Delinea

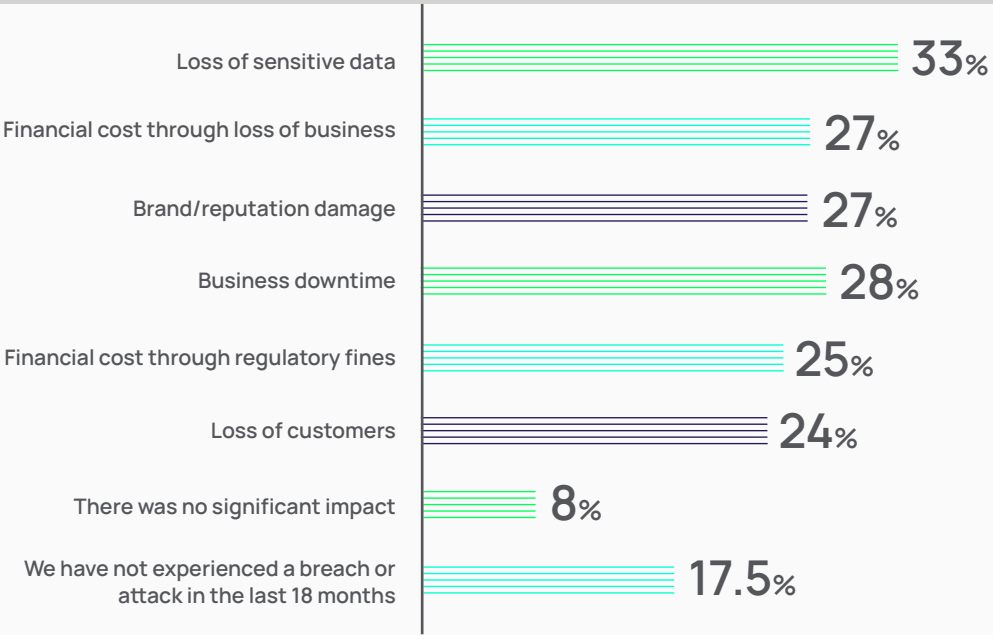
European businesses plagued by many different cyberthreats

Only 17.5% of the European companies haven't experienced a breach over the last 18 months

A wide variety of threats are common across the European cybersecurity landscape. Our survey of 10 European countries indicates each of them differ in strategies, methods, and priorities to address these threats.

Risks and challenges

FIGURE 1 | If your organisation has experienced an identity-related breach or an attack using stolen credentials in the last 18 months, what was the most significant impact of this breach? Select up to three



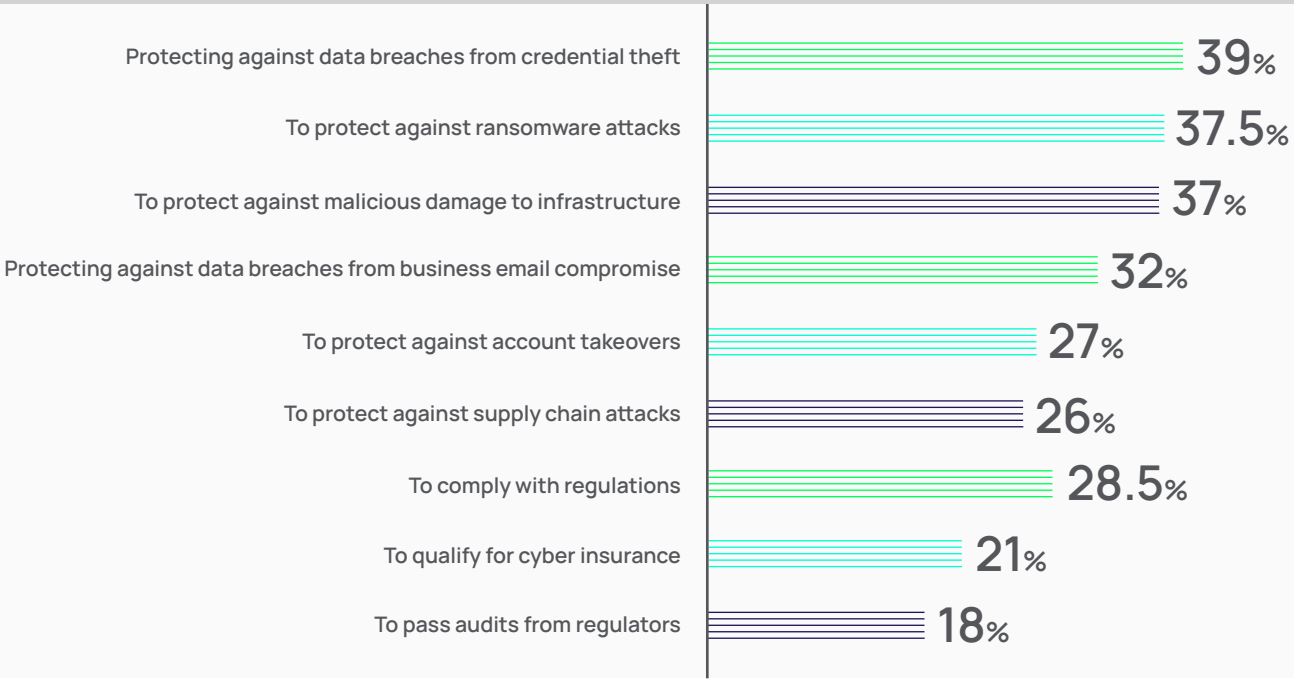
17.5% of European respondents said their businesses were not breached over the last 18 months, slightly higher than the global average of 16%. The most breached countries in Europe were Sweden, Netherlands, and Turkey. On average loss of sensitive data was the most significant impact. However, for German security teams, the most impactful were regulatory fines, similarly in Sweden, apart from the loss of sensitive data and lost customers. French teams were most impacted by business downtime.

European C-suites and boards generally understand the importance of identity security. Spanish and Italian management are among the most supportive of all countries we have interviewed. Securing identities is not reported to be a priority for the German C-suite.

Generally, European countries are constrained by the budgets allocated to protect identities, however slightly less than the global average. Sweden is the most constrained of all 19 countries and regions we have surveyed.

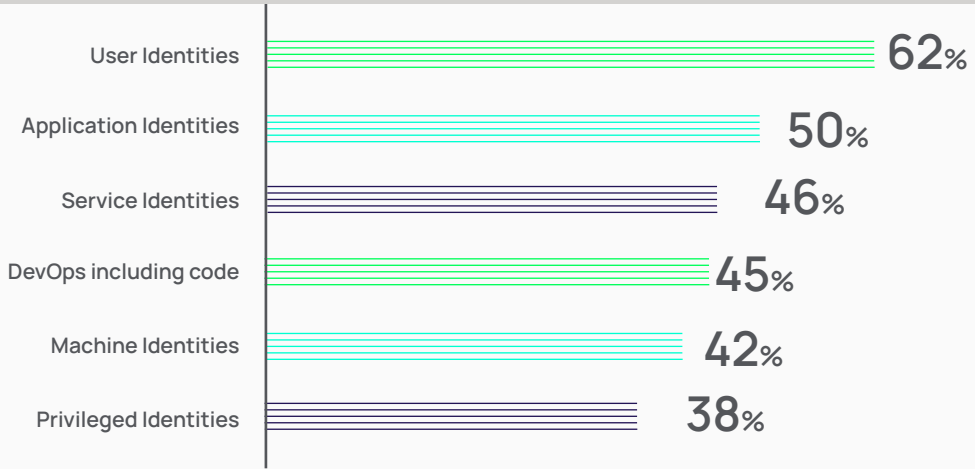
The current approach to privileged access and security

FIGURE 2 | Which of the following factors are the most important in driving decisions around securing identities in the organisation? Select up to three



When securing identities European security professionals expect to address three key threats: data breaches from credential theft, ransomware attacks, and malicious damage to infrastructure.

FIGURE 3 | To which identities have you deployed privileged access security measures? Select all that apply



Similar to the global benchmark, businesses in Europe have deployed privileged access security measures to user and application identities. IT admins and security teams are the main users of Privileged Accounts.

Europeans use the same methods as their global peers to protect privileged access. However, there are different approaches across countries. Secure keys are used by France, Spain, Germany. Whereas Polish, Dutch, Turkish, and Swedish organizations prefer two-factor authentication, and taking it a step further, multi-factor authentication is preferred in the UK&I and Italy.

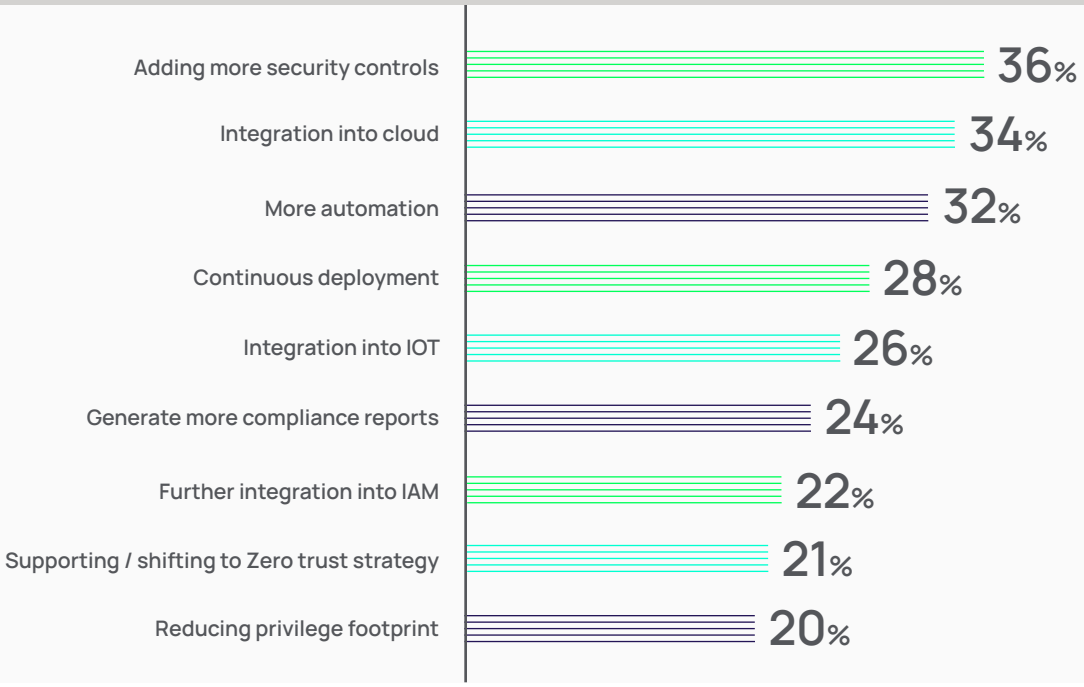
Strategies and priorities

FIGURE 4 | Which of the following best describes your overall security strategy right now? Select one

The majority of the European respondents that have an active security strategy and are adapting fast. France, Italy, Spain, and Turkey scored higher than the regional average. Although constrained by the budget and resources, Polish companies have the most active security strategy globally. Only 4% of Polish security managers indicated their approach needs reinvigoration.

Sweden is a clear European outlier wherein 57% of security professionals said they neither have an active strategy nor plan to implement anything new.

FIGURE 5 | What are your priorities over the next 12-18 months in relation to privileged access security to protect identities? Select up to three



Priorities differ from country to country. Integration into the cloud is the key task for UK and Irish (36%), French (36%), and German (37%) CISOs. Swedish are looking into continuous deployment (43%). Dutch (32%) and Polish (41%) prioritize automation. Adding more security controls has been indicated by Spanish (41%), Turkish (48%), Polish (41%), and French (35%) respondents as a top priority. Italians are looking predominately into IOT integration (46%).

Ease of use for IT admins and business users is the key factor for respondents when considering new solutions indicated in 6 out of 9 European countries. Additionally, products must have features that help to minimize risks and be easy to integrate with other solutions.

While organizations have made progress toward a more secure future, they have a long way to go. Ad-hoc, incremental changes aren't going to get the job done. In fact, they can give you a false sense of security and leave you with a lot of technical debt you'll need to unravel.

Check out how you compare to your peers and get the free complete analysis and recommendation by accessing the global report here.

Delinea

Delinea is a leading provider of privileged access management (PAM) solutions that make security seamless for the modern, hybrid enterprise. Our solutions empower organizations to secure critical data, devices, code, and cloud infrastructure to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies. **delinea.com**