ENTRUST

PrimeFactors™
Applied Data Protection

2021 APPLICATION-LEVEL DATA PROTECTION SURVEY

Learn how organizations view the challenges and strategies of protecting data in use

Table of Contents

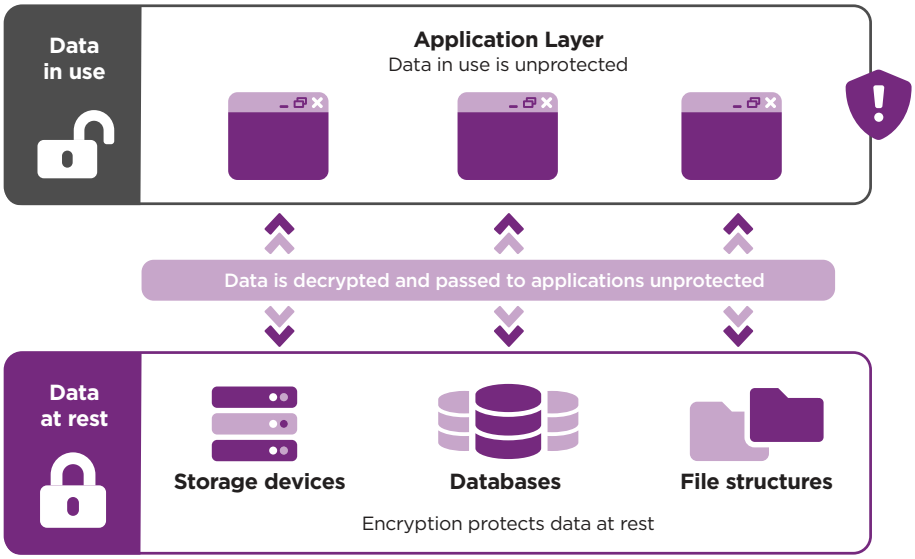
BACKGROUND

As the evolution of data protection migrates from 'encrypt data' to 'orchestrate data protection and privacy,' the challenge of data protection in the modern era can be very complex. A variety of methodologies, often so interconnected that the line between them can begin to blur common data protection vernacular, can be employed to secure sensitive information to help comply with regulatory and industry standards or meet other business objectives.

Most traditional security solutions focus on securing data at rest – applying encryption or other data protection methodologies to data to secure it where it is stored in databases, disk structures, or folders. However, data-at-rest protection does not typically address the use case of protecting sensitive data once it leaves its storage location. Applying data protection at the application level, before data is used, moved, or stored, holds the potential to increase data protection posture.

When it comes to research on how industry professionals view data protection, the vast majority of market research tends to focus on data-at-rest protection. This should not be surprising, as application-level data protection has long been perceived as too complex to be practicable. However, as solutions for protecting data at the highest level improve in their simplicity and elegance, orchestrating data protection and privacy at the application level becomes more feasible for the average corporation. The need to better understand the perceptions and plans of those that may be considering application-level data protection is both relevant and timely.

The challenge: Traditional data protection solutions leave data in use unprotected



OBJECTIVE & METHODOLOGY

In an endeavor to better understand how companies view protecting data at the application layer and to provide some insight into emerging trends in this space, Entrust and Prime Factors jointly commissioned a survey instrument focused on data protection at the application layer. Questions were architected in a manner meant to tease out some of the nuances in how people perceive data protection at the application layer, what solutions they have in place and plans they may have in this arena, and the challenges and benefits they perceive in implementing data protection at the application layer.

The survey was anonymously administered through a third-party firm to a target audience consisting of full-time professionals in the information technology (IT) field in the United Kingdom (UK) and the United States of America (USA), with an equal number of respondents from both territories (300 each).

SUMMARY OF FINDINGS

The results of this survey collectively illustrate that protecting data at the application layer can be confusing, complex, and challenging, but action is being taken. Compliance has been and will be a key driver for increasing data protection, and respondents are using a variety of data protection techniques. However, inconsistencies in answers suggest that many respondents may not clearly understand the distinctions between securing data at the application layer versus at rest. Nonetheless, there appears to be a fairly broad concern for ensuring that sensitive data is secured when in use, and a great number of respondents plan to presently implement solutions to secure data at the application layer.

DATA PROTECTION REGULATIONS' IMPACT ON BUSINESS

Data protection regulations and industry standards for securing sensitive data have impacted almost every respondent business. Only 2.5% of respondents indicated that regulations had no impact on their business, and even fewer (2%) expect that there will not be an impact to business moving forward. Approximately 4 out of 10 respondents reported that they expect regulations and standards will increase the complexity of their business in the future. A vast majority of respondents (61%) have indicated that data protection regulations have increased their need for encryption solutions, and nearly the same amount (60%) expect that this trend will continue.

PERCEPTION VS. FUNCTION

The survey findings appear to expose some misunderstanding around what exactly application-level data protection means to individuals. More than 50% of respondents indicated that their company secures data in applications with application data encryption. However, when asked to describe *how* this encryption is applied to data in the applications they control (bespoke), the vast majority described their encryption techniques using data-at-rest encryption approaches. In fact, less than 25% of all respondents listed as one of their (all that apply) responses as "We encrypt data at the application level before data is stored." This leads us to believe that the perception that data-at-rest encryption or other application-specific security measures may be misunderstood by respondents as being application-level data encryption.

This premise was further teased out in discussing the effects of only securing data at rest, which typically leaves data unprotected after it leaves the storage location. When asked about their level of concern with unprotected sensitive data at the application layer, nearly 85% of respondents reported being somewhat or very concerned. When 85% of people express concern for an issue, it is not unreasonable to expect that material action is being planned in this area, and that is precisely what the data indicated.

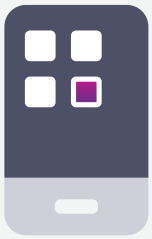
When asked what techniques are used to protect data:

51%

51% of respondents report they use application layer data encryption

When asked how their techniques are applied:

25%

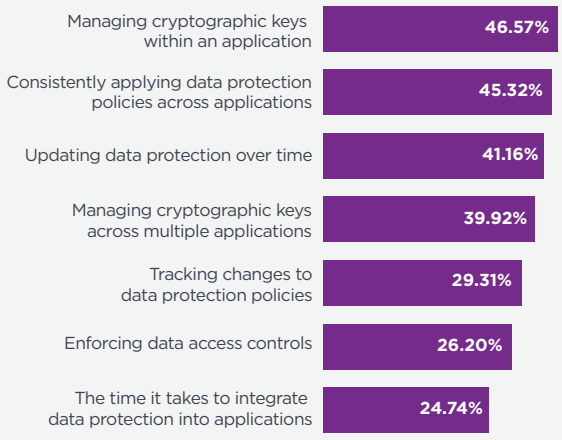


25% actually describe application layer data encryption techniques

COMPLEXITIES & CHALLENGES

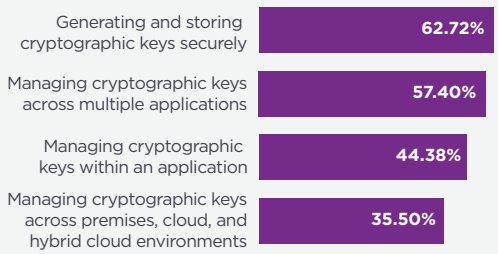
There is surprisingly little agreement on which elements of application-level data protection are most challenging. When asked to rank the top three challenges of protecting data at the application layer, the most common answers related to managing cryptographic keys and applying data protection policies consistently across applications – both of which scored statistically similar results with approximately 9 out of each 20 respondents identifying these as top challenges. However, of 11 possible answers, not a single answer received a majority consensus to be placed among the top three challenges. In fact, seven different answers were ranked among the top three by at least 1 in every 4 respondents, suggesting a fairly wide distribution of concern and perhaps too of priorities.

What are the top challenges in applying data protection in applications?



Being able to create a trusted cryptographic key and keep it safe, and being able to manage keys across multiple applications remain the biggest challenges for cryptographic key management. The challenge of generating and storing cryptographic keys was ranked among the top two challenges for 63% of respondents. While nearly half of all respondents indicated that managing cryptographic keys within an application was a top challenge of key management, nearly 30% more people indicated that managing keys across multiple applications, which may be seen as added complexity, was an even greater challenge.

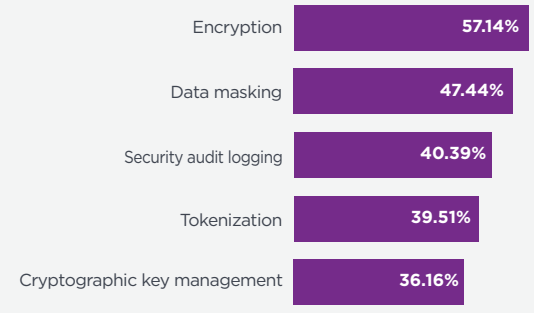
What are your top challenges when it comes to managing cryptographic keys for application-level data protection?



PLANNED ACTION

Perhaps the most surprising response of the survey was the sheer number of respondents who have impending plans to add application-level data protection functionality. In fact, only 4% of respondents reported that they *do not* plan to add application-level data protection functionality in the next 12 months. Nearly 6 in every 10 respondents reported they plan to add application-level encryption functionality, almost half of all respondents plan to implement data masking functionality at the application layer, and 4 of every 10 respondents plan to implement a tokenization solution in the next 12 months. It appears that the aforementioned concerns with data being unsecured at the application level is leading to measurable action.

Which of the following functionalities do you plan to implement in applications in the next 12 months?



CONCLUSION

Many companies are taking a variety of actions related to data protection, though these efforts tend to focus on securing data-at-rest, due in part to a perception that securing data in use at the application level is more complex than applying security to data-at-rest. However, data-at-rest security solutions are generally not designed to address protecting data once it leaves its storage location, leaving data unprotected at the application level. Very broad concern over this potential gap in security posture is supported by mounting empirical evidence.

Companies are concerned with trust, especially when it comes to generating and securely storing the cryptographic keys that lock and unlock sensitive data. They are also concerned with complexity, particularly as the number of applications and deployment environments increase and add to the already challenging task of managing cryptographic keys at the application layer. Consistency of applying data protection policies is another top issue. These central themes of desiring trust, consistency, and simplicity permeate through the various survey answers when it comes to application-level data protection.

Despite their concerns over complexities, there is widespread action being taken to address application-level data protection, with the majority of respondents reporting plans to implement functionality within the year. This suggests that the market for application-level data protection solutions is far from stagnant. Particularly well poised will be the solutions that help to simplify orchestrating data protection and privacy at the application level while using hardware security modules to protect the critical cryptographic keys.

To find out more about Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

ABOUT PRIME FACTORS

Prime Factors is a global leader in applied data protection software, helping to secure an open and collaborative digital world. Data has never been more plentiful or more valuable, and the protection of sensitive data has never been more complex. With a focus on application-level data protection, software solutions from Prime Factors help to simplify the complexities associated with protecting sensitive information where it is most at risk. For 40 years, Prime Factors has served more than 1,000 customers across six continents in a variety of industries, including 80% of the top financial institutions in North America, with cryptographic software solutions for payments, information exchange, and general data protection.

For more Information
888.963.6358
+1 541.345.4334
sales@primefactors.com
primefactors.com

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223