2021
Global Encryption Trends Study: Consolidated findings

Sponsored by Entrust

Independently conducted by Ponemon Institute LLC

Publication Date: April 2021

2021 Global Encryption Trends Study[1]
Ponemon Institute, April 2021

Appendix 2. Survey Data Tables

The following tables provide the consolidated results for 17 country samples.

Survey response	FY2020
Sampling frame	161,607
Total returns	7,331
Rejected or screened surveys	721
Final sample	6,610
Response rate	4.1%

Part 1. Encryption Posture

Q1. Please select one statement that best describes your organization's approach to encryption implementation across the enterprise.	FY2020
We have an overall encryption plan or strategy that is applied consistently across the entire enterprise	50%
We have a limited encryption plan or strategy that is applied to certain applications and data types	37%
We don't have an encryption plan or strategy	13%
Total	100%

Q2. Following are areas where encryption technologies can be deployed. Please check those areas where encryption is extensively deployed, partially deployed or not as yet deployed by your organization.

Q2a-1 Backup and archives	FY2020
Extensively deployed	51%
Partially deployed	30%
Not deployed	18%
Total	100%

Q2b-1. Big data repositories	FY2020
Extensively deployed	33%
Partially deployed	29%
Not deployed	38%
Total	100%

Q2c-1 Cloud gateway	FY2020
Extensively deployed	44%
Partially deployed	32%
Not deployed	24%
Total	100%

[1]This year's data collection was started in December 2020 and completed in January 2021. Throughout the report we present trend data based on the fiscal year the survey commenced rather than the year the report is finalized. Hence, we present the current findings as fiscal year 2020.

Q2d-1. Data center storage	FY2020
Extensively deployed	41%
Partially deployed	32%
Not deployed	26%
Total	100%

Q2e-1. Databases	FY2020
Extensively deployed	55%
Partially deployed	28%
Not deployed	17%
Total	100%

Q2f-1. Containers	FY2020
Extensively deployed	32%
Partially deployed	31%
Not deployed	37%
Total	100%

Q2g-1. Email	FY2020
Extensively deployed	41%
Partially deployed	31%
Not deployed	28%
Total	100%

Q2h-1. Public cloud services	FY2020
Extensively deployed	46%
Partially deployed	27%
Not deployed	27%
Total	100%

Q2i-1. File systems	FY2020
Extensively deployed	38%
Partially deployed	33%
Not deployed	28%
Total	100%

Q2j-1. Internet communications (e.g., TLS/SSL)	FY2020
Extensively deployed	56%
Partially deployed	27%
Not deployed	17%
Total	100%

Q2k-1. Internal networks (e.g., VPN/LAN)	FY2020
Extensively deployed	52%
Partially deployed	29%
Not deployed	19%
Total	100%

Q2l-1. Laptop hard drives	FY2020
Extensively deployed	52%
Partially deployed	27%
Not deployed	21%
Total	100%

Q2m-1 Private cloud infrastructure	FY2020
Extensively deployed	43%
Partially deployed	31%
Not deployed	26%
Total	100%

Q2n-1 Internet of things (IoT) devices	FY2020
Extensively deployed	33%
Partially deployed	28%
Not deployed	39%
Total	100%

Q2o-1 Internet of things (IoT) platforms/data repositories	FY2020
Extensively deployed	34%
Partially deployed	27%
Not deployed	38%
Total	100%

Q3. How many different products does your organization use that perform encryption?	FY2020
1 to 3	14%
4 to 6	25%
7 to 9	28%
10 to 12	21%
13 or more	13%
Total	100%
Extrapolated value	8.02

Q4. Who is most influential in directing your organization's encryption strategy? Please select one best choice.	FY2020
IT operations	37%
Security	18%
Lines of business (LOB) or general management	25%
No single function has responsibility	20%
Total	100%

Q5. What are the reasons why your organization encrypts sensitive and confidential data? Please select the top three reasons.	FY2020
To protect enterprise intellectual property	49%
To protect customer personal information	54%
To limit liability from breaches or inadvertent disclosure	31%
To avoid public disclosure after a data breach occurs	16%
To protect information against specific, identified threats	50%
To comply with internal policies	24%
To comply with external privacy or data security regulations and requirement	45%
To reduce the scope of compliance audits	30%
Total	300%

Q6. What are the biggest challenges in planning and executing a data encryption strategy? Please select the top two reasons.	FY2020
Discovering where sensitive data resides in the organization	65%
Classifying which data to encrypt	34%
Determining which encryption technologies are most effective	18%
Initially deploying the encryption technology	43%
Ongoing management of encryption and keys	26%
Training users to use encryption appropriately	14%
Total	200%

Q7. How important are the following features associated with encryption solutions that may be used by your organization? Very important and important response combined.	FY2020
Enforcement of policy	68%
Management of keys	69%
Support for multiple applications or environments	46%
Separation of duties and role-based controls	57%
System scalability	59%
Tamper resistance by dedicated hardware (e.g., HSM)	50%
Integration with other security tools (e.g., SIEM and ID management)	61%
Support for regional segregation (e.g., data residency)	42%
System performance and latency	71%
Support for emerging algorithms (e.g., ECC)	57%
Support for cloud and on-premise deployment	67%
Formal product security certifications (e.g., FIPS 140)	53%

Q8. What types of data does your organization encrypt? Please select all that apply.	FY2020
Customer information	42%
Non-financial business information	25%
Intellectual property	48%
Financial records	55%
Employee/HR data	48%
Payment related data	55%
Healthcare information	26%

Q9a. What are the main threats that might result in the exposure of sensitive or confidential data? Please select the top two choices.	FY2020
Hackers	29%
Malicious insiders	21%
System or process malfunction	31%
Employee mistakes	53%
Temporary or contract workers	25%
Third party service providers	17%
Lawful data request (e.g., by police)	12%
Government eavesdropping	11%
Other	2%
Total	200%

Q9b. Has your organization experienced a data breach?	FY2020
Yes	44%
No	56%
Total	100%

Q10a. When do you expect homomorphic encryption to reach mainstream enterprise adoption?	FY2020
1 to 4 years	39%
5 to 8 years	30%
9 to 12 years	20%
More than 12 years	10%
Total	100%
Extrapolated value	6.49

Q10b. When do you expect multi-party computation to reach mainstream enterprise adoption?	FY2020
1 to 4 years	48%
5 to 8 years	29%
9 to 12 years	16%
More than 12 years	7%
Total	100%
Extrapolated value	5.77

Q10c. When do you expect quantum algorithms to reach mainstream enterprise adoption?	FY2020
1 to 4 years	28%
5 to 8 years	26%
9 to 12 years	27%
More than 12 years	19%
Total	100%
Extrapolated value	7.90

Part 2. Key Management

Q11. Please rate the overall "pain" associated with managing keys or certificates within your organization, where 1 = minimal impact to 10 = severe impact?	FY2020
1 or 2	8%
3 or 4	14%
5 or 6	21%
7 or 8	24%
9 or 10	32%
Total	100%
Extrapolated value	6.66

Q12. What makes the management of keys so painful? Please select the top three reasons.	FY2020
No clear ownership	64%
Insufficient resources (time/money)	34%
Lack of skilled personnel	57%
No clear understanding of requirements	27%
Key management tools are inadequate	46%
Systems are isolated and fragmented	48%
Technology and standards are immature	14%
Manual processes are prone to errors and unreliable	9%
Other	1%
Total	300%

Q13. Following are a variety of keys that may be managed by your organization. Please rate the overall "pain" associated with managing each type of key. **Very painful and painful** response combined.	**FY2020**
Encryption keys for backups and storage	29%
Encryption keys for archived data	34%
Keys associated with SSL/TLS	41%
SSH keys	57%
End user encryption keys (e.g., email, full disk encryption)	42%
Signing keys (e.g., code signing, digital signatures)	52%
Payments-related keys (e.g., ATM, POS, etc.)	35%
Keys to embed into devices (e.g., at the time of manufacture in device production environments, or for IoT devices you use)	24%
Keys for external cloud or hosted services including Bring Your Own Key (BYOK) keys	58%

Part 3. Hardware Security Modules

Q14. What best describes your level of knowledge about HSMs?	**FY2020**
Very knowledgeable	37%
Knowledgeable	29%
Somewhat knowledgeable	21%
No knowledge	13%
Total	100%

Q15a. Does your organization use HSMs?	**FY2020**
Yes	49%
No	51%
Total	100%

Q15b. For what purpose does your organization presently deploy or plan to use HSMs? Please select all that apply.	
Q15b-1. HSMs used today	**FY2020**
Application level encryption	47%
Database encryption	32%
Big data encryption	24%
Public cloud encryption including for Bring Your Own Key (BYOK)	34%
Private cloud encryption	25%
TLS/SSL including firewalls, and application delivery controllers	44%
PKI or credential management	31%
Internet of Things (IoT) root of trust	21%
Key management root of trust	23%
Document signing (e.g., electronic invoicing)	21%
Code signing	19%
Payment transaction processing or payment credential issuing/provisioning	26%
With Cloud Access Security Brokers (CASBs) for encryption key management	28%
Container encryption/signing services	40%
With Privileged Access Management (PAM) solutions to protect administrative access	27%
With Secrets Management solutions to protect secrets storage	28%
Blockchain applications (e.g., cryptocurrency, financial transfer)	18%
Not planning to use	7%
Other	2%
Total	497%

Q16b-2. HSMs planned to be deployed in the next 12 months	**FY2020**
Application level encryption	49%
Database encryption	44%
Big data encryption	26%
Public cloud encryption including for Bring Your Own Key (BYOK)	32%
Private cloud encryption	23%
TLS/SSL including firewalls, and application delivery controllers	49%
PKI or credential management	30%
Internet of Things (IoT) root of trust	18%
Key management root of trust	21%
Document signing (e.g., electronic invoicing)	20%
Code signing	21%
Payment transaction processing or payment credential issuing / provisioning	30%
With Cloud Access Security Brokers (CASBs) for encryption key management	28%
Container encryption/signing services	39%
With Privileged Access Management (PAM) solutions to protect administrative access	28%
With Secrets Management solutions to protect secrets storage	33%
Blockchain applications (e.g., cryptocurrency, financial transfer)	21%
Not planning to use	14%
Other	1%
Total	527%

Q16c-1. If you use HSMs in conjunction with public cloud based applications, what models do you use today? Please select all that apply.	FY2020
Rent/use HSMs from public cloud provider, hosted in the cloud	39%
Own and operate HSMs on-premise at your organization, accessed real-time by cloud-hosted applications	41%
Own and operate HSMs for the purpose of generating and managing BYOK (Bring Your Own Key) keys to send to the cloud for use by the cloud provider	17%
Own and operate HSMs that integrate with a Cloud Access Security Broker to manage keys and cryptographic operations (e.g., encrypting data on the way to the cloud, managing keys for cloud applications)	14%
Not using HSMs with public cloud applications	3%
Total	113%

Q16c-2. If you use HSMs in conjunction with public cloud based applications, what models do you plan to use in the next 12 months Please select all that apply.	FY2020
Rent/use HSMs from public cloud provider, hosted in the cloud	39%
Own and operate HSMs on-premise at your organization, accessed real-time by cloud-hosted applications	56%
Own and operate HSMs for the purpose of generating and managing BYOK (Bring Your Own Key) keys to send to the cloud for use by the cloud provider	24%
Own and operate HSMs that integrate with a Cloud Access Security Broker to manage keys and cryptographic operations (e.g., encrypting data on the way to the cloud, managing keys for cloud applications)	24%
Not using HSMs with public cloud applications	1%
Total	144%

Q17. In your opinion, how important are HSMs to your encryption or key management strategy? Very important and important response combined	FY2020
Q17a. Importance today	66%
Q17b. Importance in the next 12 months	77%

Q18. Which statement best describes how your organization uses HSMs?	FY2020
We have a centralized team that provides cryptography as a service (including HSMs) to multiple applications/teams within our organization (i.e., private cloud model).	61%
Each individual application owner/team is responsible for their own cryptographic services (including HSMs) (i.e., traditional siloed, application-specific data center deployment).	39%
Total	100%

Q19a. Does your organization plan to use blockchain?	FY2020
Yes	59%
No	41%
Total	100%

Q19b. If yes, what applications does your organization use or plan to use blockchain for? Please select all that apply.	FY2020
Asset transactions/management	52%
Cryptocurrency/wallets	59%
Identity	45%
Smart contracts	35%
Supply chain	37%
Other	1%
Total	240%

Q19c. If yes, what is the timeframe for your use of blockchain?	FY2020
Currently using	28%
Next 1-2 years	29%
Next 3-4 years	24%
5 years or later	20%
Total	100%
Extrapolated value	2.64

Part 4. Cloud encryption: When responding to the following questions, please assume they refer only to public cloud services.	
Q20. Does your organization currently use cloud computing services for any class of data or application – both sensitive and non-sensitive?	FY2020
Yes, we are presently doing so	66%
No, but we are likely to do so in the next 12 to 24 months	21%
No	13%
Total	100%

Q21. Do you currently transfer sensitive or confidential data to the cloud (whether or not it is encrypted or made unreadable via some other mechanism)?	FY2020
Yes, we are presently doing so	60%
No, but we are likely to do so in the next 12 to 24 months	24%
No	15%
Total	100%

Q22. How does your organization protect data at rest in the cloud? Please select all that apply.	FY2020
Encryption performed in the cloud using keys generated/managed by the cloud provider	36%
Encryption performed in the cloud using keys my organization generates and manages on-premise	21%
Encryption performed on-premise prior to sending data to the cloud using keys my organization generates and manages	38%
None of the above	5%
Total	100%

Q23. For encryption of data at rest in the cloud, what is your organization's strategy? Please select one choice only.	FY2020
Only use keys controlled by my organization	42%
Only use keys controlled by the cloud provider	18%
Use a combination of keys controlled by my organization and by the cloud provider, with a preference for keys controlled by my organization	21%
Use a combination of keys controlled by my organization and by the cloud provider, with a preference for keys controlled by the cloud provider	19%
Total	100%

Q24. How important are the following features associated with cloud encryption to your organization? **Very important and Important** response provided.	FY2020
Bring Your Own Key (BYOK) management support	53%
Privileged user access control	49%
Granular access controls	55%
Audit logs identifying key usage	49%
Audit logs identifying data access attempts	39%
SIEM integration, visualization and analysis of logs	59%
Support for FIPS 140-2 compliant key management	37%
Support for the KMIP standard for key management	59%
Unified key management solutions across multiple clouds and enterprise	45%
Ability to encrypt and rekey data while in use without downtime	46%
Total	491%

Q25a. How many public cloud providers does your organization in use today?	FY2020
1	33%
2	25%
3	18%
4 or more	24%
Total	100%
Extrapolated value	2.33

Q25b. How many public cloud providers does your organization plan to use in the next 12 to 24 months?	FY2020
1	15%
2	20%
3	24%
4 or more	41%
Total	100%
Extrapolated value	2.91

Part 5. Role and organizational characteristics

D1. What organizational level best describes your current position?	FY2020
Senior Executive	3%
Vice President	3%
Director	15%
Manager/Supervisor	34%
Associate/Staff/Technician	43%
Other	2%
Total	100%

D2. Select the functional area that best describes your organizational location.	FY2020
IT operations	52%
Security	21%
Compliance	10%
Finance	5%
Lines of business (LOB)	9%
Other	3%
Total	100%

D3. Total years of business experience	FY2020
Total years of security experience	9.8
Total years in current position	6.7

D4. What industry best describes your organization's industry focus?	FY2020
Agriculture & food services	2%
Communications	3%
Consumer products	4%
Defense & aerospace	0%
Education & research	3%
Energy & utilities	7%
Entertainment & media	2%
Financial services	15%
Health & pharmaceutical	8%
Hospitality	3%
Internet & ISPs	1%
Manufacturing & industrial	12%
Pharmaceuticals	1%
Public sector	8%
Retailing	7%
Services	9%
Technology & software	9%
Transportation	4%
Other	3%
Total	100%

D5. What is the worldwide headcount of your organization?	FY2020
Less than 500	16%
500 to 1,000	26%
1,001 to 5,000	29%
5,001 to 25,000	18%
25,001 to 75,000	8%
More than 75,000	3%
Total	100%