thalesgroup.com

THALES

The enterprise encryption blueprint

Discover, define and deploy your enterprise data encryption strategy

White Paper

Contents

Developing an enterprise data encryption strategy

Lucky you! You've been tasked with setting and implementing an enterprise wide encryption strategy, one that will be used to guide and align each Line of Business (LoB), Application Owner, Database Administrator (DBA) and Developer toward achieving the goals and security requirements that you define and set forth as the model for your organization. A daunting task, for sure, but one that is certainly very achievable.

As with all strategies, it will change and become more refined over time, especially as you gain more experience, learning and getting feedback from within your organization. This guide is based on real experiences that Thales has had working with some of the largest companies in the world, deploying our products on tens of thousands of computing platforms and protecting data with encryption methods designed to meet their chosen strategy.

You should note that this guide does not contain security hype or the marketing splash demonstrating the number of breaches and their cost both financially and to the reputation of your business. Those can easily be found, almost weekly, in the headlines of any major publication. Instead, this guide will focus more on the questions that you must answer, the techniques available to use, when to use them and how to create a tactical plan to execute against.

Setting the vision

As with all things, in order to be really successful, it's best to start with the end goal in mind. That way, when you've finished and you step back and look at what was accomplished, you won't see smoldering craters of half completed attempts, but instead a string of well managed projects with measurable results, functioning as expected with all of the stakeholders sharing in the success.

With that in mind, envision what you would want to communicate to your organization, call it your press release, announcing the completion of yet another successful deployment of an encryption project. Here's a simple example that advocates the value of the project and alignment to the encryption strategy, and shows others how to get started with their own encryption project.

From: You

To: Exec Management; Business Directors
Subject: <APPLICATION or SYSTEM NAME> Successfully Encrypted per <INSERT ENCRYPTION PROJECT NAME>
<We/Team Name> are pleased to announce that the <named applications/significant assets> from our <named LoBs> are now fully encrypted and protected, compliant with <regulation name>, according to the <named directive> set forth by our <CISO/SECURITY LEADERSHIP>. Working together, the <encryption project/implementation team> along with the <named teams/application owners/dbas> accomplished this <ahead of/on> schedule, demonstrating our continued commitment to protecting our data where it matters <Insert project success metrics here, for example data set size, stage, time to value, overall impact and results> For more information, or to learn how to get your applications protected, contact <insert-project-team-owner-name-here>.

Delivering this type of message after each successful deployment shares the success of the project and the stakeholders involved, provides a continued sense of assurance and progress, proves the value of the investment in encryption, and, make no mistake, is your personal career builder.

Yes, that is putting the cart before the horse just a little, and to achieve this type of success you will have made sure that you've done the work. This includes:

- Developing and communicating the overall encryption strategy—Make sure that you use your management and stakeholders to assist you in crafting the strategy, and they support the plan. Continually review the goals and the progress, making any corrections or modifications along the way
- Understanding that encryption is just one, albeit very important, part of the overall "Defense in Depth" security strategy in use by your organization. Keeping the data encrypted and out of scope for unauthorized users and processes, including system administers, is crucial and you'll want to make sure that, however you choose to implement encryption, it fits in and plays well with your other solutions (i.e. Data loss prevention (DLP), Database activity monitoring (DAM), etc.)
- Ensuring that you've secured appropriate executive level buy-in and have a top level directive in hand. Trust me, you'll need this leverage when the pushback starts from a LoB, DBA or application owner who tries to tell you why their systems can't be encrypted
- Understanding the critical timelines you're working against—If it's not realistic, you've already failed or you should start the application process for waivers or extensions now so that your plan becomes more realistic
- Organizing the encryption program and empowering stakeholders—Make sure that the Business Owners, Application Owners, DBAs and Security teams are all sharing in the success and that they get the credit. This will be a team effort and there should be no heroes
- Prioritizing the work—The best approach to prioritization is to take a "Now—Next—Goal" view. Focus on those high value systems that must be done first, begin planning for the broader group of systems to start next, and always be working toward the end goal
- Focusing on getting a 'Quick Win'—Whatever tactical process you put in place for deployments (i.e. Crawl-Walk-Run or Live Data Transformation), plan on getting a few quick wins, targeting high profile applications or critical systems. Leverage these wins and their supporters to gather testimonials and momentum for the project
- Understanding the ongoing management required once the project has been completed—Know that whatever you implement will have a lifecycle

Know your audience

As you begin to formulate and discuss your strategy across the organization, make sure that you know who you're speaking to and what their primary concerns will be. Generally, it breaks down as follows:

- Executives and Board Members—Achieving compliance, impact on the business and the overall return on investment (ROI)
- Vice Presidents and Line of Business Owners—Total cost of ownership (TCO), impact to the organization, and time to value (TTV)
- Program and Project Managers—Time to value, time to complete and teams required
- Data Base Administrators and Application Owners—They want to understand "How it works", ensure that it's non-invasive and that it has no, or low, performance impact
- Other Admins (System, Storage, Network, Security)—They want to know "What" to do and "How" to do it

Conclusion

Don't be alarmed. Taking on the task of defining, deploying and achieving a high-value enterprise encryption strategy isn't as difficult as it sounds. Of course the devil is always in the details, but this guide is designed to help you develop your plan and provide the tools required to be successful.

Forming your encryption strategy

The scope of this guide is to provide you what you'll need to consider in order to protect the high-value enterprise assets that reside across the organization. This includes physical, virtual and cloud environments, whether public, private, on premise or off. This strategic guide focuses on the data, no matter where it resides or how it is created, which has no inherent ability to protect itself. This guide is not intended for endpoint protection, such as laptop, desktop or mobile devices.

Setting your strategy begins by asking 5 simple questions:

1. What are the broader goals, requirements or drivers that are to be measured for success/progress, or assessed for compliance?

2. Across the business, where will you choose to implement your strategy, and when?

3. How will you choose to implement your strategy?

4. What capabilities, skills and people are necessary to implement and maintain your strategy?

5. What technologies and systems are necessary to operate in order to build, maintain and sustain those capabilities, skills and people?

From these leading questions you'll derive and state the core elements that form your encryption strategy, including:

- The goals of the organization
- The critical drivers, such as regulations, legal compliance, SLAs or recent security breaches, etc
- The priorities that will drive your initial and ongoing activities, which will most likely focus on the highest value functions first
- The visibility of the overall strategy and its deployment across the enterprise
- The overall accountability of what is ultimately decided and deployed
- The systems you'll need to buy/build/maintain to your strategy
- The people you'll need to be successful in deployment of the strategy

Pro Tip: Start with the organizational goals and drivers. Use those to set your priorities, visibility (meaning who will care about and see the results), and assign the high-level accountability for the strategy and its success or failure. Next, assess the people and systems in place, or what will be needed, defining what new teams or groups need to be created, how you envision the separation of responsibilities, and what program oversight should be put in place, along with corresponding meetings for managing and reporting.

Figure 1—Forming the strategy

Ready to move forward

By now you should've noticed that all of this thinking and planning so far has been done without focusing on any specific technology vendor or encryption methods for protection. You're simply understanding where you are now, what's most important, what has to be achieved and who will be accountable. When you can articulate this, you will have your strategy.

Thinking tactics and technologies

Now that you have your strategy in hand, or at least a good understanding, it's time to start thinking about encryption techniques that may be used across the enterprise to protect data. At the highest level, you'll need to think about 'Data at Rest' and 'Data in Motion'. While 'Data in Use' may also be important to you, it is outside of the scope of this guide, as is 'Data in Motion'.

Data in Motion specifically covers how you protect data as it moves between systems and platforms, while Data at Rest covers how information is retrieved and stored, securely, by users, applications and databases. Disk Encryption is not covered in this guide, as the only real value it offers to an organization is to protect against the physical theft of a disk.

Protection of data in motion or at rest requires the use of encryption techniques, and there are many methods that can be used. However, all encryption has the same fundamental underlying need, and that is an encryption key. These keys are used to encode the data in such a way that without the same, or corresponding key, the data is rendered useless.

And this drives one of the biggest concerns that any organization will have, which is how to manage and supply keys for encryption.

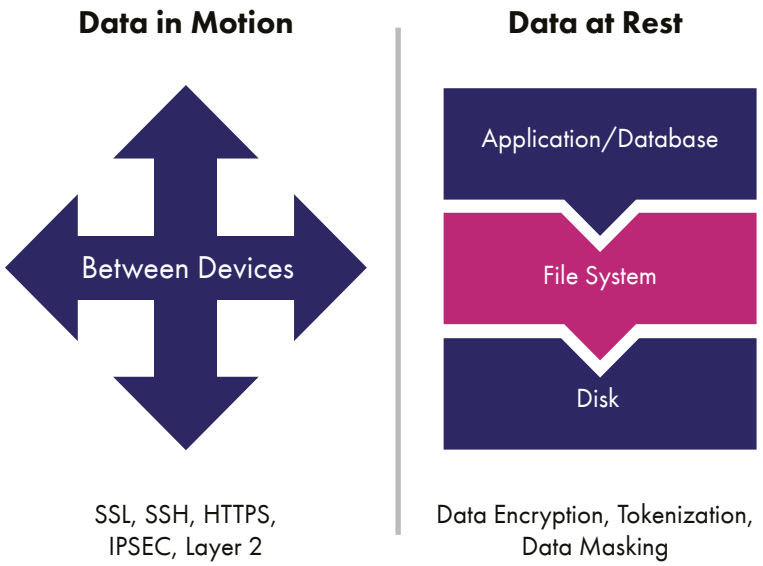

Figure 2—Data protection in motion and at rest

Encryption keys everywhere

The saying goes, "Encryption is easy! It's the key management that's hard." Of course this is true, and it will surprise you when you embark on data discovery how many encryption schemes and techniques are probably already in use within your organization. You may even take a moment and think that your work is already done, since application owners and DBAs have already deployed various techniques for their data.

Simply ask one question and you'll discover just how little thought is given to the proper encryption management, "Who is managing the encryption keys?" Once you've found that person or group, you're ready to ask the following questions:

- Should this person be managing keys?
- Who else can see or access the keys?
- How are the keys stored, maintained or backed up?
- What would happen if the keys were lost or compromised?
- How is key rotation managed?

As an example, if a DBA is using Transparent Data Encryption (TDE) for Oracle or Microsoft databases, you'll need to decide if that is consistent with your encryption and key management strategy, if the DBA controls the keys. Most likely it isn't.

Pro Tip: Getting tactical about encryption deployments and technologies means that you recognize the high value placed upon the management of the encryption keys that are in use across the enterprise. Therefore, you should focus on centralized key management that will store, protect, manage, rotate and backup any of the keys you use for protecting data. Centralized key management is a corner stone for assuring success in deploying your encryption strategy.

Also, if an application owner is creating and using encryption keys for their application data or configuration files, you'll need to assess the overall management and control of those keys to see if that also fits the strategy. The odds are that it doesn't meet the requirements and that you can greatly simplify the application owner's efforts by removing their key management concerns through a centrally managed capability.

Also, make sure you are realistic about the risks of not properly managing data encryption keys. Compromised keys can result in providing access to anyone that has access to the key. Note that lost or deleted keys can have the same impact as shredding the data, making it unusable forever.

Tactics for deployment of encryption

At the highest levels, defining your encryption strategy sets the "why?" for using encryption across the business, now you'll need to move to defining the "how?" for deploying encryption on platforms across your lines of business.

To achieve this, you should focus on the drivers for encryption for each system or platform, and how they align to your overall encryption strategy. Generally, the tactics are driven by answering the following questions:

What drives tactics for encryption deployment?

Why should you encrypt this system/platform/data? This is where you are making sure you are aligned with your strategy's goals and drivers

Who does the work? You're looking to make sure you have properly defined the teams and resources needed to complete the project

What data needs to be protected? This should align with your strategy's drivers, but also any discovery techniques that you may have defined in the systems part of your strategy

Figure 3—Tactical drivers

How does it get protected? Selection of an encryption method that is best suited for the application or data, but also must bring the types of controls that are needed to the surface. (We'll cover this more in detail later)

Where does it reside? This should begin to bring out all of the ways data can move in and out of your systems, and also onto the cloud. Additionally, your software development lifecycle (SDLC) will now come into play. Does data get shared between production and QA or development? Also, how are you managing and handling data archives?

When does it happen? As they say, timing is everything, and knowing when you can apply encryption will certainly impact your schedules. You should be developing your understanding of maintenance windows, business seasonality and downtime requirements, and any SLA or contractual obligations you may have to third parties

Even more important are your post deployment tactics:

- How will you review the deployment?
- How will you verify that the deployment and controls were properly deployed?
- What audit methods do you have in place for ongoing monitoring and controls?
- How do you report to your stakeholders?

Understanding that encryption isn't free

Whether it's impact on the applications, platforms, storage, personnel or program management, the deployment of your encryption strategy will have an impact on the organization. BE REALISTIC.

Manpower: There will be resources and manpower associated with the deployment of any new technology. Where will this come from? Who owns it and how should it be managed? Who should own roles and responsibilities and how do you want them enforced?

Encryption is math: Simply put, encryption is math and that has to occur somewhere. Will it be on the CPU or in a platform chipset accelerator? What impact will that have on performance and workloads? What happens to your fragile or legacy applications? What impact will that have on upgrades or environment changes?

Not all applications are good candidates for encryption. If you have applications running that are already pushing the limits of the hardware they're running on, or are resource constrained, the addition of encryption is only going to exacerbate or create new performance issues that could have additional cascading effects. Additionally, allocating more CPUs, memory or disk space could trigger new licensing events for other products that run on the platform, such as databases. Make sure that the discovery process
you are using for each targeted platform includes a broader understanding of any specific bottlenecks or limits that could prevent successful deployment.

The lifecycle of encryption keys: The keys that are used for data encryption, regardless of the specific encryption technique, will have a lifecycle, much of this driven by regulatory compliance. For example, PCI requires the Data Encryption Keys (DEKs) to be rotated (resulting in the rekeying of the data) on a consistent basis (typically every 24 months). The impact of rotating data encryption keys can be significant, possibly even resulting in application downtime. You need to determine what the key rotation requirements are for your business, capture and communicate those up front, and then drive awareness around the impact it will have on the encryption techniques chosen for the applications and databases. A 'rekey event' should never be a surprise to the business. Having everyone understand the necessity and the associated effort required to rotate keys, and the options that exist to assist in reducing or even eliminating downtime, will ensure that this is a well understood and planned exercise.

Plan for the future and plan on the cloud: Developing your approaches for platforms should be looking 3 and 5 years down the road, and where your business is going, how technologies change and where the cloud figures into the plans. Your approach should include both on premises and off premises in order to support private and public cloud options. Additionally, keeping up with the trends that are driving your developers and application owner's products, such as Dev Ops and containerization, may require unique capabilities. Look ahead and be sure that you've included their requirements so that you're ready with solutions when the time arrives, and the transition will be both seamless and supported.

Beware of legacy: In larger enterprises it's no surprise that there are legacy applications running on older hardware and operating systems. These can be terrible candidates for applying modern data security measures. There will be those platforms running End-of-Life operating systems or third party applications, typically requiring significant investments in custom maintenance and support with vendors. They will also be the most fragile systems in the enterprise, where changes or updates are rarely made, so as not to break them. You may also see new or updated systems popping up around these legacy systems, trying to keep them on life-support for just one more year while the organization spends its budgeted dollars in other areas. Owners will say "If it isn't broke, don't fix it!" to which you should add, "Then don't encrypt it either!" Even if you do successfully encrypt it, you can be assured that no matter what happens from that point on the encryption that was applied will be blamed as the root cause of every new problem, whether it is or not.

Sometimes you may need to take a longer term approach and let the demand to encrypt the platform drive or align with a system upgrade event or platform replacement. If the legacy environment is being phased out, replaced or upgraded a few months from now, maybe that's the best time to target your deployment.

Watch out for one-offs: Many times legacy environments won't have an exact matching Dev/Test/User acceptance testing (UAT) or Performance environments where you can accurately stage and prove out your encryption prior to going to production. Working directly in production environments is never advised, but is often unavoidable. Proceed with caution.

Understand performance requirements upfront: As stated above, encryption is math, and that means overhead. Everyone wants to understand how that overhead will impact their applications. Before starting an encryption project on any platform, make sure you understand how performance is being measured today. Where possible, you should always press the business, application owner or DBA for their performance metrics and how they manage their application changes today, before you begin. If they can't quantify it today, then doing it after encryption is completed will provide anecdotal evidence, at best, of the overall impact.

Also, to understand where the potential impact may occur, think in terms of workloads running on platforms using storage. Where:

- Workloads can be transactional, batch, ETL, File Server, etc.
- Platforms consist of CPUs, networks, memory, operating systems
- Storage is DAS, SAN or NAS, and how it's attached to the platform

Acceptance and performance test plans: Before you start an encryption project on a system, you'll want to make sure that you fully understand two specific areas of application or database testing. The first is a Basic Acceptance Test (BAT) that the application owners will run once the encryption is completed and that will show that the system is functional. The second level of testing will be performance testing which, as described above, should have already been reviewed in either QA, performance or DR environments.

The BAT should be something that can be run immediately upon completion of the encryption deployment, and it should provide a general indication of success. Any performance testing, while typically not run in production, should be consistent with tests run in other environments.

More importantly, the application owners and DBAs should be providing this information in advance and set the proper expectations, which should be realistic and aligned with deployment requirements.

Encryption with backups and storage requirements: Encrypted data, when viewed, is random binary digital information. There is no pattern to it by design, and therefore it does little to help support compression techniques and, in many cases, can increase the size of resulting compressed dataset. Most of the commercial grade backup and archive storage solutions in the marketplace today support their own internal encryption methods, which are typically applied to the data after it has been compressed. Be sure to understand what the data archive requirements are for your organization, the methods used for both archiving and restoring the data, and the impact of encryption in that process. You should also consider the long term reliance upon the vendors involved. Additionally, if backups are encrypted, understand the key management that is in place, and how it fits with the strategy you have in place.

Encryption & key management methods

In order to properly execute your encryption strategy it's important to take note of the encryption and data protection methods that are available, the requirements the applications or data to be protected have, and the reasons for applying the chosen protection method. Choosing a vendor with the broadest solution set available, and one that provides centralized key and policy management, will provide you easier deployment and management controls as you begin to grow your installed base.

The Vormetric Data Security Platform, which is centered around the Data Security Manager, is just such a platform. This provides the broadest coverage of capabilities, with industry leading features, and covers the broadest number of operating systems on the market. Since 2001, the Vormetric platform has been in use by the world's largest companies and governments, protecting hundreds of thousands of servers and untold amounts of data. A proven scalable platform supporting centralized key and policy management, making it easier to realize and support your Enterprise Encryption Strategy.

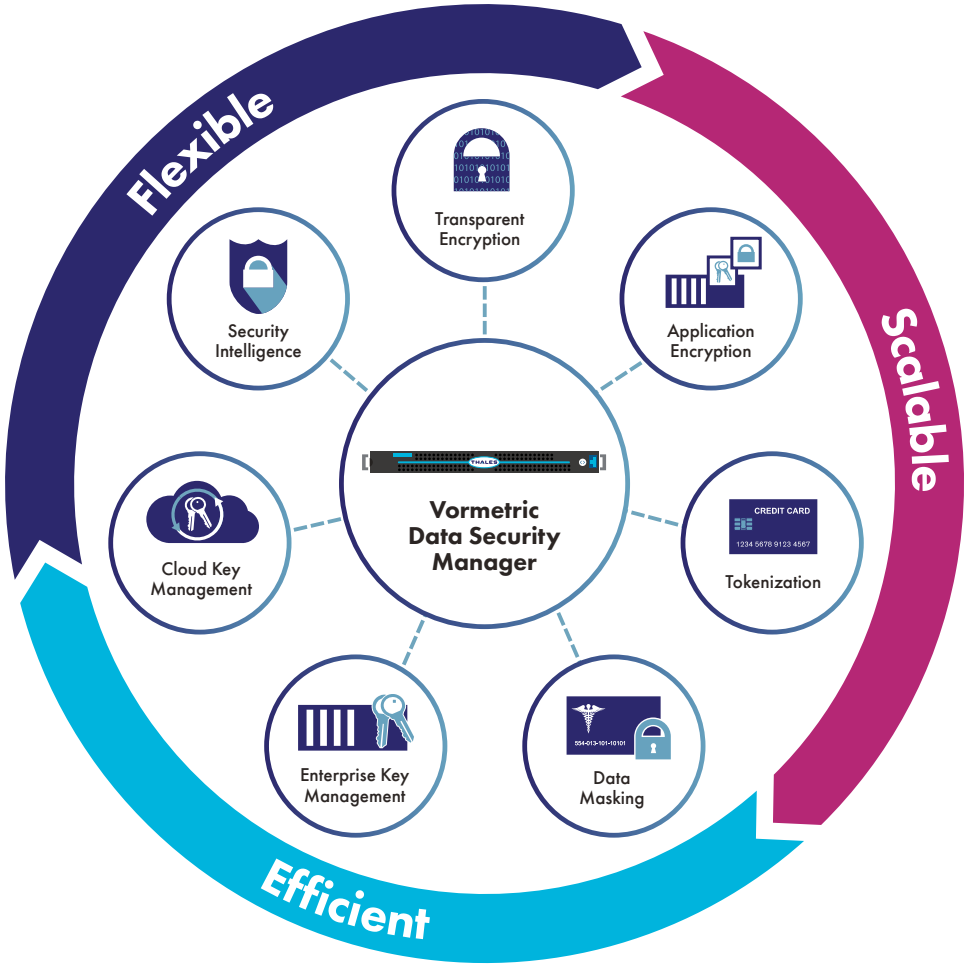

Figure 4— The Vormetric Data Security Platform

Encryption methods and deployment

When choosing the layer at which you will deploy encryption, you will ultimately make the tradeoff between complexity and security (refer to the figure on the right). The more complex implementations, including application level encryption and tokenization, will require changes be made to the source code or the database tables or stored procedures. These types of changes come at a cost, typically measured in the amount of time and effort to change the software, fully test, and then deploy it ultimately into production. While the least complex, full disk encryption offers no specific user or access controls to prevent unauthorized users from viewing data. It simply just encrypts the data on the disk, making it unusable should it be removed from the storage array. Certainly it provides encryption, but provides no protection and at a very significant cost.

What's needed is a broad set of techniques that gives your LoB, Application Owners and DBAs the wide array of options to protect the data how they choose and to participate in your encryption strategy at whatever level they choose.

Techniques

As described above, there are many techniques and methods that can be used to deploy your encryption strategy, and there may be no "one size fits all" technique, but having the options available on a single unified platform (Vormetric Data Security Platform) creates an easier task for you to manage. Below are quick overviews of some of the Vormetric encryption products you can use to meet all of your strategic objectives.

Transparent data encryption

The Vormetric Transparent Encryption solution protects data with file and volume level data-at-rest encryption, access controls, and data access audit logging without re-engineering applications, databases or infrastructure. Deployment of the transparent file encryption software is simple, scalable and fast, with agents installed above the file system on servers or virtual machines to enforce data security and compliance policies. Policy and encryption key management are provided by the Vormetric Data Security Manager. A quick time-to-value solution that provides enhanced capabilities for Live Data Transformation (no downtime), Docker Containers, Big Data and privileged user controls.

Tokenization

Vormetric Vaultless Tokenization with Dynamic Data Masking dramatically reduces the cost and effort required to comply with security policies and regulatory mandates like PCI DSS. The solution delivers capabilities for database tokenization and dynamic display security. This allows you to efficiently address your objectives for securing and anonymizing sensitive assets—whether they reside in the data center, big data, container or cloud environments.

Tokenization allows you to remove card holder data from PCI DSS scope with minimal cost and effort, and you can properly mask any production data before sharing with non-production environments or before moving it to the cloud or into shared big data environments.

Application level encryption

Application encryption solutions feature a set of documented, standards-based APIs that can be used to perform cryptographic and key management operations. Vormetric Application Encryption eliminates the time, complexity, and risk of developing and implementing an in-house encryption and key management solution, and provides the most popular OS and runtime compatible environments for your developers (Java, .NET, C, etc.).

Application encryption allows you to encrypt specific fields or files at the application layer, securing sensitive data before it is stored in database, big data, or cloud environments.

Key management and support for TDE, KMIP and more

With Vormetric Key Management, you can centrally manage keys from all Vormetric Data Security Platform products, and securely store and inventory keys and certificates for third-party devices—including IBM Security Guardium Data Encryption, Microsoft SQL TDE, Oracle TDE, and KMIP-compliant encryption products. By consolidating key management, this product fosters consistent policy implementation across multiple systems and reduces training and maintenance costs.

Or, use standards based APIs, (SDK or REST), to store keys and certificates you already use.

Secrets and other data

Understand and decide how the organizations needs to manage and control the use of a wide variety of objects beyond encryption keys, such as certificates, initialization vectors for application encryption, salts, and other secrets for Docker deployments.

Application encryption allows you to encrypt specific fields or files at the application layer, securing sensitive data before it is stored in database, big data, or cloud environments.

The enterprise encryption deployment lifecycle

Generally, you will have a deployment lifecycle for each encryption technique or method that you choose. This will be defined by you and the deployment teams and take into account any of the unique aspects of your organization and its requirements.

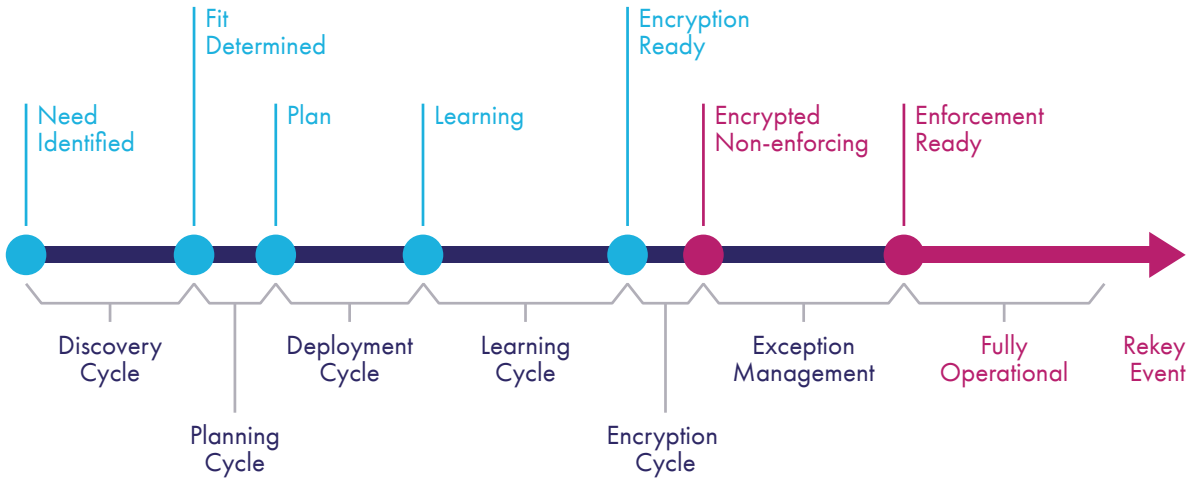

Figure 6— A sample deployment cycle for Vormetric Transparent Encryption

The figure above shows an example of a typical deployment lifecycle for Vormetric Transparent Encryption, from being made aware of application or platform needs, all the way through fully-protected encryption. This particular technique, referred to as Crawl-Walk-Run, allows for you to 'ease into encryption', applying all of the value and benefits of encryption before ever encrypting a single byte of data. This strategy allows you to demonstrate the proof points for encryption of data without putting any data at risk, to minimize the overhead of getting started and to understand who is accessing what data, with no impact on the organization.

The sample deployment plan includes:

Need – LoBs, Application Owners and DBAs will present systems for evaluation and participation into the encryption strategy, looking for guidance on best techniques, best known methods for deployment, and ultimately the ongoing monitoring and maintenance after integrating with the strategy. Once the need has been made known, you can progress through the steps for qualification and planning.

Discovery – The investigation of the systems, platforms, OS, datasets, requirements and constraints will all be gathered as part of the deployment exercise, and in accordance with the wide array of techniques, their advantages and disadvantages.

Fit determination – Ultimately, based upon information collected during discovery, there will be a decision on the value, method and approach for alignment to the encryption strategy.

Planning cycle – The planning cycle will take into consideration the inputs from Discovery and Fit determination and will begin laying out the project plan for deployment. This will include looking at the application or data lifecycle, how it moves through the SDLC, how best to begin and covers all aspects of getting to production and disaster recovery.

Deployment plan – Once completed, the deployment and project plans should be in place, and the teams should begin executing according to that plan.

The plan should cover the use of orchestration, where possible, and phasing in any installed agents during maintenance windows. The general outline for 'Change Tickets' that are typically required prior to performing those changes will be defined in this step, with the owners identified.

Learning – In this example, using Transparent Encryption, you would take advantage of the unique Learn Mode feature provided by the Vormetric platform, and begin tuning policies and techniques, typically without any impact on the applications or users. This low impact methodology is the beginning Crawl phase, of the industry leading Vormetric pioneered practice referred to as Crawl-Walk-Run. All of the policy controls are put in place, but the data is not yet encrypted. This is really the trial phase of the Transparent Encryption and can easily be turned on and off with no downtime requirements.

When 'Learning' you will specifically define the "WHO" aspects of data encryption, meaning which users, processes and resources will be protected, and how they will be protected.

Encrypting – Once the learning phase is completed to general satisfaction, the actual steps to encrypt that data are put into place. This, the Walk phase, allows for the data to be encrypted but no blocking by the policy. Learning is still enabled, any exceptions to the policy can easily be managed and you have complete assurance that access to the data will never be blocked, even though it is encrypted.

Enforcing – This is the Run phase. Once the policy has been sufficiently vetted, you simply disable learn mode, and begin blocking access to unauthorized users and processes, auditing all of the unwanted access via your syslog or SIEM tools. This is the go forward state that stays in place and keeps you protected.

Key rotation – At some point in the future, data encryption keys will need to be rotated. Whatever was defined by the encryption strategy, either following PCI or NIST standards, you will have to move the underlying data to a new encryption key. This event will take you back to the "Encrypting" phase above. However, if you are using the Vormetric premier feature of Live Data Transformation, this will happen automatically, and without any intervention required.

Similar deployment plans can be provided for each of the Vormetric data protection methods, and you can work with your deployment teams to determine the best processes for your environments.

Post deployment areas to watch

After the deployment of your techniques that meet your strategic objectives, you'll need to make sure that you have the teams and controls in place to monitor what has been accomplished, and continue to demonstrate alignment to the strategy. Any outliers or violations should be immediately visible and managed.

So, just like all things of value, even when you're done, you're never really done. You need to demonstrate operational ROI, and the value of your continued investment in the encryption strategy. There are several ways this should be done.

Integrating with SIEM tools and auditing activity

Ensure that the solutions deployed provide meaningful inputs to the SIEM tools you already use, and then use that data to demonstrate their value. Being able to see access violations by users, applications and privileged users within your organization will begin to give you better insight into the value of your encryption strategy. It will also provide guidance toward changes that should be made to eliminate those events in the future.

Monitoring system health

Being able to get an operational view of your deployed strategy, by systems, OS, policy and keys will provide real-time insight into how the strategy is working. Additionally, strong controls and options to manage your business continuity, disaster recovery and limit downtime will be key to the success of your strategy.

Personnel changes

It's good practice to always make sure that any new hires have training in the security and encryption products that they will support. Take the time to augment hiring and onboarding procedures and place this activity as an immediate requirement with HR or the manager. Also, make sure that any staff transitions include appropriate turnover of important system information related to management of any security, data protection or encryption systems that are in operation.

LoB and business QBRs

Quarterly Business Reviews (QBRs) are a great way to keep in touch, gain feedback and discover new opportunities for additional encryption projects. Set these up and use them to educate your organization on additional capabilities or changes from vendors. This will go a very long way to ensure that no one is ever surprised by upcoming advancements or changes, and that you have direct visibility into the impact of your encryption strategy and tactics. Take this opportunity to use real feedback to augment your strategy or techniques.

Vendor QBRs

Work with your vendor account team and go through a Quarterly Business Review. The QBR should cover a full year, quarter by quarter, and set both strategic and tactical sessions, where:

Strategic session – At least once per year you should invite your vendor and their executives to come onsite and visit your executive team. This is the opportunity for both organizations to understand and communicate what is or isn't working and commit to any changes. Additionally, you should review objectives, share any upcoming projects and discuss product roadmaps, futures and directions. This is always a great time to see how your vendor views changes in the industry and check for alignment.

Tactical sessions – Every quarter you should be meeting with your vendor by phone, WebEx or onsite, if possible, to cover overall product success and progress. Cover SLAs, outstanding support tickets, documentation, deployment guides, product quality, usability, and any requests for enhancements that you may have or need to be successful. Assign owners and responsibility and follow-up as needed to ensure you're receiving what you need to achieve success.

Vendor health checks

Schedule semi-annual health checks to make sure that your best practices are being followed and are aligned with the vendor's practices. Identify any shortcomings and address them.

Quarterly executive updates

"Reporting up" is an important factor to keeping the encryption strategy alive and moving forward within the enterprise. Make sure to take the opportunity to message on the metrics that demonstrate the success you have, and also call out any failures along with the 'RCA' (root cause analysis) and lessons learned. Any changes to strategy or tactics should also be communicated to the organization.

Summary

Congratulations! Hopefully you are well on your way to discovering and defining the encryption strategy that suits your enterprise. Whether large or small, the general process is the same for everyone, it's just a matter of how many players are involved in putting it to paper and getting the approvals needed to put it into motion. Maybe you've discovered something that you think should have been included or that you feel needs more detail.

The strategy and tactics described by this document are designed to force the discussions, derive the ownership and then lead to the assignments of the roles and responsibilities of the teams that will ultimately be involved in the work.

As we stated in the early part of this document, the devil is always in the details, and as you take up this challenge you'll need to maintain your focus, continually refer back to the strategic and tactical drivers that have put you on this path, and drive organizational commitments and personal ownership. For those who stand up to this challenge, the journey, the learnings, the failures (hopefully not many) and the successes (hopefully abundant!) provide some of the most rewarding experiences and lead to real understanding of just how the business really works.

Defining the strategy and seeing it put to work will be an experience that improves your overall visibility across the organization and results in increased responsibilities, as well as add value to your lists of skills. There are truly few such opportunities to make a real difference as impactful as this.

References & resources

Five Questions to Build a Strategy, Roger L. Martin, Harvard Business Review: https://hbr.org/2010/05/the-five-questions-of-strategy

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

THALES

Americas
Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 or +1 512 257 3900
Fax: +1 954 888 6211 | E-mail: sales@thalesesec.com

Asia Pacific – Thales Transport & Security (HK) Ltd
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 8141 | E-mail: asia.sales@thales-esecurity.com

Europe, Middle East, Africa
350 Longwater Ave, Green Park,
Reading, Berkshire, UK RG2 6GF
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

> thalesgroup.com <