Making the Business Case
FOR ENTERPRISE KEY AND CERTIFICATE MANAGEMENT
Executive Overview

At a time when most IT organizations are looking for ways to streamline operations—in order to deliver more value to the organization for less—every configurable component of the enterprise infrastructure is a candidate for automation. Implementing and maintaining encryption has long been conducted as a number of separate, unrelated tactical initiatives. Two conditions are rapidly causing such an approach to become impractical. First, unlike just a few years ago, today nearly every IT system is capable of encrypting; and second, nearly every type of organization is being pressured by external regulatory forces and internal practices to improve the protection of their critical data; and encryption is central to those initiatives.

By deploying more automation companies are able to achieve higher scale at a lower cost and they can actually free up resources that they’d like to invest in IT projects that actually help them grow the business. 1

Some of the less visible bi-products of the trend toward broadly enabling encryption include more encryption certificates and keys, and more variations in the way applications, platforms and systems are configured to encrypt. Venafi invented the industry’s first automation platform which allows organizations to more effectively implement and maintain encryption throughout their varied, and often disparate environments. Venafi calls its approach Enterprise Key and Certificate Management (EKCM). Venafi customers—which include some of the world’s most prestigious organizations in financial services, telecommunications, government, aerospace, healthcare, retail, airlines, technology, food services and other industries—have reported measurable improvements in operational efficiency, system uptime, compliance measurement, audit readiness and overall data security as a result of implementing their Venafi systems.

This document is designed to help organizations quantify and qualify the business value that can be attained from implementing EKCM solutions. The document reviews the problems and proposed systems to alleviate the problems from the perspectives of three organizational stakeholders: IT Operations (IT Ops), Privacy, and Information Security.

Making the Business Case for Enterprise Key and Certificate Management (EKCM)
As the number of encryption-enabled applications and platforms grows, and as certificate and key volumes continue to increase, administrators are struggling to keep up. Each vendor’s approach to encryption is different, offering no standard process for management. Thus, creating ownership confusion and overall under-management of encryption across the enterprise. These challenges are forcing companies to take a reactive approach to encryption management, just trying to keep up, rather than taking advantage of new business growth opportunities. In other words, encrypting data impacts existing business processes. Enterprises must be prepared for the organizational and operational changes that encryption will introduce by adhering to industry best practices.

Venafi products and solutions offer built-in best practices and helps organizations effectively deploy, manage, and control encryption from the desktop to the datacenter. Regardless of the environment, Venafi products perform four major functional operations in order to deliver comprehensive Enterprise Key and Certificate Management:

- **Discovery**: Allows administrators to identify all keys and digital certificates being deployed in systems that encrypt data. By broadly deploying encryption to protect sensitive data—in order to comply with policies and regulations—IT Ops and InfoSec teams are struggling to balance the requirement to protect critical data with the increased operational costs that will be required to properly maintain encryption, in order to avoid negatively impacting operational uptime or data effectiveness.
- **Monitoring**: Provides comprehensive metrics detailing the state of encryption across all environments, and delivers actionable alerts to key operators and decision makers.
- **Enrollment**: Facilitates continuous and automatic maintenance of certificates and keys throughout all stages of their lifecycle—from request to renewal or revocation.
- **Provisioning**: Automatically deploys keys and certificates, and configures applications to use them according to administrator-defined policies.

By automating encryption management, Venafi eliminates costly and error-prone manual processes, while ensuring consistent enforcement of encryption policies across the enterprise. As a result:

- CEOs and Boards of Directors are able to improve information risk management and IT governance, and demonstrate compliance.
- IT Executives (CIOs, CSOs, CISOs) have systemic, enterprise-wide compliance and control which provides measurement and accountability previously unavailable, and a platform to facilitate future growth.
- IT Operations is able to increase critical system uptime and operational efficiency.
- Information Security is able to improve compliance management and increase data security.

(InfoSec). These organizations are responsible for finding the appropriate balance between total security and total operational efficiency. While these objectives conflict with each other in many situations, Venafi customers have discovered that Enterprise Key and Certificate Management is one infrastructure decision that helps each discipline achieve their primary goals without negatively impacting the others, and often, while delivering useful benefits to all.

**Pressure Driving the Use of Encryption**

Regulatory and security concerns are driving organizations to deploy encryption more broadly than ever before. CIOs and Boards of Directors are responding by implementing organizational policies, which are handed down as mandates to IT executives (figure 1). These mandates are forcing IT departments to augment their traditional firewalls, intrusion detection systems, and security-hardening patches with additional layers of encryption technologies to protect their systems and applications.

This pressure has led to a spike in the number of keys and digital certificates being deployed in systems that encrypt data. By broadly deploying encryption to protect sensitive data—in order to comply with policies and regulations—IT Ops and InfoSec teams are struggling to balance the requirement to protect critical data with the increased operational costs that will be required to properly maintain encryption, in order to avoid negatively impacting operational uptime or data effectiveness.

More than 100 million personally-identifiable, customer records have been breached in the US over the past two years. Most of these breaches occurred at companies that are household names. These breaches solidified the threat for many executives who had previously not taken security very seriously. As a result, boards and top executives are demanding reports from their IT and security staff on the effectiveness of security controls within their organizations. 

Venafi products and solutions offer built-in best practices and helps organizations effectively deploy, manage, and control encryption from the desktop to the datacenter. Regardless of the environment, Venafi products perform four major functional operations in order to deliver comprehensive Enterprise Key and Certificate Management:

- **Discovery**: Allows administrators to identify all keys and certificates automatically, so they can be brought under management.
- **Monitoring**: Provides comprehensive metrics detailing the state of encryption across all environments, and delivers actionable alerts to key operators and decision makers.
- **Enrollment**: Facilitates continuous and automatic maintenance of certificates and keys throughout all stages of their lifecycle—from request to renewal or revocation.
- **Provisioning**: Automatically deploys keys and certificates, and configures applications to use them according to administrator-defined policies.

EXECUTIVE OVERVIEW

Figure 1 – Pressure driving the use of encryption

"In an environment where data breaches are happening with increasing frequency and severity, enterprises need a comprehensive solution that provides them with an end-to-end view of all encryption assets. Venafi’s solutions enable organizations to manage and control encryption assets throughout their lifecycle, from request to renewal or revocation, ensuring compliance and reducing security risk. By automating encryption management, Venafi eliminates costly and error-prone manual processes, while ensuring consistent enforcement of encryption policies across the enterprise. As a result:

- CEOs and Boards of Directors are able to improve information risk management and IT governance, and demonstrate compliance.
- IT Executives (CIOs, CSOs, CISOs) have systemic, enterprise-wide compliance and control which provides measurement and accountability previously unavailable, and a platform to facilitate future growth.
- IT Operations is able to increase critical system uptime and operational efficiency.
- Information Security is able to improve compliance management and increase data security.

As the number of encryption-enabled applications and platforms grows, and as certificate and key volumes continue to increase, administrators are struggling to keep up. Each vendor’s approach to encryption is different, offering no standard process for management. Thus, creating ownership confusion and overall under-management of encryption across the enterprise. These challenges are forcing companies to take a reactive approach to encryption management, just trying to keep up, rather than taking advantage of new business growth opportunities. In other words, encrypting data impacts existing business processes. Enterprises must be prepared for the organizational and operational changes that encryption will introduce by adhering to industry best practices.

Venafi products and solutions offer built-in best practices and helps organizations effectively deploy, manage, and control encryption from the desktop to the datacenter. Regardless of the environment, Venafi products perform four major functional operations in order to deliver comprehensive Enterprise Key and Certificate Management:

- **Discovery**: Allows administrators to identify all keys and certificates automatically, so they can be brought under management.
- **Monitoring**: Provides comprehensive metrics detailing the state of encryption across all environments, and delivers actionable alerts to key operators and decision makers.
- **Enrollment**: Facilitates continuous and automatic maintenance of certificates and keys throughout all stages of their lifecycle—from request to renewal or revocation.
- **Provisioning**: Automatically deploys keys and certificates, and configures applications to use them according to administrator-defined policies.

By automating encryption management, Venafi eliminates costly and error-prone manual processes, while ensuring consistent enforcement of encryption policies across the enterprise. As a result:

- CEOs and Boards of Directors are able to improve information risk management and IT governance, and demonstrate compliance.
- IT Executives (CIOs, CSOs, CISOs) have systemic, enterprise-wide compliance and control which provides measurement and accountability previously unavailable, and a platform to facilitate future growth.
- IT Operations is able to increase critical system uptime and operational efficiency.
- Information Security is able to improve compliance management and increase data security.
Building the Business Case
The table below lists some of the encryption management challenges experienced by IT Ops, InfoSec, and Privacy groups. The pages that follow address the issues associated with each of these challenges, and explain how Enterprise Key and Certificate Management and Venafi can help.

<table>
<thead>
<tr>
<th>IT Operations</th>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Reputational Risk</td>
<td>Information Security</td>
</tr>
<tr>
<td>2. Strategic Sourcing</td>
<td>1. Audit Readiness &amp; Compliance</td>
</tr>
<tr>
<td>3. Best Practices</td>
<td>2. InfoSec Agility</td>
</tr>
<tr>
<td>5. Operational Efficiency</td>
<td>4. Data &amp; Key Security</td>
</tr>
<tr>
<td>6. Disaster Recovery</td>
<td></td>
</tr>
</tbody>
</table>

Current State
The best known indication of un- or under-managed encryption manifests itself in the form of a “Security Alert” pop-up message in a web browser (figure 2). Security alerts appear if the browser cannot validate the authenticity of a website’s SSL certificate. This can have a devastating effect on an organization’s operating costs and reputation.

IT OPERATIONS: Reputational Risk
According to a recent study, 91% of respondents said they have seen an expired certificate manifest itself in the form of a security alert pop-up message in a web browser. Of those individuals, 43% said they stop using a website when they see a security alert. As a result, organizations are losing revenue due to lost transactions. On the other hand, 41% indicated they close security alert pop-up messages and proceed with their transactions (figure 3). In this case, companies are conditioning their customers to be more susceptible to identity theft (i.e. phishing or evil twin attacks). Essentially, un- or under-managed encryption is leaving organizations dangerously vulnerable.
Monitoring from Venafi gives enterprises the ability to send and receive advance reminders of pending certificate expirations, including the escalation of pending expiration notifications to ensure problems are addressed in a timely manner.

The Venafi enrollment capabilities simplify the certificate lifecycle and renewal processes by implementing self-service certificate requests and a renewal portal. Additionally, administrators can use a single, centralized process to work with any of the major CAs to reduce errors and user training and re-training.

Venafi gives organizations the ability to automate all previously manual processes, guaranteeing timely and accurate management of certificates and keys. This prevents embarrassing expirations from ever being seen by customers, prospects or partners.

ROI Formula
Use the following equation to calculate the cost of unexpected certificate expirations and security alerts.

```
Cost of lost customers x Average value of a customer + Cost of missed transactions x Average transaction value + Cost of increased call center volumes x Cost per call + Cost of unplanned certificate expirations/security alerts = Business losses following an outage— in many cases irretrievable losses—include missed sales opportunities, damaged credibility, and brand name degeneration.”
```

How Venafi Helps
With Venafi organizations are able to protect their reputation by discovering all certificates (including self-signed) and keys so owners can be notified in time to complete maintenance prior to expiration. Additionally, administrators are able to use regularly scheduled discovery surveys for continuous monitoring of their encryption environments throughout the enterprise—ensuring previously unknown (self-signed or rogue) or under-managed certificates never cause unanticipated downtime.
Current State

With certificates ranging in price from $100 to $1,400+, many organizations spend hundreds of thousands of dollars procuring all of the necessary encryption certificates each year. Internal Certificate Authorities (CAs) can be just as costly. Additionally, the migration process is time consuming and cost prohibitive—causing some organizations to get locked in with certain vendors.

These costs can often be reduced by consolidating certificate procurement to obtain volume pricing from CA vendors, or switching to a lower-cost CA vendor where appropriate. In addition, organizations can employ an effective internal CA strategy that ensures more costly certificates issued by a commercial CA are not being used in applications where certificate brand is not important (such as in machine-to-machine connections).

Clearly, strategic sourcing is a way to more effectively align IT governance with the business. The challenge is to find the best set of sourcing solutions to meet the strategic needs of the organization.

In cost-conscious times, IT sourcing and procurement executives are faced more than ever to deliver measurable results in the shortest amount of time possible. It is also imperative that their strategy and execution have a positive, visible impact on the bottom line.\(^1\)

How Venafi Helps

Enterprise Key and Certificate Management allows companies to catalog all discovered certificates and CAs to determine the most cost-effective vendor selection, and uses spend tracking to identify systems where lower-cost certificates could be used (self-signed or from less-expensive CAs). This helps eliminate vendor lock-in and helps IT Ops negotiate pricing with CA vendors.

Additionally, Venafi provides early warnings of non-compliant certificates and keys to ensure situations can be remedied before a security breach or failed audit occurs.
Current State
The IT Infrastructure Library (ITIL) was developed by the UK government and outlines best practices in IT Service Management (ITSM). It is intended to assist organizations develop a framework for ITSM. A configuration management database (CMDB) is an essential component of the ITIL framework. A CMDB is a repository area with details related to all components of an information system. In the context of ITIL, a CMDB represents the authorized configuration of the significant components of an IT environment. A major goal of a CMDB is to help an organization understand the relationships between components and track their configuration.

How much time do you spend fixing unplanned outages? If IT firefighting and last-minute changes often sap your nights and weekends, and you don’t know where to begin when a critical system fails, there’s hope. The prescription for this chaos is ITIL (IT Infrastructure Library), a set of best practices for running an IT organization.

“ITIL is really common sense. It’s what many successful organizations already do—the processes we’ve learned from the school of hard knocks. ITIL forges a bond between IT, management and external customers by offering them a single language and defined channels for communicating with one another.

“IITL normalizes the language describing best practices. For example, a resolution process like incident management indicates a single failure in ITIL parlance. Problem management, another ITIL resolution process, stitches together all incidents that relate to a particular problem.”

One of the top challenges organizations face when implementing a service management program is measurement. Most organizations do not have the ability to test and ensure ITSMs work and are used properly. This is in large part due to the costs and time required to gather and collate data indicators. Many organizations set policies, and put them in motion without determining how they will track adherence, until it’s too late.
How Venafi Helps
Venafi allows organizations to inspect all systems throughout the infrastructure on a regular basis, and to identify previously unknown certificates and keys and add them to a master inventory list. Venafi monitors for things such as approved CAs, key lengths, time to expiration, and validity periods.

Next, Venafi allows administrators to use meta information such as department, cost centers, policies or regulatory requirements, etc. with systems utilizing encryption. Administrators can also send proactive notifications to system owners of pending expirations. This enables enterprises to improve their change control processes and enrich ITIL and CMDB initiatives.

With Venafi, organizations are able to establish clear certificate issuance and renewal process workflow to ensure proper approvals are given at the appropriate intervals. Administrators are also able to generate reports to track compliance with established policies and procedures, and analyze and refine best practices, including the removal of self-signed, rogue, and non-approved certificates.

IT professionals are able to institutionalize best practices by automatically configuring platforms and applications in a universal manner according to organizational policies and industry regulations, as well as inspect systems to ensure they are configured according to policy and regulation.

The automation software emerging today also relies heavily on best practice frameworks, such as the IT Infrastructure Library, or ITIL. The coupling of best practices with automation could help IT managers introduce more operational efficiencies into their environments.  

ROI Formula
Use the following equation to calculate the cost of implementing and adhering to best practices:

Cost to properly configure and maintain inventory of certificates and keys

Cost of (re)training, admin turnover, version changes, growth, etc.

Cost of (re)creating reports

Cost of implementing best practices
Current State
The first step in managing encryption is to understand where encryption certificates and keys are already deployed and what risks are imminent—such as which certificates are about to expire and where self-signed or rogue certificates are being used in violation of organizational policies. In order to wrap their arms around their situations, most organizations rely on manual processes such as making requests in meetings or sending emails.

Due to limited visibility and inappropriate configuration of encryption environments, organizations have minimal understanding and control of their infrastructure—including rogue, self-signed, intermediate root, partner and other certificates they do not know about. Many systems and applications automatically install certificates that are often non-compliant with corporate policies and industry best practices. Subsequently, they go unmonitored—increasing the risk of system failures. As a result, companies are losing revenue. According to the Meta Group the average cost-per-hour of downtime for large enterprises is over $1M. Additionally, the intangible impact of downtime includes employee dissatisfaction, decreased productivity, dissatisfied customers, reputational damage, etc.

For companies that rely entirely on technology, such as online brokerages, trading platforms and e-commerce sites, hourly downtime risks can be $1 million or more, making availability an even greater concern.

Critical system downtime can also occur if expired root or intermediate root certificates are unknowingly reinstalled when administrators re-image machines or systems, or when there are changes in application and system support matrices. As software and hardware vendors create patches and updates to their products, the configuration of encryption needs to be updated.

How Venafi Helps
The Venafi discovery capabilities ensure system availability by collecting an inventory of all certificates and keys that are currently in use and identifying the most urgent certificates that pose downtime risks. With continuous monitoring, Venafi allows organizations to use regularly scheduled discovery surveys of their encryption environment throughout the enterprise, ensuring previously unknown certificates never cause unanticipated downtime.
Venafi also sends notifications to certificate owners of approaching expiration dates and can automatically escalate them if certificate renewal is not completed in sufficient time. This also includes monitoring intermediate root certificates.

With encryption management from Venafi, organizations can accelerate and simplify certificate provisioning and replacement with CA task automation. Administrators can use reports to identify and prioritize problems, and ensure the most important tasks are completed first.

Venafi can be set to automatically replace risky or non-compliant certificates (including self-signed certificates) upon discovery or expiration, as well as automatically distribute intermediate root certificates. These automated and repeatable processes reduce administrator errors.

ROI Formula
Use the following equation to calculate the cost of downtime per certificate:

\[
\text{Cost of system downtime} = \text{Frequency} \times \text{Impact} \times \text{Cost per hour of downtime} \]

According to a recent Venafi survey, companies are spending an average of 4.5 hours per year\(^1\) to manually manage each certificate deployed within their infrastructure. Multiplying this time by the number of administrators, certificates, and systems in place, one begins to understand the work involved in manually managing digital certificates (figure 4). As a result, administrators are struggling to keep up, let alone implement best practices.

Venafi also sends notifications to certificate owners of approaching expiration dates and can automatically escalate them if certificate renewal is not completed in sufficient time. These manual processes can be inefficient, error-prone, and consume valuable human resources that could be better allocated to developing and implementing new business systems and responding to new business challenges. Meanwhile, regulatory bodies continue to craft new regulations, costs continue to increase and IT staffs continue to remain stagnant or contract.

Venafi’s encryption management solution can accelerate certificate provisioning and replacement with CA task automation. Administrators can use reports to identify and prioritize problems, and ensure the most important tasks are completed first.

Venafi can be set to automatically replace risky or non-compliant certificates (including self-signed certificates) upon discovery or expiration, as well as automatically distribute intermediate root certificates. These automated and repeatable processes reduce administrator errors.

**Figure 4 – Manual Certificate Management Steps**

---

\[\text{PRIVACY} \quad \text{OPERATIONAL EFFICIENCY} \quad \text{DISASTER RECOVERY} \quad \text{POLICY ENFORCEMENT} \quad \text{AUDIT READINESS & COMPLIANCE} \quad \text{INFOSEC AGILITY} \quad \text{DATA & KEY SECURITY} \]

---

\[^{1}\text{The company}\] renewed its certificates last week prior to their expiration on the 7 March, but when these new certificates were installed on Tuesday night/Wednesday morning, there was a typographical error on one half of our clustered servers which didn’t show up on our commission tests.” \(^{11}\)
Current State
Although most businesses understand the operational and financial risk a disruption to their business systems could pose, disaster recovery (DR) planning is costly work that many organizations undertake reluctantly. However, implementing a comprehensive DR strategy is not optional. According to analyst firm IDC, over 90 percent of companies fail within one year of a significant data loss. Additionally, the Disaster Recovery Journal estimates that as many as 80 percent of all U.S. companies and 90 percent of European companies do not have an effective DR plan.

The world’s leading organizations constantly test and re-evaluate their disaster recovery plans and procedures. Some encryption-related scenarios that many Venafi customers are beginning to address in their planning include Certificate Authority (CA) compromise, encryption algorithm breaches, private key compromise, and intermediate root expiration. Most organizations would risk sustained periods of downtime if any of these events occurred, and they were required to manually respond, because each of these scenarios would require a wholesale replacement of affected certificates.

How Venafi Helps
Venafi provides administrators with self-service Web interface to request certificates. This allows them to build an automated workflow approval process which is consistent with internal policies and procedures. Additionally, Venafi helps eliminate the training and re-training of administrators due to turnover or because they manage certificates and keys infrequently.

With automated encryption provisioning, Venafi eliminates the manual work required to configure applications to utilize encryption. As a result, it reduces anxiety, and improves the ability to reallocate one FTE to other business responsibilities or initiatives for every 500 certificates brought under automation.

Having a DR plan is obviously important, but without thorough testing and documented recovery plans, the effectiveness of any plan is only theoretical. For many organizations, end-to-end testing is considered too cumbersome and disruptive to operations, so it is simply replaced by more limited testing.

How Venafi Helps
Venafi provides administrators the ability to maintain a detailed record of all encryption keys and certificates, and their locations. This assists in responding to disasters such as a CA-root or encryption algorithm compromise. Additionally, they are able to discover expired or soon-to-expire certificates residing on failover and DR sites. Additionally, Venafi helps administrators ensure intermediate root certificates do not expire unexpectedly.

Venafi also allows administrators to provision replacement certificates rapidly if necessary, and automatically maintain DR and fail-over sites with appropriate keys and certificates.

IT OPERATIONS: Disaster Recovery

How Venafi Helps
With automated discovery capabilities, administrators no longer need to use manual certificate tracking methods—such as calendar reminders and spreadsheets. Venafi will automatically notify certificate owners of pending expirations. With the ability to maintain an accurate inventory of certificates, companies are able to avoid unexpected outages. By proactively monitoring certificates and keys, administrators will be able to improve the predictability of resource planning. When unexpected system failures occur, discovery results accelerate the troubleshooting process.

Venafi provides administrators with a self-service Web interface to request certificates. This allows them to build an automated workflow approval process which is consistent with internal policies and procedures. Additionally, Venafi helps eliminate the training and re-training of administrators due to turnover or because they manage certificates and keys infrequently.

With automated encryption provisioning, Venafi eliminates the manual work required to configure applications to utilize encryption. As a result, it reduces anxiety, and improves the ability to reallocate one FTE to other business responsibilities or initiatives for every 500 certificates brought under automation.

ROI Formula
Use the following equation to calculate the annual cost of administration.

\[
\text{Annual cost of administration} = \frac{\text{Total number of systems to manage} \times \text{Average time required to manage each system} \times \text{Cost per hour of admin}}{\text{(I+3) training admin turnover, version changes, growth, etc.}}
\]
Current State

The potential impact of privacy breaches on a company’s brand is significant. It is safe to say that bad press equals brand damage—and few things cause more brand damage than the data breach of an employee’s or customer’s private data. Enterprises realize the need to encrypt their company data, but often delay doing so due to the complexity of manual encryption management. As a result, they are putting their brand reputation at risk.

Some companies are dragged into compliance kicking and screaming, but there’s nothing like the prospect of brand reputation damage and lawsuits to get them to do what’s necessary to secure systems and respond properly when there is a breach. 19

In addition to brand management, large financial fines and penalties due to regulatory compliance are also drivers for the implementation of encryption. For example, the United States Department of Commerce and the European Commission have agreed on a set of data protection principles and frequently asked questions (the “Safe Harbor Principles”) to enable U.S. companies to satisfy compliance with the requirements under European Union law that adequate protection be given to personal information transferred from the European Union to the United States. Although most organizations value the importance of developing and adhering to Safe Harbor policies, they do not have the ability to enforce them. This is due to the inability to deploy and manage the necessary certificates and keys to protect customer and employee data.

Safe Harbor stipulations require that: companies collecting personal data must inform people that the data is being gathered, and tell them what will be done with it; they must obtain permission to pass on the information to a third party; they must allow people access to the data gathered; data integrity and security must be assured; and a means of enforcing compliance must be guaranteed. 20

How Venafi Helps

Venafi allows organizations to demonstrate the breadth of encryption in use throughout the enterprise by providing detailed inventory reports. Systems can be configured to send and receive advance notifications of pending certificate expirations to ensure an unexpected expiration never occurs. This includes the escalation of pending expiration notifications, if necessary, to ensure problems are addressed in a timely manner.

ROI Formula

Use the following equation to calculate the cost of recovery across all systems protected by certificates and keys.

\[
\text{Cost of disaster recovery per incident} = \left( \frac{\text{Number of certificates/keys} \times \text{Cost per hour of downtime}}{\text{Average time to replace each certificate/key}} \right) \times \text{Number of certificates/keys that can be replaced simultaneously} \times \text{Total number of admin for manual operations}.
\]
The certificate enrollment process is also simplified by automating interaction with certificate authorities for certificate issuance or renewal. By automating all previously manual processes, organizations can guarantee timely, accurate management of certificates and keys in all instances, before embarrassing expirations are seen by customers or partners. As a result, they are able to demonstrate that the standard of due care has been met, consistent with safe harbor requirements.

There are two axioms that we have to live with. Data wants to be free and shared. It’s just the nature of data. And the second is that networks will be attacked. The combination of the two says we really have to take a data-focused approach to protecting information regardless of where it is, where it’s located and its status whether it is in transit or not. Data will ultimately become visible to people to whom you don’t want it visible and the answer is that it has to be protected regardless of where it is. The only way to effectively protect it is a well implemented and well constituted data encryption program.” 21

ROI Formula
Use the following information to qualify the value of improved privacy controls.

### Consideration 1

| Value of improved risk posture due to ability to enforce policies that leverage safe harbors | Cost of failed audit due to inability to demonstrate compliance with standard of due care |
| Values of automatically enforcing compliance with privacy regulations | Value of automatically enforcing compliance with privacy regulations |

### Consideration 2

| Cost of a breach resulting in lost data subject privacy laws that could be prevented by encryption | Severity of breach |
| Brand erosion | Impact on value of company | Fine |
| Cost of reporting | Lost customers |

**INFORMATION SECURITY: Audit Readiness & Compliance**

**Current State**

An auditor’s job is to ensure enterprises are exercising due caution when dealing with certificates and keys because certificates and keys are the roots of trust protecting the information auditors are trying to make sure organizations are effectively protecting. They want to ensure companies know who has access to what, when they accessed it, why they accessed it, and that everything is in line with policies and regulations. Additionally, corporate executives want to ensure compliance and avoid large lawsuits and financial fines—including replacement of compromised cards, fraudulent charges, etc.

Automated, cost-effective enterprise data protection solutions are now available to secure data both within an organization and among business partners. Centralized management of encryption solutions allows information protection to be aligned with corporate security policies and regulatory or business-partner mandates. A holistic approach to data protection—at rest, in motion and in use—allows security best practices to be automatically enforced throughout the enterprise.” 22

Manually managing compliance to adhere to regulations and policies takes time and money, which puts pressure on information security professionals, and in most cases, distracts them from their other job responsibilities. Information Security departments struggle to find repeatable processes to help them identify security threats and prove to external auditors that they have in place the security controls they need to protect sensitive data. Due to the lack of automated logging and reporting, and the ability to associate data classification with the business drivers for encryption, many organizations put themselves in an indefensible position by not being able to quickly and cost-effectively prove sensitive data is properly protected. As a result, they put themselves at risk of large financial penalties. Even after considerable effort, organizations still may not be able to provide a complete view of their encryption practices. Additionally, if they are found to be out of compliance, organizations have to repeat the entire audit process again to show they have corrected any errors and that they have become compliant.

Chief Information Security Officers (CISOs) are often tasked with providing to auditors reports that show that the organization is exercising due care when dealing with sensitive data. Due care often includes monitoring access and managing event logs effectively, remediating vulnerabilities as they surface, and making sure configurations are in line with policy.” 23

Additionally, organizations struggle with adherence to Separation of Duties (SoD) policies. SoD is commonly used in large IT organizations so that no single person is in a position to introduce risk to data without detection. However, strict control of software and data changes will require that the same person or organization performs only one of the necessary functions of any operation. For example, if Employee A is responsible for encrypting data and is also the primary operational owner for key management, an organization is not complying with SoD policies.

**POLICY ENFORCEMENT**

**CONCLUSION**

**AUDIT READINESS & COMPLIANCE**

**INFOSEC AGILITY**

**DATA & KEY SECURITY**

**ROI Formula**
Use the following information to qualify the value of improved privacy controls.

**Consideration 1**

| Value of improved risk posture due to ability to enforce policies that leverage safe harbors | Cost of failed audit due to inability to demonstrate compliance with standard of due care |
| Values of automatically enforcing compliance with privacy regulations | Value of automatically enforcing compliance with privacy regulations |

**Consideration 2**

| Cost of a breach resulting in lost data subject privacy laws that could be prevented by encryption | Severity of breach |
| Brand erosion | Impact on value of company | Fine |
| Cost of reporting | Lost customers |
How Venafi Helps
To ensure audit readiness and compliance with industry regulations and organizational policies, Venafi allows administrators to maintain a detailed record of all encryption keys and certificates and their locations.

The Venafi monitoring capabilities allow administrators to demonstrate that processes are in place to notify owners of certificates and keys whenever issues are detected or attention is required. Certificates and keys can also be assigned to specific owners so they can be reminded of scheduled maintenance. Meta data tags let administrators generate reports by department, cost center, associated applications, regulatory requirement, and so on; as well as maintain forensically durable logs of discovery results and renewal alerts.

Encryption management from Venafi also allows security professionals to enforce a standard workflow for certificate issuance and renewal processes that are consistent with internal policies and procedures. Additionally, it enables administrators to maintain forensically durable logs of CA task automation and self-service operations across all CAs in use, as well as meet separation of duty (SoD) requirements.

The provisioning capabilities provided by Venafi protect organizations from costly and time-consuming failed audits. Venafi allows organizations to remedy non-compliant systems by automatically applying compliant system configurations and inspect systems to ensure they are compliant with external regulations and internal policies.

With the ability to maintain forensically durable logs of all encryption management operations, security professionals can quickly and easily demonstrate that a standard of due care has been met, consistent with safe harbor requirements by illustrating the breadth and depth of encryption deployments and management processes.

Venafi helps enterprises avoid costly follow-up audits, fines, and lawsuits caused by failed audits by regularly conducting self-compliance inspections.

ROI Formula
Use the following equation to calculate the cost of showing compliance.

\[
\text{Cost of achieving compliance} \times 2 = \begin{cases} \text{Average time to audit} \\ \text{Systems Management application} \\ \text{Cost of non-compliance (finas)} \\ \text{Reputational impact} \\ \text{Hourly cost of auditor} \\ \text{Hourly cost of admin/consultant} \end{cases}
\]

Icon Legend
- Discovered value is in compliance with policy
- Discovered value should be inspected vs. policy
- Discovered value is out of compliance with policy
- Value matches policy
- Policy suggests value, user can overwrite
- Policy requires specific value be used

Figure 5 – Certificate policy compliance interface
Current State

The costs associated with manual encryption management often prevent organizations from deploying the appropriate levels of encryption and putting proper processes in place. The tug-of-war between IT Operations and Information Security professionals (figure 6) is often referred to as the “IT Security Conundrum,” is also slowing down the deployment of encryption. IT Operations wants full business application functionality, but Information Security teams want total security. In many cases, increasing security negatively impacts application performance; and increasing application performance often requires more open, less secure systems.

Referring to “The IT Security Conundrum,” IDC states:

- There is a struggle to achieve a balance between level of protection and business productivity.
- Security adds complexity and costs.
- Threats impact availability and opportunity.
- Security solutions must be manageable to provide real benefit.

The key is to find the proper point on a continuum between total security and no business application functionality on one end and no security and full business application functionality on the other." 24

Figure 6 – Tug of War between IT Ops and Information Security
How Venafi Helps

Venafi provides administrators the ability to discover imminent expirations and rogue CAs, and quickly remedy any problems. Administrators can also discover new encryption deployments early on to ensure InfoSec policies and requirements are being followed. In the case of one organization acquiring another, Venafi can quickly assess the state of encryption of any new infrastructure and prioritize pertinent maintenance work required.

With proper monitoring capabilities, organizations can properly scale encryption deployments and manage more encryption at a lower cost by automating compliance and maintenance alerts and notifications. This, in turn, frees up funds for additional encryption deployments by replacing unnecessary high-cost certificates with lower-cost ones.

Venafi also simplifies certificate requests and issuance processes through a self-service portal, making it more palatable to use certificates. Additionally, administrators are able to use a centralized certificate request and renewal portal to meet new business requirements for increased encryption deployments, whether with new or existing CAs.

 Provisioning from Venafi decreases the operational costs of encryption and lowers the TCO, making it possible to implement more encryption for less. By taking an Enterprise Key and Certificate Management for encryption approach, and by automatically configuring applications in a way that is consistent with policies, organizations will reduce organizational friction (IT Security Conundrum), and eliminate the operational burdens caused by broad encryption deployments.

ROI Formula

Use the following equation to calculate the value of increased InfoSec agility.

\[
\text{Value of increased InfoSec Agility} = \frac{\text{Cost to compare systems of acquired entity to policies of acquiring company}}{\text{Cost to modify systems of acquired entities to comply with policies}} + \frac{\text{Value of integrating systems of acquired entity with no impact on customers}}{\text{Cultural value of eliminating a point of internal friction/hassle (neutralize IT setup-of-war)}}
\]
Current State

Due to the fact that most organizations struggle to efficiently deploy encryption, they labor to implement it thoroughly throughout the enterprise, whether it is data in transit, or data spread across highly distributed environments. Moreover, because manually deploying encryption is so operationally challenging, organizations are making a conscious decision not to deploy encryption. As a result, companies are not only leaving themselves vulnerable to various attacks and data breaches—internally and externally—but they are putting themselves at risk of losing revenue, diminishing their company brand, and paying fines.

Companies complain that encryption products are cumbersome, expensive and difficult to manage. Really? You know what else is expensive and difficult to manage? A data theft. It’s bad enough that attackers are able to get inside the perimeters of the companies, but they certainly shouldn’t be able to find any unencrypted customer records once they get there.27

Even if organizations are able to implement an adequate level of encryption, their struggle then becomes key management, which requires numerous steps and processes. Encryption is only as good as an organization’s ability to appropriately manage the associated certificates and keys.

How Venafi Helps

Expired certificates can become attack vectors, because they often indicate systems that have not been properly patched and are therefore vulnerable to attacks. With the ability to discover and identify certificates and keys that are of insufficient strength, or are otherwise weak or need attention, Venafi helps organizations improve their data security and key management capabilities. With the ability to identify deployed encryption, management practices can be reviewed. Additionally, reports can be generated showing unsecured systems (ports without certificates).

Venafi can be set to notify application and system owners automatically when certificate and key management issues are detected, such as unapproved CAs, weak key lengths, upcoming expiration, and improper validity periods.

Venafi also helps organizations improve their security posture by automatically controlling key and certificate specifications. Decreasing the operational costs of encryption lowers the TCO, making it possible to implement more encryption for less. Due to the nature of the work the Venafi system performs, there are a number of security features included in the product, including forensically durable logging, HSM integration (optional), separation of duties, trust management, and other relevant features.

INFORMATION SECURITY: Data & Key Security

Figure 7 – Source: Forrester Research, Inc.26

ROI Formula

Use the following equation to calculate the cost of enforcing security policies and regulations.

Even if organizations are able to implement an adequate level of encryption, their struggle then becomes key management, which requires numerous steps and processes. Encryption is only as good as an organization’s ability to appropriately manage the associated certificates and keys.

How Venafi Helps

Expired certificates can become attack vectors, because they often indicate systems that have not been properly patched and are therefore vulnerable to attacks. With the ability to discover and identify certificates and keys that are of insufficient strength, or are otherwise weak or need attention, Venafi helps organizations improve their data security and key management capabilities. With the ability to identify deployed encryption, management practices can be reviewed. Additionally, reports can be generated showing unsecured systems (ports without certificates).

Venafi can be set to notify application and system owners automatically when certificate and key management issues are detected, such as unapproved CAs, weak key lengths, upcoming expiration, and improper validity periods.

Venafi also helps organizations improve their security posture by automatically controlling key and certificate specifications. Decreasing the operational costs of encryption lowers the TCO, making it possible to implement more encryption for less. Due to the nature of the work the Venafi system performs, there are a number of security features included in the product, including forensically durable logging, HSM integration (optional), separation of duties, trust management, and other relevant features.
Modern IT organizations need a holistic enterprise encryption and key management platform to address data security in a comprehensive manner. Venafi offers the industry’s first enterprise-wide system for automating the deployment, management, and control of encryption certificates and keys across applications, platforms, certificate authorities, and different key protocols within major operating environments—from the desktop to the datacenter. Venafi helps organizations automate the complex processes required to manage the full lifecycle of encryption assets and reduces system downtime and helps improve regulatory compliance. Some of the world’s most prestigious organizations are already using Venafi, including financial services, telecommunications, government, aerospace, retail, healthcare, airlines, technology companies, food services and others.

To support the broader deployment of encryption and to deal with the management of encryption and the encryption key lifecycle, organizations with top performance are looking towards increased automation and centralized, heterogeneous approaches to management. In doing so, the research shows that they are delivering the benefits of improved security, sustained compliance, and lower operational costs. 28

Aberdeen Group

---

Conclusion

Modern IT organizations need a holistic enterprise encryption and key management platform to address data security in a comprehensive manner. Venafi offers the industry’s first enterprise-wide system for automating the deployment, management, and control of encryption certificates and keys across applications, platforms, certificate authorities, and different key protocols within major operating environments—from the desktop to the datacenter. Venafi helps organizations automate the complex processes required to manage the full lifecycle of encryption assets and reduces system downtime and helps improve regulatory compliance. Some of the world’s most prestigious organizations are already using Venafi, including financial services, telecommunications, government, aerospace, retail, healthcare, airlines, technology companies, food services and others.

Venafi Encryption Director is an encryption key and certificate management platform that simplifies the lifecycle management of encryption technologies across diverse operating systems and infrastructure environments. The Director product line consists of three products: Director Certificate Manager, Director SSH Key Manager and Director Symmetric Key Manager.

Learn more at www.venafi.com/products.

---

Tables on Pages Following

Venafi Encryption Director is an encryption key and certificate management platform that simplifies the lifecycle management of encryption technologies across diverse operating systems and infrastructure environments. The Director product line consists of three products: Director Certificate Manager, Director SSH Key Manager and Director Symmetric Key Manager.

Learn more at www.venafi.com/products.

---

Figure 8 – Venafi™ Encryption Director™

---

Consideration 1

<table>
<thead>
<tr>
<th>New systems that can be encrypted due to automation</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of systems with encryption deployed after Venafi installation</td>
<td></td>
</tr>
<tr>
<td>Number of systems with encryption deployed prior to Venafi installation</td>
<td></td>
</tr>
</tbody>
</table>

Consideration 2

<table>
<thead>
<tr>
<th>Value of improved risk posture due to broader encryption coverage</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost of a breach that could be prevented by encryption:</td>
<td></td>
</tr>
<tr>
<td>- Brand erosion</td>
<td></td>
</tr>
<tr>
<td>- Fine</td>
<td></td>
</tr>
<tr>
<td>- Cost of reporting</td>
<td></td>
</tr>
<tr>
<td>- Lost/customer/transactions</td>
<td></td>
</tr>
<tr>
<td>- Lawsuit/litigation</td>
<td></td>
</tr>
<tr>
<td>- Lost/stolen personal information</td>
<td></td>
</tr>
<tr>
<td>- Employee</td>
<td></td>
</tr>
<tr>
<td>- Lost intellectual property/data</td>
<td></td>
</tr>
</tbody>
</table>

Cost of additional encryption technologies

---

ROI Formula

Use the following information to qualify the value of increased security as a result of reduced operational costs of deploying and managing encryption.

---

Figure 8 – Venafi™ Encryption Director™
Provisioning

- Automate all previously manual processes to guarantee timely, accurate management processes
- Eliminate unpositioned manual processes to guarantee timely, accurate management processes
- Demonstrate the breadth of encryption in use through inventory reports.

Discovery

- Identify all certificate (including self-signed and keys) so owners can be notified in time to complete maintenance prior to expiration.
- Escalate pending expiration notifications, if necessary, to ensure problems are addressed in a timely manner.
- Demonstrate the breadth of encryption in use through inventory reports.

Enrollment

- Streamline certificate renewal processes by providing users with a self-service interface to request certificates.
- Eliminate the use of spreadsheets and email reminders and spreadsheets, by automatically notifying certificate owners of pending expirations.
- Eliminate the need for spreadsheets and email reminders.

Discovery

- Use catalog of discovered certificates and certificate authorities to determine root certificate or vendor selection and to identify systems where root certificates must be self-signed or from a root-certified CA.
- Monitor intermediate root certificates to help admins avoid unexpected downtime.
- Automate all previously manual processes to demonstrate the breadth of encryption in use through inventory reports.

Enrollment

- Regularly solicit data from certificate authorities to improve understanding of certificate issuance and renewal processes.
- Monitor intermediate root certificates to help admins avoid unexpected downtime.
- Ensure the breadth and depth of encryption deployments and management processes.
**Discovery**

- **Provisioning**: Maintain a detailed record of all encryption keys and certificates and their locations. Identifying imminent expirations and rogue CAs and quickly remedying problems. Discover new encryption deployments early to ensure policies and requirements are followed. Expose infrastructure of acquired organizations to quickly assess state of encryption and prioritize maintenance work required.
- **Monitoring**: Monitor new encryption deployments in a highly-scalable manner. Manage more encryption at a lower cost by automating compliance and maintenance alerts and notifications. Free up funds for additional encryption deployments by replacing unnecessary high-cost certificates with lower-cost ones.
- **Enrollment**: Simplify certificate request and issuance process through self-service portals, making it more palatable to use certificates. Use centralized certificate request and renewal portal to scalably meet new business requirements for increased encryption deployments, whether with new CA(s) or existing.
- **Business Case**: Decreasing the operational costs of encryption lowers the TCO, making it possible to implement more encryption for less. NOTE: There are also a number of additional security features included in the product, including forensically-durable logging, HSM integration (optional), separation of duties, trust management, and other features.

**Monitoring**

- **Provisioning**: Demonstrate processes are in place to notify owners of certificates and keys whenever issues are detected or attention is required. Assign certificates and keys to specific owners so they can be reminded of scheduled maintenance. Generate reports by department, cost center, associated applications, regulatory requirement, etc. using metadata tags. Maintain forensically-durable log of discovery results and renewal alerts.
- **Enrollment**: Enforce standard workflow for certificate issuance and renewal process, consistent with internal policies and procedures. Maintain forensically durable log of CA task automation and self-service operations across all CA(s) in use. Demonstrate separation of duty (SoD) requirements.
- **Business Case**: Decreasing the operational costs of encryption lowers the TCO, making it possible to implement more encryption for less. NOTE: There are also a number of additional security features included in the product, including forensically-durable logging, HSM integration (optional), separation of duties, trust management, and other features.

**Enrollment**

- **Provisioning**: Avoid costly follow-up audits, fines, and lawsuits caused by failed audits, by regularly conducting self-compliance inspections. Remediate non-compliant systems by automatically applying compliant system configurations. Automatically inspect systems to ensure they are compliant with external regulations and internal policies. Maintain forensically-durable log of all encryption management operations. Demonstrate that the standard of due care has been met consistent with safe harbor requirements by illustrating the breadth and depth of encryption deployments and management processes.
- **Enrollment**: Enforce standard workflow for certificate issuance and renewal process, consistent with internal policies and procedures. Maintain forensically durable log of CA task automation and self-service operations across all CA(s) in use. Demonstrate separation of duty (SoD) requirements.
- **Business Case**: Decreasing the operational costs of encryption lowers the TCO, making it possible to implement more encryption for less. NOTE: There are also a number of additional security features included in the product, including forensically-durable logging, HSM integration (optional), separation of duties, trust management, and other features.