

Venafi™ Encryption Director™

Datacenter Editions

SIMPLIFY THE MANAGEMENT OF ENCRYPTION TECHNOLOGIES WHILE IMPROVING OPERATIONAL EFFICIENCY, DATA SECURITY AND COMPLIANCE ENFORCEMENT

WHAT IT DOES

Venafi Encryption Director simplifies the management of encryption technologies across diverse operating systems through:

- Continuous Discovery
- Monitoring & Alerts
- Lifecycle Management
- App. Configuration



WHY IT'S VALUABLE

Venafi applies a strategic approach to the tactical challenges of managing encryption, resulting in increased data security, improved operational efficiency and critical system uptime, and enhanced compliance and audit readiness.

In a growing and interconnected economy, the use of and dependence on electronic data has increased dramatically in recent years. Organizations of all sizes and industries maintain extensive financial, personally identifiable and mission-critical business data. When sensitive information is lost or compromised, organizations often pay a heavy price: recent high-profile security breaches and data losses have cost organizations millions in revenue and lost customer and investor confidence. These fears, along with new security policies and regulations, have driven IT professionals to deploy encryption more broadly.

Enterprise-wide Encryption Management And Venafi Encryption Director

As the mandate to encrypt widens and as encryption keys and certificates find greater prevalence and security significance, organizations need comprehensive, enterprise-wide key management systems—that address the needs of both InfoSec and IT Ops departments alike. Traditional approaches have proven limited, especially when keys and certificates are issued from a variety of certificate authorities and deployed across disparate systems and applications.

A much broader, systems management approach is required. Such an approach includes automating the creation and management of keys and certificates, configuring the applications that use them and providing comprehensive tools to monitor and report on the status of each component being managed. This broader, more holistic approach results in improved data security, critical system uptime, operational efficiency and audit readiness.

Venafi Encryption Director is an enterprise encryption management platform that helps organizations simplify the management of encryption keys and certificates across their diverse operating systems and infrastructure environments—from the desktop to the datacenter. Director performs four progressively more-valuable operations, including Discovery, Monitoring, Enrollment and Provisioning.

Discovery

The first step in managing encryption is to determine where keys and encryption certificates are deployed within the enterprise environment, and assess where imminent risks exist (such as which systems are using weak key strengths, which certificates and keys are about to expire, where rogue certificate authorities are in use, etc.). To utilize the discovery services in Venafi Encryption Director, administrators simply enter an IP address or range of IP addresses and define the relevant ports to inspect. The discovery engine systematically and non-invasively queries each host for certificates (including SSL, SSL-EV, TLS, SMTP and self-signed) from any CA, collects information about the certificates, and presents a status report to the administrator. Users can then easily identify



systems that are at risk or require attention and place those certificates under management. The discovery engine can be configured to regularly survey the infrastructure on a schedulable basis, and alert administrators whenever anything new is found.

Monitoring

Once keys are deployed across an enterprise, it is critical to track the health and operation of those keys and corresponding encryption systems. Venafi Encryption Director performs continuous monitoring and assessment of encryption certificates and technologies—including status and expiration dates—for all root, intermediate root, SSL, VPN, authentication, code signing and other types of certificates. Administrators are able to enter information about the applications and systems where certificates and keys are deployed for improved inventory and asset management. When a certificate nears its expiration or other issues are encountered, Director automatically sends notifications to the correct owner at user-defined intervals prior to expiration, and will automatically escalate if no action is taken. The contents of the notification messages are fully configurable, ensuring that certificate renewal instructions are provided consistent with organization-specific policies and procedures.

Policy-based monitoring is critical, for instance, when an automated maintenance process becomes delayed or fails. Active monitoring ensures business continuity and helps organizations move quickly and proactively to remedy problems before they result in service interruptions. The built-in reports in Director provide visibility into the status of managed encryption assets, allowing administrators to troubleshoot problems easily, perform

COMPLIANCE AND AUDIT

Configuration elements can be “locked,” “suggested” or left “open.” Enforce approved CAs, key strengths, and validity periods, while admins and auditors are notified when policies are modified or violated.

CA STRATEGIC SOURCING



Reduce costs through volume pricing or by replacing high-cost with lower-cost certificates to avoid vendor lock-in. Execute one-click CA migrations—either immediately or upon certificate expiration.

operational reviews, verify compliance with corporate policies and regulations, and quickly respond to audit requests.

Enrollment

When the time comes for a certificate to be renewed or for a key to be rotated, Venafi Encryption Director can manage the entire process from start to finish via the native workflow engine. Using its patented technology, Director can concurrently manage the enrollment of encryption certificates by multiple certificate authorities (CAs), and interface directly with all leading CAs, including VeriSign, Microsoft and others. Administrators now find it simple to migrate certificates from one CA to another, and the system allows for multiple approval steps throughout the process. This centralized and automated lifecycle management not only helps reduce administrative costs, but also reduces the errors common in manual work (that often requires nearly thirty steps per certificate renewal) and ensures compliance with corporate policies and regulations.

Provisioning

Venafi Encryption Director also provides full, end-to-end automation of encryption lifecycle management—from the CA all the way down to the target application or platform. Director automatically replaces expired certificates and out-of-date keys on the target platforms, replacing formerly manual processes including: key and CSR generation, CSR submission to CAs, approvals at the CA, issued certificate retrieval, certificate installation, operational validation, private key backup, and certificate renewal. Managed certificates and keys can be provisioned to one or more systems, supporting full, automated management of complex,

load-balanced environments. The policy-based management in Director enables granular control of all aspects of the provisioning process so that organizational policies can be enforced and tracked for compliance. In addition, administrators can define policies and parameters for each application, ensuring consistent and efficient operations on time every time.

BUSINESS CHALLENGES AND SOLUTIONS: VENAFI ENCRYPTION DIRECTOR

Venafi Encryption Director automates the process of installing, monitoring and renewing the encryption technologies necessary to protect sensitive data wherever it resides, while ensuring compliance reporting with internal policies and external regulations. By automating the full lifecycle management of encryption technologies, Director reduces costs and organizational complexity and typically demonstrates a return on investment within two years of deployment. Only Venafi Encryption Director enables organizations to reap the following benefits.

Policy Compliance and Audit Enforcement

Compliance with government, industry and organizational policies and regulations is consuming more and more of the security practitioners time, often at the expense of strategic business activities. In order to maintain compliance, management systems must allow administrators to set policies, enforce the application of those policies and audit ongoing operations in relation to those policies.

Venafi Encryption Director provides an

PROACTIVE INCIDENT PREVENTION

Notify the right people at the right time, with escalations based on configurable policies and rules via email or SNMP. Customizable message notifications per specific organizational needs.

DISASTER RECOVERY & BUSINESS CONTINUITY

Discover expired or soon-to-expire certificates on failover and DR sites.

Quickly migrate thousands of certificates or CAs and provision new certificates rapidly with one-click replacement functionality.

extensive hierarchical policy framework and allows every configuration element to be either “locked,” “suggested” or left “open.” This way, mandatory enterprise-wide encryption policies can be established, enforced and inherited down to individual systems. Divisional, departmental or group policies can also be set and locked in the same manner. Items such as approved CAs, key strengths, and validity periods are among the configuration elements Director can enforce and report on. Director also notifies administrators, managers, business owners and auditors whenever pre-defined policies are modified or violated.

CA Spend Management and Strategic Sourcing

Large organizations spend hundreds of thousands of dollars procuring encryption certificates each year. These costs can often be reduced by consolidating procurement to secure volume pricing from CA vendors, or by replacing high-cost certificates with lower-cost alternatives, where appropriate. Unfortunately, changing from one CA vendor to another typically involves cost-prohibitive migration processes. As a result, organizations feel trapped due to vendor lock-in.

Venafi Encryption Director makes it simple to discover and catalog all discoverable certificates and issuing CAs. Inventory reports provide the data necessary to determine the most cost-effective CA vendor mix. Organizations can execute one-click migrations from current CA(s) to any of the many popular CAs supported natively in Director—either immediately or upon certificate expiration. This allows for flexible strategic sourcing, enabling the business to make decisions based on the right technology and not simply on the basis of the least

expensive or disruptive implementation. Current Venafi customers have saved hundreds of thousands of dollars by leveraging the CA spend management and one-click migration capabilities in Director.

Proactive Incident Prevention

Most IT administrators live in an information-rich world and are often overburdened with daily responsibilities and longer-term projects. In this fast-paced role, if a single email or calendar appointment is ignored, overlooked or inadvertently sent to the wrong administrator, an encryption certificate may expire unexpectedly and cause costly system downtime and business interruption.

Venafi Encryption Director ensures the right people get the right alerts at the right time by pulling its certificate ownership data directly from an enterprise directory. This allows Director to escalate notifications intelligently up the management chain as appropriate—based on configurable policies and rules—ensuring the responsible parties always know the status of each encryption object. Notifications can be sent via email or SNMP, and can be written to a Flat File or MySQL, MSSQL or Oracle database. Director also sends notification messages that can be formatted and customized to meet the specific needs and requirements of the organization.

Disaster Recovery and Business Continuity

The work of encryption security experts has uncovered weaknesses in the RSA 1024 and DES algorithms, identified vulnerabilities in Debian Linux, and more recently, discovered an MD5 collision hack. In light of these

developments, responsible executives and managers must ask themselves: “What is our disaster recovery plan for digital certificates and keys?” and “How could we quickly migrate from one certificate type or CA to another if a new threat requires it?”

With Venafi Encryption Director administrators can manage complex certificate types and CA combinations. Should the need arise, Director can quickly migrate thousands of certificates or CAs, and do so without an army of administrators. Director also provides the native ability to discover expired or soon-to-expire certificates that reside on failover and DR sites, and allows IT operations administrators to provision replacement certificates rapidly. Administrators, managers and business units can operate with greater confidence with the recovery and one-click certificate replacement functionality in Director.

Reduced Administrative Workload

With an ever-shrinking pool of human resources and the drive for increased scale and data proliferation, today’s IT administrators are expected to do more with less. IT automation is the answer. Administrators cannot afford to spend between four and eight hours, the industry average, to roll over and renew individual keys and certificates manually, often struggling to remember correct processes or navigate multiple approvals in the process. Such an approach can quickly overwhelm and monopolize precious, though limited, resources.

Venafi Encryption Director automates the entire process of provisioning and renewing digital certificates according to an organization’s pre-defined processes and policies. Turning a five-hour project into a five-minute task allows organizations to reallocate valuable, full-time employees to more strategic, priority initiatives—as well as decrease errors caused by manual tasks. By replacing manual operations with automated processing, Director also provides better visibility into the stability of data security provided by encryption keys and certificates through real-time status monitoring, proactive notifications and alerts, and detailed reports.

REDUCED ADMIN WORKLOAD

Automate provisioning and renewal processes according to pre-defined policies. Truncate lifecycle management steps and reallocate valuable employees to more strategic, priority initiatives.

CONCLUSION

At a time when most IT organizations are looking for ways to better secure critical data and 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. The increased use of and dependence on encryption within organizations for improved data security has created more and more manual processes that, in most cases, are inefficient. By deploying automated encryption lifecycle processes, organizations achieve more with less, and free up resources to focus on projects that will help them grow their businesses.

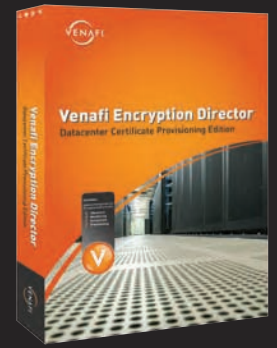
Venafi invented the industry's first automation platform allowing organizations to more effectively implement and maintain encryption throughout their varied and disparate environments. Venafi Encryption Director represents the next-generation

Systems Management for Encryption platform. As such, Director automatically deploys keys and certificates, manages the full lifecycle of these assets—from request, to renewal and revocation—and configures applications to use them according to administrator-defined policies.

The Venafi Encryption Director product line consists of three products: the Monitoring Edition, the Enrollment Edition and the Provisioning Edition, and each includes licenses for the Discovery Engine. The table below provides a feature overview by product edition. Director product feature sets are additive. Learn more about Venafi Encryption Director at www.venafi.com/Director today.

WHICH EDITION IS RIGHT FOR YOU?

	Monitoring Edition	Enrollment Edition	Provisioning Edition
Network Discovery	✓	✓	✓
Reporting	✓	✓	✓
Logging	✓	✓	✓
Notifications	✓	✓	✓
Escalations	✓	✓	✓
Policy-Based Management	✓	✓	✓
Root Monitoring	✓	✓	✓
Self Service	✓	✓	✓
Network Validation		✓	✓
Certificate Authority Enrollment Workflow		✓	✓
Automated Key Generation			✓
Platform Lifecycle Automation			✓
Application Configuration			✓
Distributed Key Generation			✓
Base Application Modules			✓
Onboard Validation			✓



SUPPORTED SYSTEMS

Web Servers:

- IBM® HTTP Server
- IIS
- Apache

Application Servers:

- IBM® WebSphere Application Server

Middleware:

- IBM® WebSphere MQ™-Server
- IBM® WebSphere MQ™-Client
- IONA Artix

SSL Accelerators:

- F5® Big-IP®
- F5 Local Traffic Manager

Other:

- IBM Tivoli® Access Manager
- PKCS (#7, #10, #12)
- PEM
- IBM Global Secure Kit (GSK)

* Platforms and versions subject to change without notice. Contact a Venafi Sales Representative for a current list of supported platforms



Contact **Venafi** at:

Worldwide: +1 801-676-6900
 EMEA: +44 (0)20 3178 3912
info@venafi.com

www.venafi.com