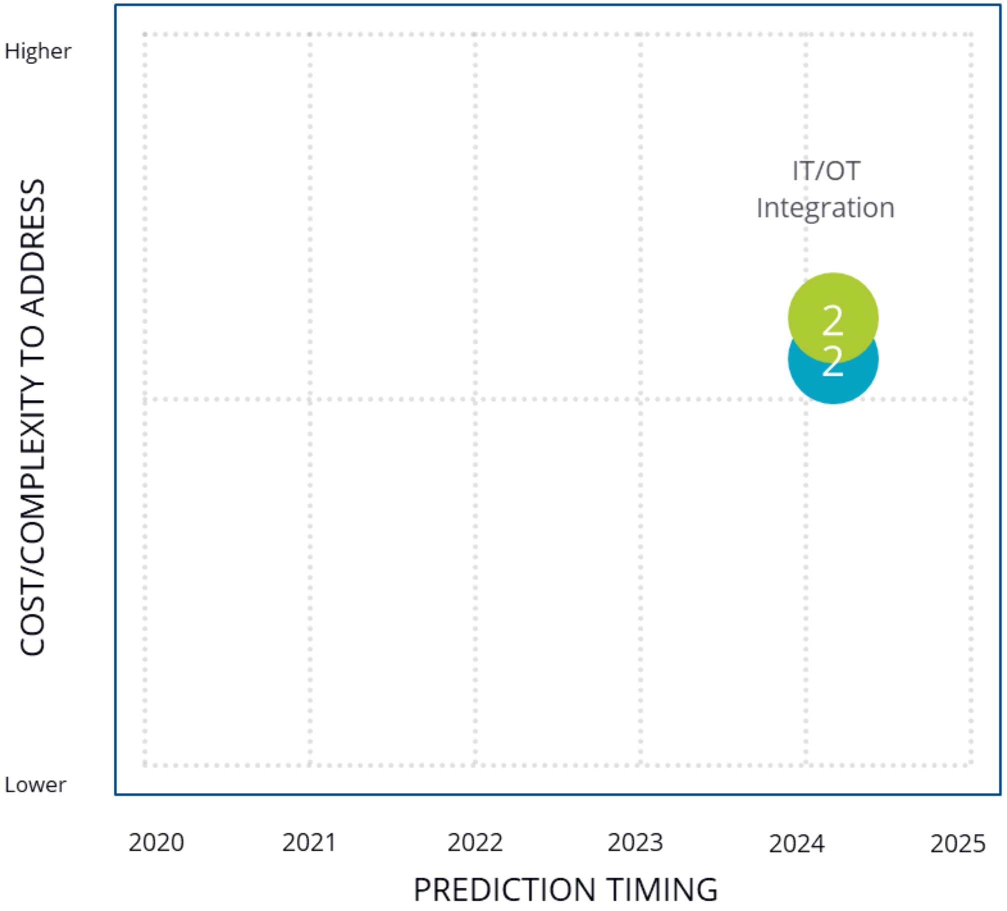
Guidance for Technology Buyers

- Understand exactly what telemetry each security appliance or platform provides. Pointing out anomalies is insufficient; the systematic application of priority ratings for alerts alongside clearly presented steps for investigation and remediation will be critical to scaling and improving SOC operations.
- Cross-train personnel in both basic IT and security skill sets. Ideally, security analytics removes the drudgery of assembling incident timelines, websites and IP addresses visited, and details on corrupted files and memory. In return, security analysts are folded into IT/OT functions. IT/OT personnel, however, still need a functional understanding of newly generated security alerts.
- AI tools need a vast amount of data to be properly trained, which could pose issues under GDPR, especially when coupled with user behavioral analysis. Organizations will have to be mindful of this and adopt a proper data governance strategy for processes that utilize AI.

Prediction #2: IT/OT Integration

Advancements in operational technology (OT) visibility tools will propel 66% of major European industrial firms to adopt an IT-OT integrated approach to security monitoring by 2024

- A shift of enterprise transactions from analogue channels to digital has brought many benefits, but it often favors the enterprise over the individual. Digital models must match social expectations if enterprises are to guarantee their ongoing relevance and success.
- Digital trust is key to successful IT/OT integration. Users and consumers expect enterprises to demonstrate that their data is being handled with due care and respect.
- According to IDC, only 26% of European organizations manage physical and data security as an integrated system (from IDC's 2018 European IT/OT convergence survey).
- Integrating IT and OT can increase an organization's vulnerability. But adopting appropriate security-related policies can help reduce the risk. This is an area in which tight alignment and collaboration between IT and OT executives can deliver positive results. Security must be a core element of any IT/OT convergence initiative.
- Europe benefits from the existing framework of regulations around data privacy — namely, from GDPR, ePrivacy, and the NIS Directive. The European Union Agency for Cybersecurity (ENISA) has already put forward some recommendations around the convergence of IT and OT, which should help European organizations with their governance models.



Source: IDC, 2019

Prediction #2: IT/OT Integration

Advancements in operational technology (OT) visibility tools will propel 66% of major European industrial firms to adopt an IT-OT integrated approach to security monitoring by 2024

IT impact

- The continued onslaught of ransomware infections has prompted increased awareness about the disruption cyberattacks can cause to IT and OT environments. Ignoring the risks caused by increased connectivity in OT environments is out of the question, as the production downtime and recovery costs caused by security incidents are steep. Due to the nature of OT operations, the safety of populations and the environment is also at risk should an attack be successful.
- European organizations are increasingly connecting data from OT environments to data analytics repositories, and CIOs are beginning to make addressing OT security risks a boardroom imperative to maintain the integrity of data and avoid any cyberattacks that may result from such connectivity.
- Providers of network and endpoint security products for OT environments should consider agentless visibility via a flexible deployment model that can be altered to provide incident response in the future.
- Integrated environments (and the products that underpin them) must appeal to both OT personnel, who need to understand the value of such integration, and the IT and security teams, which need to mitigate risks to acceptable levels.

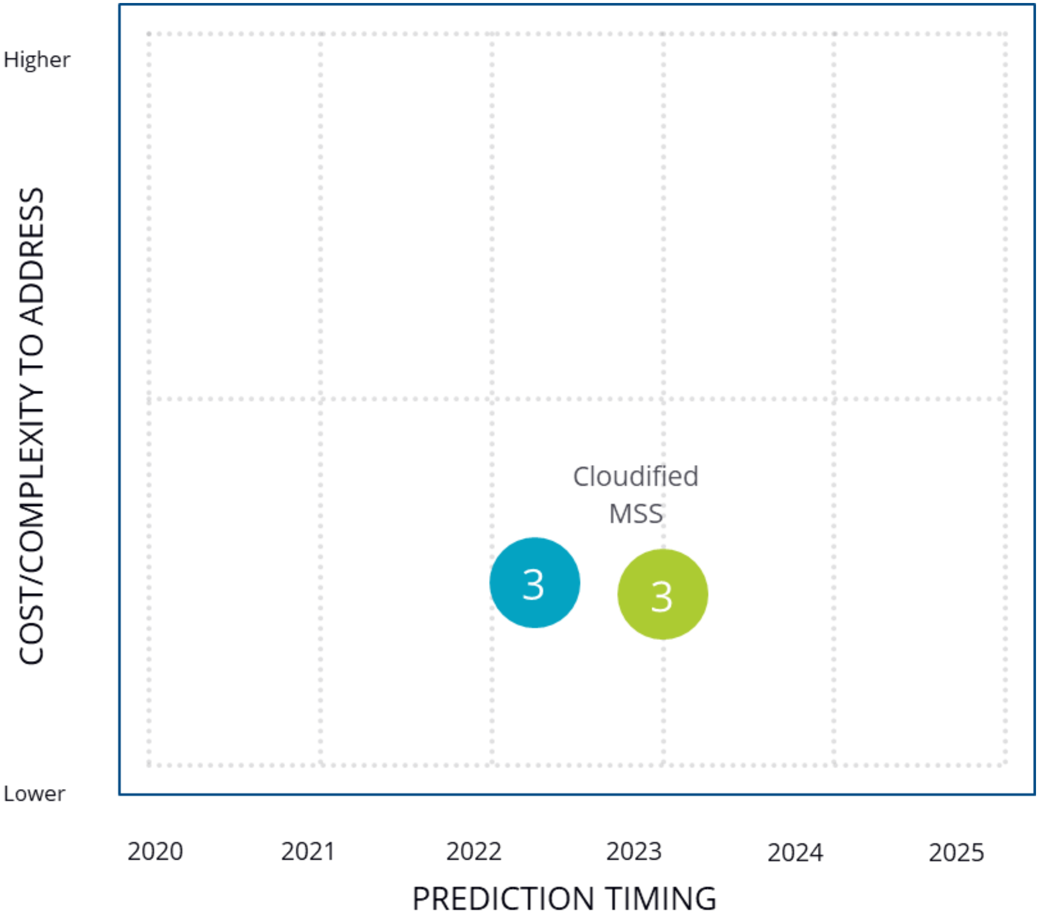
Guidance for Technology Buyers

- Think holistically before applying new policies. Security teams must first gain a clear understanding of what they are trying to protect before creating new policies and their accompanying enforcement mechanisms in an OT environment.
- Know your inventory. Conduct a thorough discovery exercise to document existing network enabled devices and their connectivity, communications protocols, and device firmware.
- Identify solutions that can comprehensively discover and accurately categorize OT devices and can monitor device behaviors using agentless and transparent approaches.
- Demand support from vendors for the establishment of basic security hygiene and best practices. This includes consulting and support services that assist enterprises in establishing enforceable data governance, risk management, and compliance policies.
- Despite convergence initiatives, OT will remain very different from IT, and IT security teams will not be able to replace OT staff nor fully take over operations — but it is very important to create the right collaborations between the teams to ensure the success of the project.

Prediction #3 – Cloudified MSS

Shifting of workloads to the cloud is shifting consumption of managed security services (MSS), and by 2023, 35% of European MSS customers will be served by cloudified MSS providers

- Workloads are moving to multiple public and private cloud instances, and these environments are under pressure to drive greater speed and performance. Currently, 27.5% of European companies are running multi-cloud environments.
- Delivery of services has changed with the migration into a "cloudified" and increasingly complex world; firms embarking on these migrations without comprehensive understanding often end up with with poorly configured solutions. However, if executed correctly, SaaS represents a cost-effective, infrastructure-driven MSS provisioning option.
- As organizations gain a greater understanding of trust and cloud services, their needs evolve, and more flexible and cost-effective security becomes a priority.
- As the top-four public cloud vendors (AWS, Microsoft, Salesforce.com, and Google) are all U.S.-based and control one-third of the European public cloud services market, data residency and portability concerns are center stage when it comes to provider selection, with considerable value to be found for Europe-based players.
- This incursion of sophisticated competitors leads to an increase in mergers and acquisitions of managed security service providers, which are already over capitalized in European markets.
- Europe lags behind the rest of the world when it comes to MSS penetration: These represent only 4.7% of the total expenditure for managed services, against a worldwide average of 5.0%. For that reason, cloud MSS provisioning will reach one-third of the customer base a year later than IDC predicts globally, yet growth will be at a higher pace.



Source: IDC, 2019

Prediction #3 – Cloudified MSS

Shifting of workloads to the cloud is shifting consumption of managed security services (MSS), and by 2023, 35% of European MSS customers will be served by cloudified MSS providers

IT impact

- As providers anticipate a shift in consumption models, the added value and flexibility of the services proposition will become crucial as organizations encounter more choices.
- As IT environments' requirements evolve, security will be of greater importance for those organizations with limited IT resources and smaller budgets, driving demand for MSS offerings delivered via an SaaS model.
- Both IT and security functions will shift from a “maintenance and control” position to one focused on monitoring, procuring, and reporting, increasing the importance of service-level agreement (SLAs).
- "Multi-cloud" security service providers with expertise in on-premises, cloud, and multi-cloud environments will grow their customer bases. Providers with a principal focus on legacy deployments that address only one type of environment will lose market share.

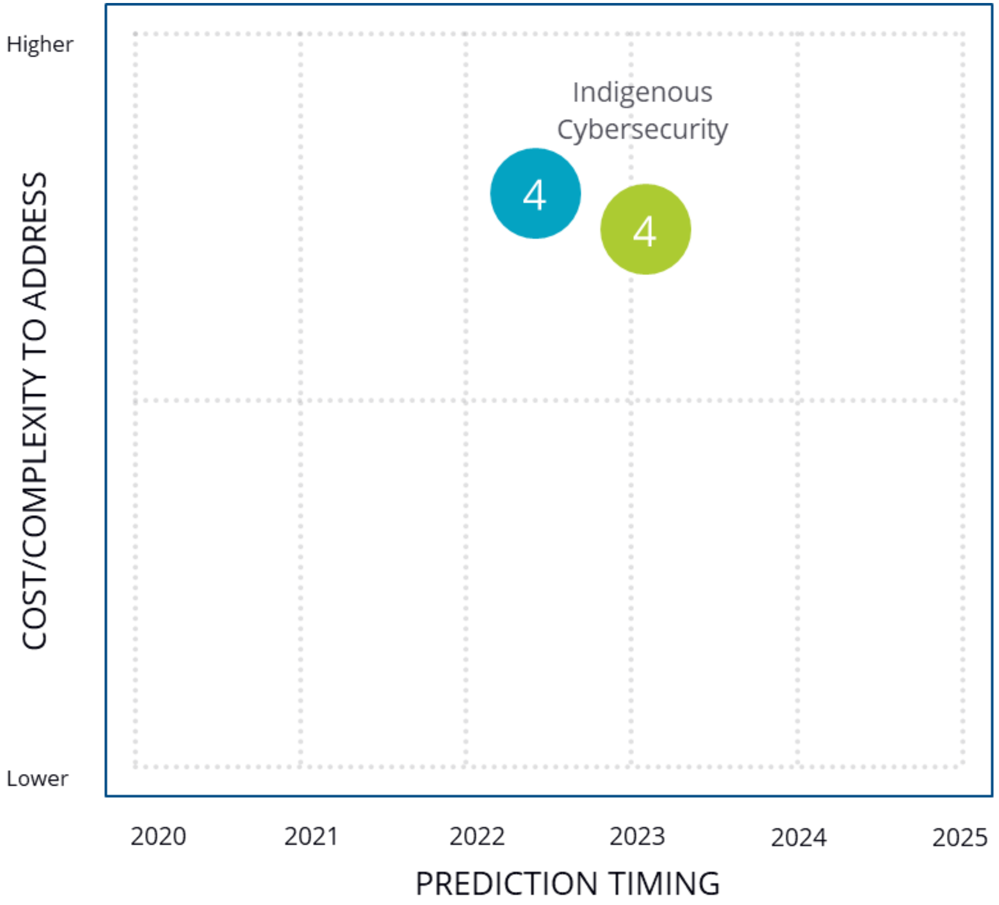
Guidance for Technology Buyers

- Evaluate your IT infrastructure, assets, and environment, and carefully review which services are suitable as a cloud service and which cloud environments are effectively serviced by managed security service providers (MSSPs).
- Perform risk assessments to objectively determine your organization's current security state and its desired future state. Evaluate MSSPs on how they can help you in planning and prioritizing your organization's path to improved security.
- Prepare the governance processes for onboarding and managing multiple MSSPs and managed services providers (MSPs) with meaningful SLA mapping and assessment.
- For compliance-heavy organizations, score service providers on their capabilities in optimizing configurations, onboarding, and building integration.

Prediction #4: Indigenous Cybersecurity

Driven by rising aversion to "foreign" technology, 20% of developing markets in Europe will mandate the use of indigenous cybersecurity vendors to secure government and critical infrastructure by 2023.

- Cyberwarfare is in the spotlight as more governments are attributing attacks to other nation states. Linked to this, and against a backdrop of rising nationalism, organizations and authorities in some markets are questioning their reliance on foreign IT security technologies to protect their critical systems.
- Europe is no exception to these trends: From political and election interference in France, Poland, and the U.K. to cyberattacks on critical infrastructure in Germany, Sweden, and Ukraine, cyberwarfare has impacted many European states. Attacks are frequently attributed to advanced persistent threat (APT) groups based in Russia and China, along with a few other states. Notably, those are among the most controlling when it comes to allowing global tech firms to sell in their markets. For example, it was reported that McAfee, Symantec, and SAP allowed a Russian defense agency to examine their source code in order to gain access to the Russian market.
- The above-referenced activities have created concern among European governments, with many taking steps to reduce their perceived exposure to this cyber-risk. Some vendors, such as Huawei and Kaspersky Lab, have been blacklisted when it comes to providing technology for government and critical infrastructure. In other cases, procurement might take a cautious approach to vendors that have shared their code with foreign governments.
- This creates opportunities for local and regional security providers from trusted markets, and Europe has no shortage of these: The likes of ESET, F-Secure, Sophos, Bitdefender, Avast, and Avira could all benefit. Additionally, governments may support local IT security start-ups and scale-ups that can provide additional tools and capabilities to replace the international technologies currently used to secure critical systems.



Source: IDC, 2019

Prediction #4: Indigenous Cybersecurity

Driven by rising aversion to "foreign" technology, 20% of developing markets in Europe will mandate the use of indigenous cybersecurity vendors to secure government and critical infrastructure by 2023.

IT impact

- Businesses deemed critical to national security will be given strict mandates on where specific vendor technology can and cannot be used within the organizations. Over time, these mandates may be backed by legislation. The EU adds a further layer of control here, with the potential for regulations and directives (e.g., the NIS Directive) to be developed and extended with guidance on tools and procedures where it is considered necessary to safeguard critical infrastructure within the Union.
- In some markets, government funding may be made available to support joint-venture start-ups, with the stipulation that intellectual property remains within the country or is dedicated to specific needs of government entities.
- Starting with universities, governments will create long-term cybersecurity skills road maps with the objective to produce more graduates with the required skills in their local markets. Some experts are also calling for cybersecurity education options to be made available even earlier in the academic career. Inclusion is also on the agenda, with many cybersecurity companies looking to attract more women, minorities, and people with disabilities to boost their workforces and bring in more diverse perspectives and skills.

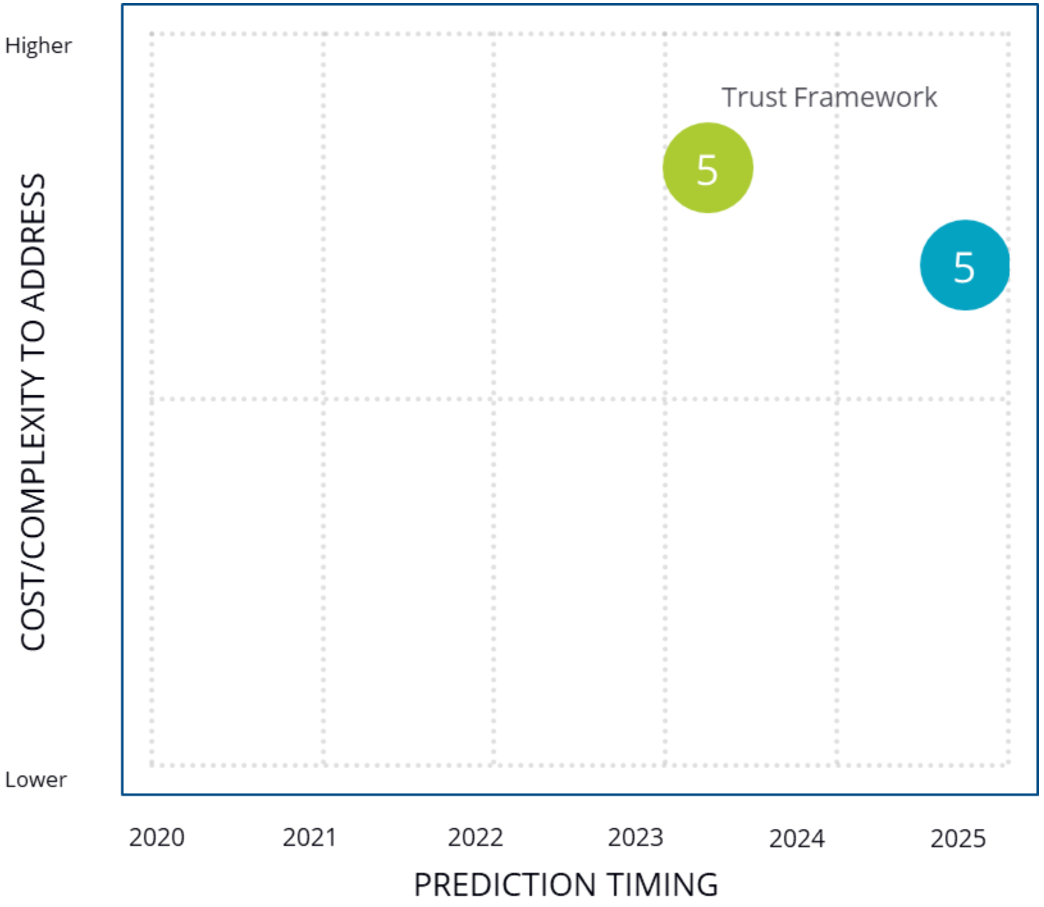
Guidance for Technology Buyers

- Understand where you fit within your government's view of critical infrastructure. If your organization falls within this definition, ensure you have a full audit of the security technologies in place and their countries of origin, as well as a strong defense of these choices should your government mandate the use of local technology. Should such an audit reveal potentially restricted technology suppliers, it may be worth proactively investigating alternatives and preparing a road map for migration.
- Explore with local education institutions their IT security development plans and provide feedback and guidance on where you see a requirement. The IT security challenge will not go away, so this is a long-term play.
- Identify the local security vendors in your market, and start creating partnerships that address your specific needs for the future.

Prediction #5: Trust Framework

With the business criticality of digital trust rising, 55% of European spending on security services will be devoted to developing, implementing, and maintaining a ‘trust framework’ by mid-2023.

- To succeed with digital transformation, enterprises must embrace "digital trust.”
- Europeans (and the European Union in particular) care about privacy and data protection. Privacy regulations such as GDPR are forcing companies to be more attentive to how they handle customer data, while bringing consumers new ways to control their data and tougher enforcement of existing privacy rights.
- The EU is shaping regulatory strategy on new digital technologies, such as AI, to reflect and enshrine European values and to ensure adherence to high ethical standards.
- To meet societal and regulatory expectations, European companies will lead in the development of "trust programs" to show customers, partners, suppliers, and business stakeholders that the risks are understood well and effectively managed.
- Trust-by-design models will be established by placing data privacy and cybersecurity as key enablers for driving customer centricity when generating new ideas, products, and services.



Source: IDC, 2019

Prediction #5: Trust Framework

With the business criticality of digital trust rising, 55% of European spending on security services will be devoted to developing, implementing, and maintaining a 'trust framework' by mid-2023.

IT impact

- IT, privacy, and security teams can be strong allies if they develop, from different angles, a common transformative agenda to build trust into corporate culture. With a growing proportion of business activity dependent on digital elements, the tighter integration of enterprise IT and business strategy is needed to translate technology risk into business risk. To mitigate business risk, meet regulatory compliance, and drive value from data, enterprises must have visibility of the entire data lifecycle; it is critical. To deliver digital trust, enterprises need to leverage the GDPR's call for privacy by design and, by extension, security by design into all new initiatives and maintain them throughout their lifecycles.
- Enterprises need to look more closely at the concept of resilience, which includes cybersecurity and governance. Resilience goes beyond being able to react to a breach or system failure to ensuring that all business mission-critical applications are "always on." The Threat Intelligence-Based Ethical Red Teaming (TIBER-EU) framework — an initiative of the European Central Bank (ECB) to ensure financial institutions adjust their cybersecurity programs by taking a cyber-resilience approach to strengthen digital trust — will be extended to underpin the EU's strategy of business cyber-resilience.
- Expectations of new technologies (notably, AI adoption) will include the proactive assessment of business impact and appropriate responses to safeguard brand reputation. EU regulation around new technology use (e.g., the ePrivacy regulation and EU commitment to regulate AI) will drive further activity.

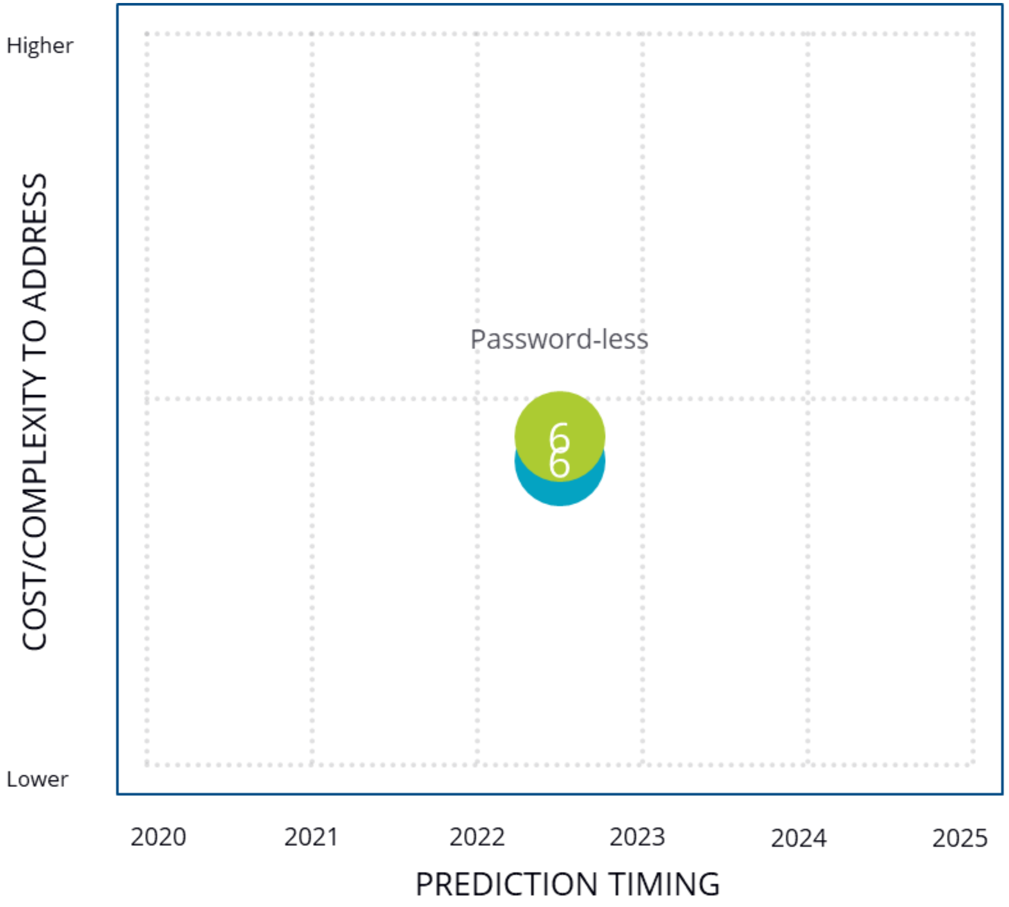
Guidance for Technology Buyers

- European security teams have seen success in driving up security awareness and hygiene by appointing "security champions" within lines of business. This can be developed by expanding the role to focus on trust more generally, or by seeking "trust champions" to accompany their security equivalents. These trust champions need clear responsibilities and objectives to establish accountability for managing and maintaining trust guidelines.
- Organizations need to build verifiable trust through a layer-of-assurance approach: contractual agreements, independent validation, integrated information security management systems, and secure architecture. Certification pursuant to the EU Cybersecurity Act may gradually become mandatory in the EU for critical products or activities. Businesses should monitor the state of adoption of cybersecurity certification schemes and/or consider certification once the schemes are available.
- Build on ISO 27001 to deliver a Privacy Information Management System (PIMS) with ISO 27701. The standard is the closest an organization can get to attesting to its adherence to the GDPR. Enterprises will also start to mandate compliance in their supply chains.
- IT, security, privacy, risk, and compliance teams need to build consistent enterprise-wide standards and metrics to support enterprise trust. This ought to include a focus on a corporate code covering points such as ethics, transparency, objectivity, and privacy. A particular focus must be placed on the ethical and trusted use of AI to support decision making. Deploy tools to automate compliance monitoring internally and externally (partners/suppliers), distributing consistent trust levels.

Prediction #6: Passwordless

Intolerant of trade-offs between superior digital experiences and identity assurance, consumers demand both; by 2022, 30% of consumer online transactions in Europe will be high trust and passwordless.

- The market has been clamoring for an alternative to password-based identity authentication for several years now, both from the perspective of frustrated users (who must manage anything from tens to hundreds of login credentials) and from their employers or those providing a product or service to their customers (and dealing with tens or hundreds of password resets per week).
- Despite the need for a silver-bullet solution, most consumers have seen no change and are still managing (or failing to manage) scores of text-based passwords and adhering to demanding requirements regarding password length and complexity for key applications.
- Nevertheless, authentication capabilities that leverage smartphones are improving with every new generation. Outcomes can be driven by the user base and vary according to the nature of those users: Consumers demand the most convenient and frictionless user experience (UX), while employees and contractors must accede to some security imperatives of their employers and partners. Tech-savvy younger generations may reject processes if they feel access is unnecessarily difficult.
- This will drive increasing adoption of federated single sign-on (SSO) using social media identities — at least for acceptable-risk communication and low-value purchase transactions — without requiring a one-time password (OTP). Fast Identity Online 2 (FIDO2) certificates built into smartphones and tablets are also driving change in the acceptance of security certificate use. The coupling of such certificates with biometric authentication technology will enable European consumers to use two-factor authentication (2FA) via a finger placement, phrase statement, or a quick eye scan.



Source: IDC, 2019

Prediction #6: Passwordless

Intolerant of trade-offs between superior digital experiences and identity assurance, consumers demand both; by 2022, 30% of consumer online transactions in Europe will be high trust and passwordless.

IT impact

- Password-based systems and unnecessary OTP confirmations will no longer be acceptable as low-cost techniques for consumer authentication.
- According to Capgemini/BNP Paribas, Europe will see 132 billion non-cash transactions in 2019, creating a challenge of scale for the mechanisms that enable those transactions. Identity and access management (IAM) solutions that do not scale and cannot support the safe collection of consumer data will reduce the number of visitors, shorten the time they spend on a website, and reduce the likelihood of a transaction.
- Retained consumer data must be safeguarded by the organization in a manner compliant with regulations such as the EU's GDPR. In some cases, this retained data must also be made accessible to data subjects.
- Facebook, Twitter, and other social media identity suppliers will challenge existing business-to-consumer leaders in providing a preferred authentication route for federated SSO capabilities.

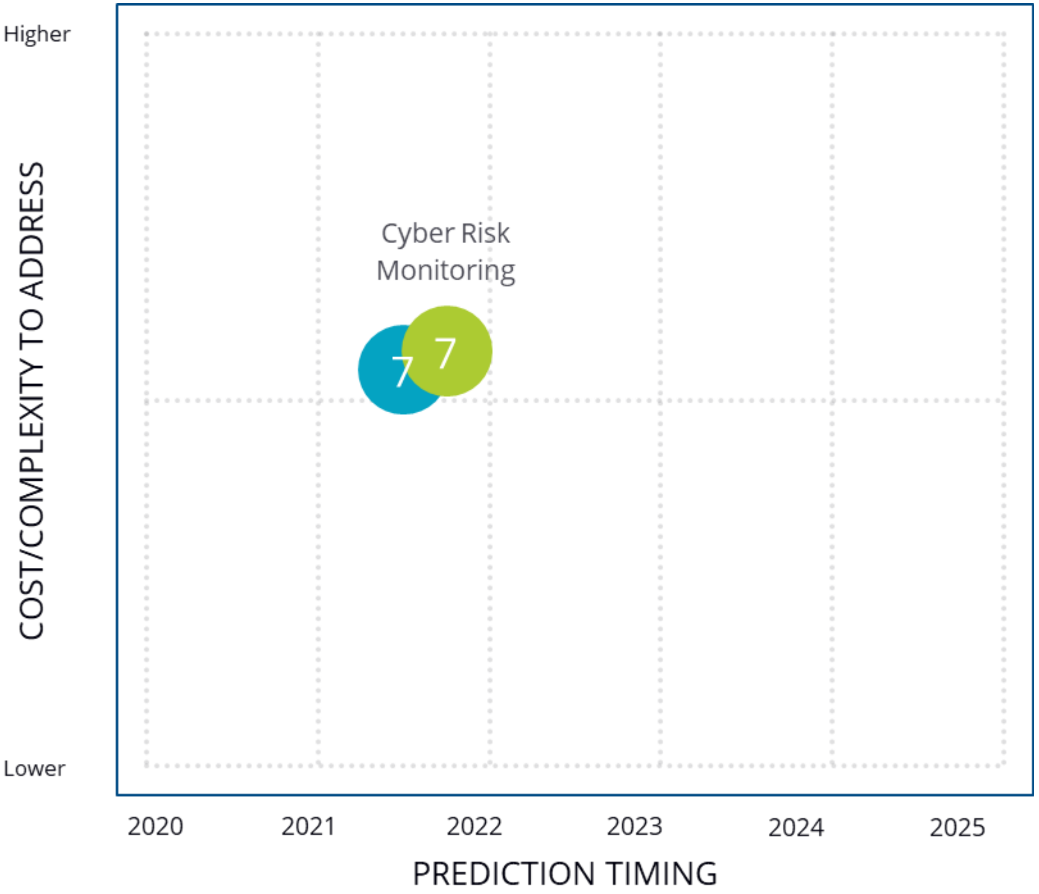
Guidance for Technology Buyers

- Any digital transformation project that exposes more of your environment to consumers is likely to require an identity and authentication technology upgrade. Born-on-the-web organizations will face fewer issues than those lifting and shifting on-premises solutions unsuited to supporting low-friction UX and authentication risks.
- Evaluate IAM solutions that can securely collect and retain consumer attributes, browsing habits, purchase histories, and other metadata that improves the overall customer experience. Knowledge of preferences will help direct suggested activities and target new offers to consumers most likely to appreciate such content.
- Produce professional YouTube materials to quickly and easily explain the benefits of a product or service and make these materials entertaining, as your consumers will increasingly be Gen Z. Gen Z will comprise 40% of all consumers worldwide in 2020, are twice as likely to connect to the internet using a mobile device, and typically spend 10+ hours online every day.

Prediction #7: Cyber-Risk Monitoring

Brand and attentiveness to cyber-risk have become tightly entwined, and by 2021, 75% of large European companies will embed cyber-risk monitoring into their business planning and quarterly reporting.

- The link between brand reputation and cyber-risk is increasingly clear to European enterprises. The fines issued to British Airways and Marriott Hotels as a result of personal data breaches demonstrate this impact.
- The added reputational and financial risks associated with connected business activities in the 3rd Platform era cannot be mitigated by periodic audits. Continuous and validated cyber-risk monitoring will become prerequisite and foundational in business-to-business relationships.
- Consequently, European enterprises are under intense pressure to embed cyber-risk into their corporate reporting as a constant and ongoing activity given its criticality to both financial performance and brand perception.
- Furthermore, third parties will look for assurance that cyber-risk is being minimized, which requires cyber-risk to be measured and managed before any new enterprise can be accepted into the supply chain.
- In the future, IDC expects cyber-risk monitoring to produce a standardized score to enable third parties and investors to quickly and objectively evaluate the security practices of the enterprises with which they are considering conducting business.
- Technology adoption tends to be more established in more mature markets such as the U.S. However, the EU's GDPR means that European enterprises are already adopting controls-based approaches to information management and risk-based response plans in the event of a data breach. Consequently, IDC expects the complexity and timing of this prediction in Europe to be broadly in line with the worldwide scenario.



Source: IDC, 2019

Prediction #7: Cyber-Risk Monitoring

Brand and attentiveness to cyber-risk have become tightly entwined, and by 2021, 75% of large European companies will embed cyber-risk monitoring into their business planning and quarterly reporting.

IT impact

- Security providers can benefit from increased demand from European enterprises seeking to understand the risk posture of their supply chains and to audit prospective partners. IDC expects demand for risk services and solutions, as well as for the deployment of governance and control technologies, to grow.
- Security teams cannot just record and monitor security logs; they must also analyze them in order to understand risk posture. This pressure will come through board-level demand to quantify and control security risk. This development can be expected to drive demand for faster decision making and more predictive outcomes from security operations.
- European enterprises will seek further insight into their risk postures via threat intelligence. Demand will also rise for incident response management tools and for incident response service providers. Organizations increasingly recognize that not all risks can be mitigated and that risks will occasionally turn into incidents. In order to minimize reputational damage, enterprises will look for specialist guidance and automation to control their responses to these incidents.

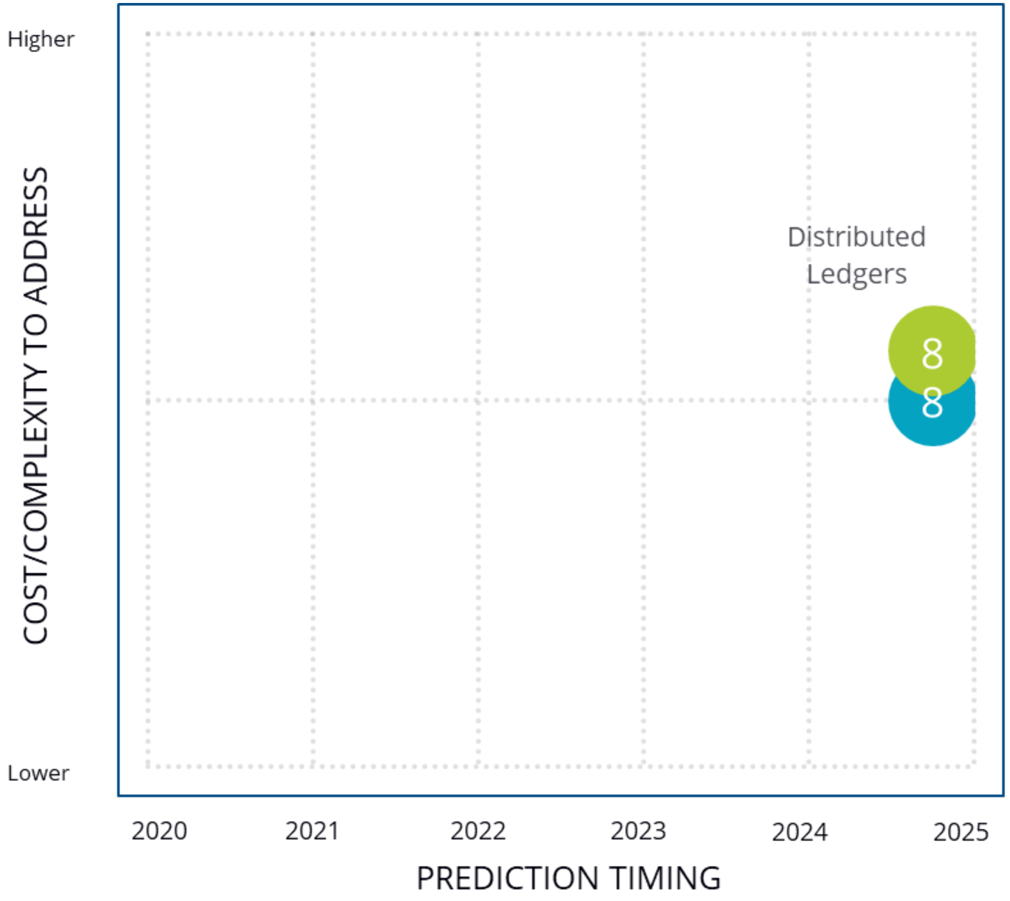
Guidance for Technology Buyers

- Rather than “reinventing the wheel,” European enterprises can build on the achievements of their GDPR compliance programs to fuel their security risk monitoring and management approaches. Applying the principles of information security to personal data protection can help understand and guide data risk management more generally.
- Prioritize risk profiles across the entire organization, as risk can only be mitigated, not eliminated. By focusing on the most critical risks and monitoring them continuously via a variety of security and governance tools, the total risk facing the enterprise can be drastically reduced. Create and maintain a data map to bring visibility into the data within your organization and the risks associated with it. This establishes an organized and repeatable process for the rest of your organization's risk mitigation activities.
- Plan for loss events by earmarking funds for use in the event of a major data breach or administrative action. Despite best efforts to mitigate risk, material losses can still occur and have the potential to cripple a business. Financial planning is just as important a business resiliency practice as mitigating risk.

Prediction #8: Distributed Ledgers

Explosions in data and analysis force the adoption of edge computing; to guarantee data provenance and security, 20% of European enterprise data will reside in distributed ledger systems by 2025.

- The massive volume of data generated, held, processed, and analyzed is increasingly happening at the edge, outside of traditional locations — the core of the enterprise and its datacenters.
- Traditional centralized approaches to data handling are insufficient to cope with the volumes of data that will be generated, requiring alternative structures.
- Competitive pressures mean that business insights from enterprise data must be generated and applied to operations faster than ever before. This requires data analysis to occur closer to, or even at, the edge in these future structures.
- The generation of data from such diverse, and often remote and unsupervised, digital assets will raise questions concerning data provenance. If business decisions are to be made based on this data, it must be clear beyond any doubt where the data has come from, what has been done to it, and who has access to it.
- The "immutability" of data held within distributed ledger technologies (DLT), such as blockchain, and the clarity of who has access to the data and what they have done to it in private DLT models, make it well suited to European needs. Consequently, European blockchain spending is expected to expand by more than 65% over the 2019–2023 period.
- Nevertheless, a key challenge resulting from the immutability of DLT data is that it contradicts regulatory requirements. Specifically, it goes against the “right to be forgotten” principle enshrined within the EU’s GDPR. With European adoption of DLT at a lower level of maturity than markets such as the U.S. and with the inherent characteristics of DLT standing counter to regional regulatory requirements, IDC expects this prediction to take longer and be more complicated to realize than elsewhere.



Source: IDC, 2019

Prediction #8: Distributed Ledgers

Explosions in data and analysis force the adoption of edge computing; to guarantee data provenance and security, 25% of European enterprise data will reside in distributed ledger systems by 2025.

IT impact

- DLT is still at an experimental stage, with few deployments of any scale in live environments. Pressure will grow on DLT vendors and standards consortia to demonstrate how DLT can operate at scale in edge environments.
- While immutability and control over access are positive developments in moving toward DLT, enterprises cannot afford to assume standalone security products are unnecessary. With the growth and diversity of assets linked to edge environments, defense-in-depth strategies will be increasingly important across endpoint, network, and data security.
- To understand if and how personal data can be handled within DLT environments, edge and DLT initiatives must be accompanied by a reappraisal of information management. Enterprises must understand their "data lifecycle" (i.e., what data they have, how it is classified, how long it should be retained, and when it ought to be deleted). The friction between immutability and the European “right to be forgotten” means that organizations will need to have a very firm grip on their personal data, which ought to be handled separately — outside of DLT environments.

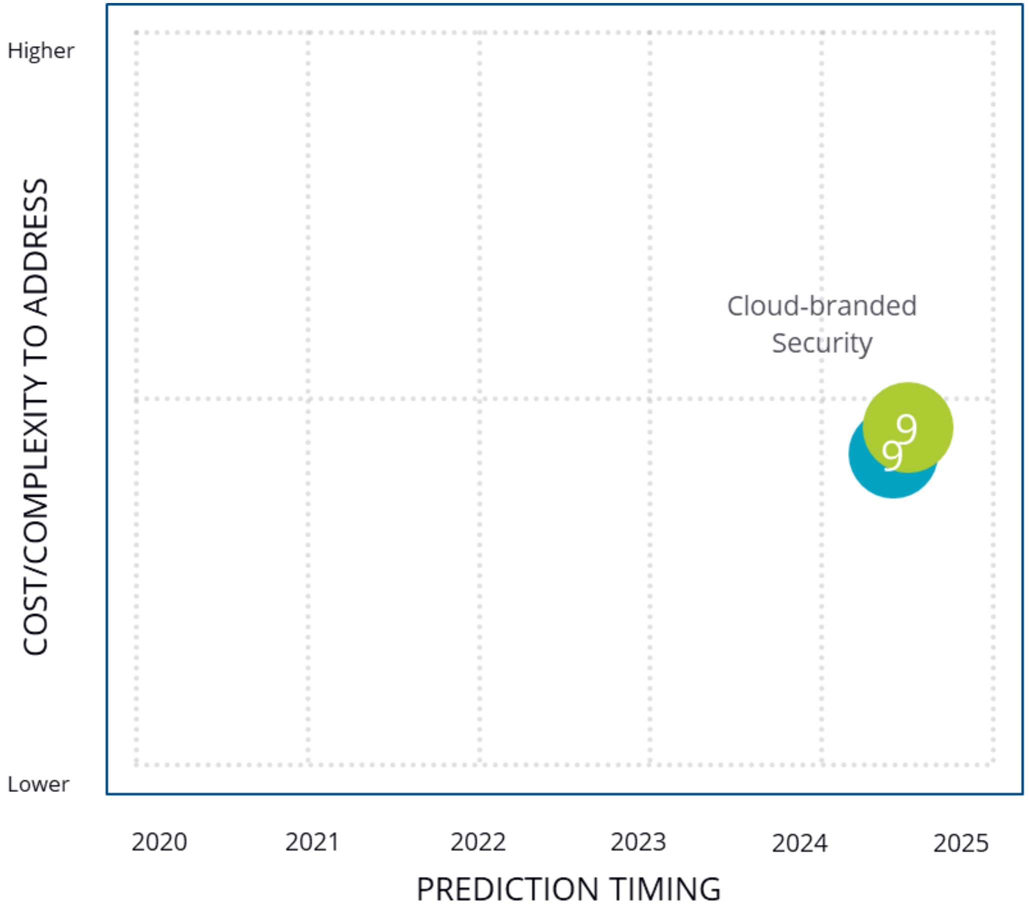
Guidance for Technology Buyers

- Challenge your European providers and prospective partners as to how they can handle the scale of the challenge that your edge and DLT plans to represent. Request insight into existing deployments to demonstrate how this complexity is already being handled.
- Incorporate your edge and DLT plans within a broader enterprise security strategy and environment. Integration, automation, and oversight will be critical to ensure that enterprise data remains protected within defense-in-depth strategies.
- Build a clear view of the data lifecycle for the data that you plan to generate, store, and analyze within edge and DLT environments. You must understand how to classify, separate, and manage your data, especially when it comes to the appropriate handling of personal data under regulatory requirements.

Prediction #9: Cloud-Branded Security

Innovation, opportunity, and market demand collide to place hyperscale cloud providers directly and permanently in the security business; by 2025, 9% of their revenue will be attributed to security.

- According to IDC data, 43.0% of organizations across industries are moving workloads to the cloud, driving the need for security solutions to protect this flow of data. This incentivizes hyperscale cloud providers (e.g. Google, Azure, and AWS) to invest in platform security.
- These providers will leverage cloud scalability and data richness to correlate threat intelligence from a multitude of sources; analyze network traffic across datacenter, cloud, edge, and endpoint; and triage and prioritize security tickets that flood SOCs.
- IDC predicts that, by 2025, the security capabilities of hyperscale cloud providers will provide up to 8.7% of their revenue and could account for 15.0% of overall security spending in Europe.
- In the short term, cloud providers are not positioned to compete feature for feature with market-leading security service providers. However, the enhanced security capabilities that are baked in and developed for use in their cloud platforms will make cloud providers a compelling alternative.
- Given that organizations are rationalizing and consolidating the vendors they use for cybersecurity tools and services, cloud-native capabilities represent opportunities to further reduce entities' portfolios of security platforms and vendor relationships.
- The move from vendor to service provider will be slowed by the shift in marketplace purchasing culture to solutions developed by security vendors (e.g., Trend Micro's Deep Security on AWS), given that these can easily be deployed across platforms, whereas security tools developed in house by a hyperscaler (e.g. Sentinel on Azure) can be deployed in only one dimension.
- Data sovereignty and European regulations will limit workload and information transferability. Those service providers that can manage and resolve governance, risk, and compliance issues will have the upper hand in winning over European customers.



Source: IDC, 2019

Prediction #9: Cloud-Branded Security

Innovation, opportunity, and market demand collide to place hyperscale cloud providers directly and permanently in the security business; by 2025, 9% of their revenue will be attributed to security.

IT impact

- As artificial intelligence and machine learning capabilities become a must-have for modern SecOps teams, traditional pure-play MSSPs will struggle to match the prices that these hyperscale cloud providers offer as raw computing costs eat into their profit margins.
- Some MSSPs will exit the market, while others will partner with hyperscale cloud providers to transform their platforms and delivery models to better align with client needs.
- Management across clouds for multicloud implementations will become a bigger issue and a slowing factor for the expansion of SP-provisioned security.
- The added value of security for colocation services will decrease as SPs roll out their own security services for their platforms.

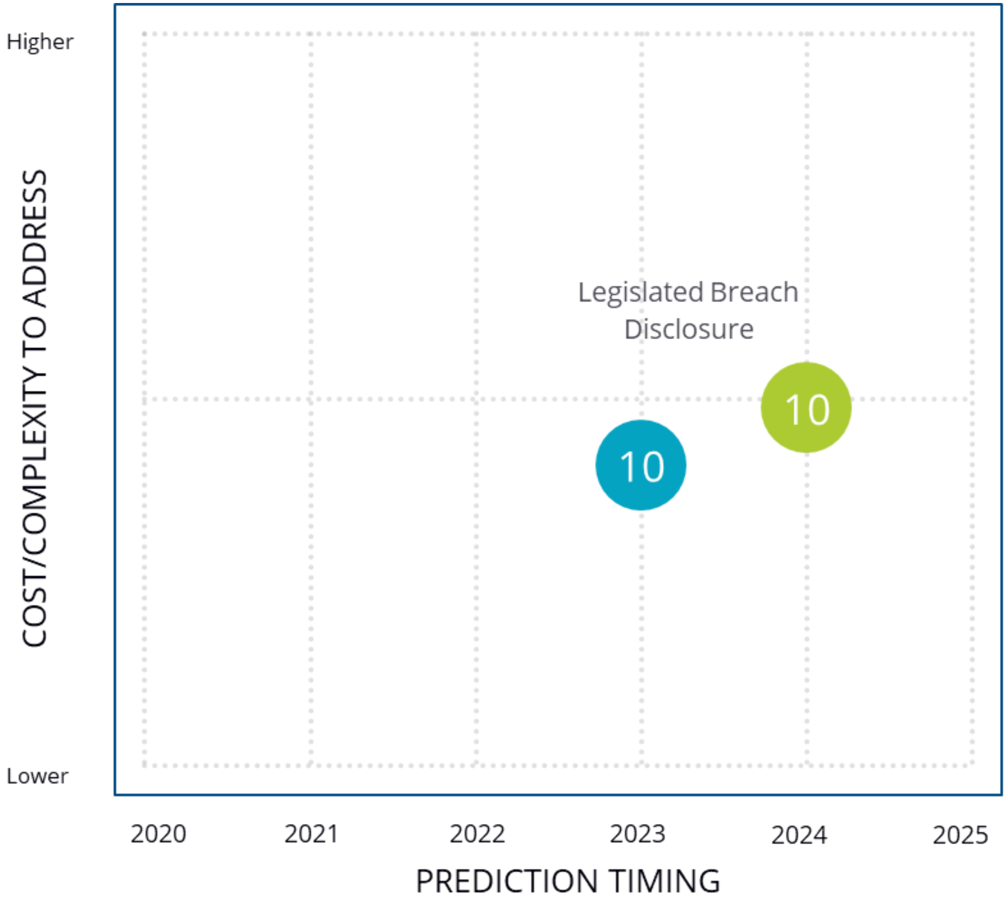
Guidance for Technology Buyers

- Evaluate the security needs of the organization, and determine whether the current setup or vendors are sufficiently equipped with the capabilities to meet both current and future needs. If the solutions are not growth friendly or scalable, consider security solutions offered by cloud providers.
- Consider how you can rationalize your security stack by embracing the native security within your SP platform.
- Monitor the evolution of SP security technology (e.g., AI/ML) and dynamic threat intelligence to protect complex IT environments. Assess the maturity and relevance of those technologies for your current and future IT estate.
- Reduce the use of long-term support contracts for security services or tools. The coming flood of security products and services from hyperscale cloud providers will follow different tech cycles, with lower prices for products/services that are as good as, if not better than, current market offerings.

Prediction #10: Legislated Breach Disclosure

Effectively combating attacks by nation-states and cybercriminals is data dependent, and by addressing this dependency, 70% of European markets will legislate full cyberbreach disclosure by 2024.

- Organizations need to raise their security game to defend themselves against 21st century cyberattacks. Speed of response and a better understanding of who is behind the attack will separate the winners from the losers.
- Knowledge, insight, and understanding require collaboration. Cybersecurity success hinges on the sharing of information within industry sectors and between organizations and people.
- Under the NIS Directive, “a network of Computer Security Incident Response Teams (CSIRTs)” facilitates, at the EU member-state level, the sharing of information about risks and ongoing threats to critical infrastructure.
- Although there are public/private partnerships on sharing threat information, such sharing remains incomplete when it comes to the techniques, tactics, and procedures (TTPs) that particular actors are employing. A lack of governance models and trust in sharing sensitive information is a key inhibitor to the growth of these partnerships. GDPR has no data-breach reporting requirements to make sharing TTPs mandatory.
- Harmonizing existing regulatory IT incident-reporting practices makes sense for EU authorities. In recognition that information sharing is an essential tool for boosting EU cyber-resiliency, related upgrades will incorporate full breach disclosure.



Source: IDC, 2019

Prediction #10: Legislated Breach Disclosure

Effectively combating attacks by nation-states and cybercriminals is data dependent, and by addressing this dependency, 70% of European markets will legislate full cyberbreach disclosure by 2024.

IT impact

- Breach disclosure has become a much more technical procedure, essentially illuminating the TTPs necessary to replicate the breach. Capturing forensics during breach recovery has become critical, as a seize-and-wipe defence could result in additional fines and penalties for insufficient disclosure.
- Organizations should seek to leverage automation for the real-time detection of attacks, supporting proactive responses to security threats. Tightly integrated cyberintelligence services could help provide the near real-time detection of advanced persistent threats while leveraging trained users as “human sensors.”
- Design breach disclosure with privacy protection in mind. Breach disclosure efforts must respect privacy and data protection regulations such as GDPR.
- Full breach disclosure underpins the concept of digital trust. Furthermore, trust-orientated strategy dictates convergence of IT, security, risk, and business objectives and measurements. Traditional approaches to governance, as a result, are facing challenges in both scope and scale.

Guidance for Technology Buyers

- Review cybersecurity architecture and playbooks to ensure that information captured during a potential breach not only relates to malware, but also captures the complete TTPs of the cyberassailant. Cyberthreat intelligence platforms can help analysts build a watchlist of threats of interest and profile threat actors by their usual TTPs, related tools, and malware. Cyberthreat intelligence frameworks, such as the MITRE ATT&CK knowledge base and Cyber Killchain, enable better understanding of the TTPs of cyberthreat actors.
- European regulations like the NIS Directive and the Cybersecurity Act encourage the creation of Information Sharing and Analysis Centers (ISACs) — non-profit organizations that provide a central resource for gathering information on cyberthreats. Consideration should be given to joining an ISAC — for example, the European FI-ISAC for financial institutes or the Cyber Security Information Sharing Partnership (CiSP) in the U.K. Not every organization can keep a fully staffed forensic- or threat-intelligence team. Through shared analysis capabilities, members can benefit without having to deploy these capabilities on their own.
- Full data breach disclosure will require organizations to demonstrate accountability for the robustness of their security policies, procedures, and technology structures. Well-managed audit trails will be needed as proof of compliance, operational integrity, and digital trust.

Predictions at a Glance – European Implications

1. **Resolving Skill Shortages —** Hampered by perpetual security skill shortages, by 2022, 50% of tier 1 security operations center (SOC) analysts in Europe will permanently elevate their productivity and improve operational security metrics by harnessing artificial intelligence (AI) and machine learning (ML).
2. **IT/OT Integration —** Advancements in operational technology (OT) visibility tools will propel 66% of major European industrial firms to adopt an IT-OT integrated approach to security monitoring by 2024.
3. **Cloudified MSS —** Shifting of workloads to the cloud is shifting consumption of managed security services (MSS), and by 2023, 35% of European MSS customers will be served by cloudified MSS providers.
4. **Indigenous Cybersecurity —** Driven by rising aversion to "foreign" technology, 20% of developing markets in Europe will mandate the use of indigenous cybersecurity vendors to secure government and critical infrastructure by 2023.
5. **Trust Framework —** With the business criticality of digital trust rising, 55% of European spending on security services will be devoted to developing, implementing, and maintaining a ‘trust framework’ by mid-2023.
6. **Passwordless —** Intolerant of trade-offs between superior digital experiences and identity assurance, consumers demand both; by 2022, 30% of consumer online transactions in Europe will be high trust and passwordless.
7. **Cyber-Risk Monitoring —** Brand and attentiveness to cyber-risk have become tightly entwined, and by 2021, 75% of large European companies will embed cyber-risk monitoring into their business planning and quarterly reporting.
8. **Distributed Ledgers —** Explosions in data and analysis force the adoption of edge computing; to guarantee data provenance and security, 20% of European enterprise data will reside in distributed ledger systems by 2025.
9. **Cloud-Branded Security —** Innovation, opportunity, and market demand collide to place hyperscale cloud providers directly and permanently in the security business; by 2025, 9% of their revenue will be attributed to security.
10. **Legislated Breach Disclosure —** Effectively combating attacks by nation-states and cybercriminals is data dependent, and by addressing this dependency, European markets will legislate full cyberbreach disclosure by 2024.

Learn More

- *IDC FutureScape: Worldwide Security and Trust 2020 Predictions* (IDC #US45582219, October 2019)
- *Critical External Drivers Shaping Global IT and Business Planning, 2020* (IDC #US45540519, October 2019)

IDC ANALYZE THE FUTURE

IDC is the most trusted IT research advisory firm in the market. IDC's IT Executive Programs support businesses globally in the Digital Transformation (DX) of their organizations. Our IT advisory services not only advise on the technologies underpinning digital transformation (e.g., cloud, analytics, IoT, mobility, 3D printing), but also on effectively leading and executing Digital Transformation (DX) initiatives across both IT and the line of business. For over 50 years, IDC has provided strategic insights to enable clients to achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.