

인증서 관리 솔루션

Certificate Lifecycle Management

April 2026

네트워크상에 존재하는 두 가지 행위자



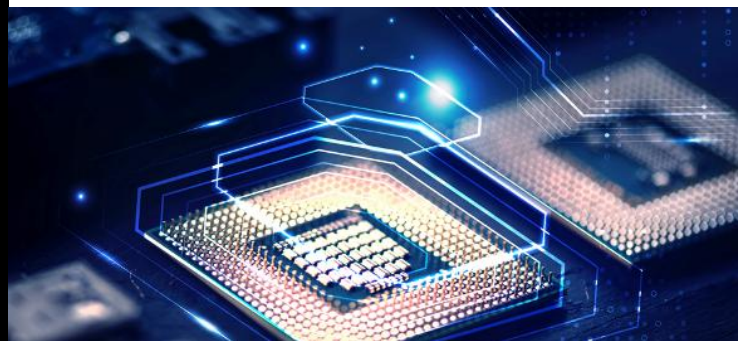
PEOPLE

Username and Passwords



MACHINES

Machine Identities

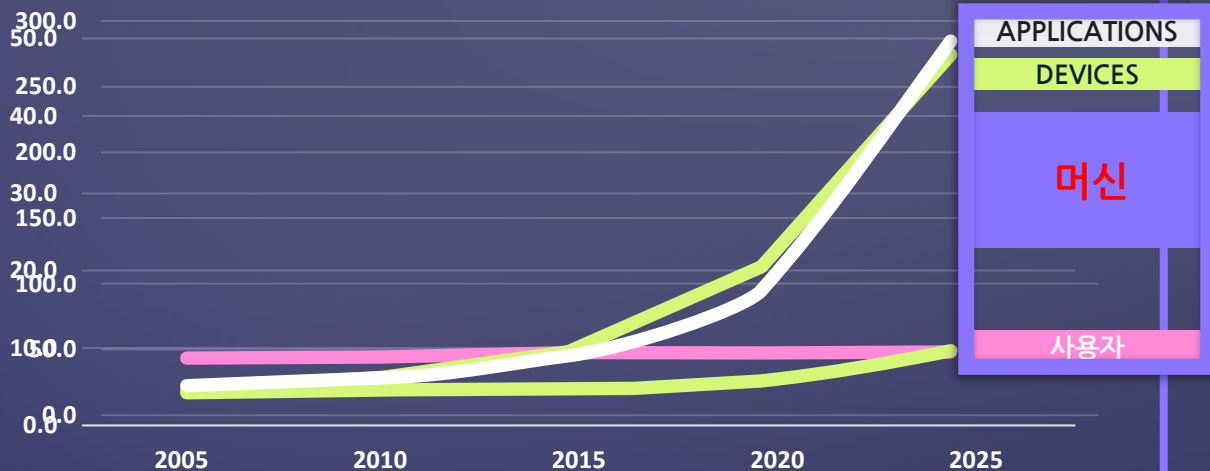


Secure and protect identities

사용자 보다 많은 머신 수

사용자

PROJECTED GROWTH (IN BILLIONS)



Growth Factors

- 클라우드
- 가상 머신
- 컨테이너
- DevOps
- 모바일 디바이스
- IOT
- 산업 기기
- 데이터 액세스

더 많은 머신 = 더 많은 아이덴티티

머신 아이덴티티 유형 및 현황

SSL/TLS 인증서

SSH 키 및 인증서

모바일 인증서

쿠버네티스 인증서

코드 사인닝

IoT 인증서

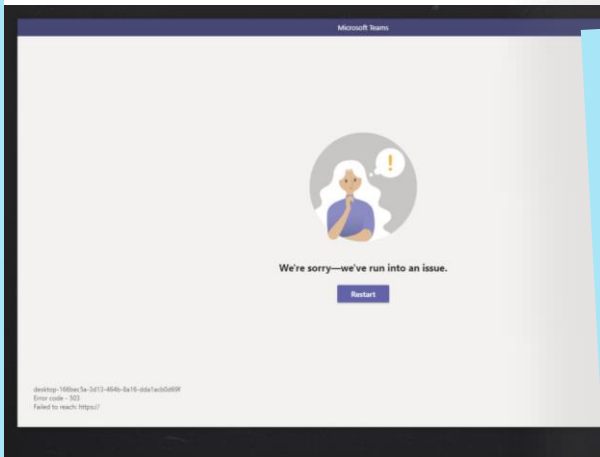
JSON 토큰

SPIFFE

TLS 기반 서비스 중단 상황은 자주 발생

Microsoft Teams goes down after Microsoft forgot to renew a certificate

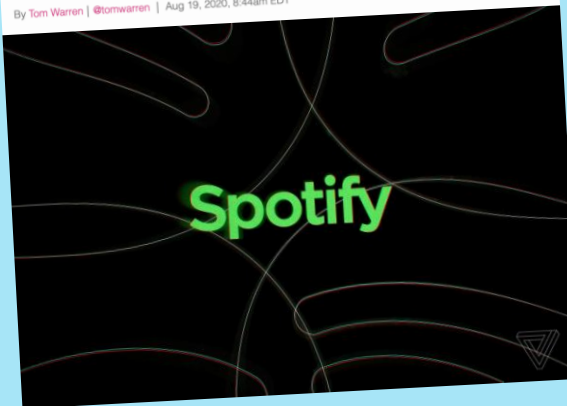
Oops



Spotify went down for an hour after a certificate expired

The music streaming service is experiencing some issues today

By Tom Warren | @tomwarren | Aug 19, 2020, 8:44am EDT



Google Voice Outage: Expired TLS Certificate Brings Down Yet Another Giant

Posted on March 3, 2021 by Nishevitha Ramamoorthy

Between February 15th and February 16th, 2021, Google Voice, Google's telephone service over Internet (VoIP) calls for over four hours. On February 28th, 2021, Google released an incident report stating the cause of the outage – **an expired TLS**



서비스 중단은 엄청난 비용을 발생 시킴

인증서 만료 사고, 왜 반복 될까? - 인증서 & PKI 관리 이슈



만료된 인증서

- 가장 흔한 사고 원인
- 인증서 갱신 누락 시 서비스 중단, 장애 발생



인증서 자산 가시성 부족

- 조직 내에 배포된 인증서 위치, 사용처, 만료일 등을 정확히 파악하지 못함
- Shadow Certificate 문제 발생



수동 관리

- 엑셀이나 이메일, 업체 전화로 인증서 관리를 진행
- 실수, 중복, 갱신, 폐기 등 운영상 누락이 빈번하게 발생



과도한 인증 기관(CA) 분산

- DevOps, 멀티 클라우드, 컨테이너 환경에서 인증서 발급/폐기 빈도가 폭증
- 자동화 되지 않아 통제 불능 상태 쉽게 빠짐

CA, 브라우저가 바꾸는 보안 게임의 법칙

인증서 유효 기간 감소

RSAConference™

Where the World
Talks Security™

HOME > LIBRARY

Google's 90-Day Digital Certificate Proposal: Better Security, More Work

Posted on September 26, 2023 by Murali Palanisamy

It appears that the validity period for Transport Layer Security (TLS) certificates, also known as Secure Sockets Layer (SSL) certificates, is once again going to shrink – at least if Google has its way. The internet giant has proposed only 90 days, down from the current 398 days.

Google has the option of effecting this change via a CA/Browser Forum ballot proposal. But if that fails

<https://www.rsaconference.com/library/blog/googles-90-day-digital-certificate-proposal>

CA / Browser Forum



CA/BROWSER FORUM

Home

About

Server Cert
WG

Code Signing Cert
WG

NetSec
WG

S/MIME Cert
WG

Definitions
WG

Proceedings

Resources

WELCOME TO THE CA/BROWSER FORUM

The Certification Authority Browser Forum (CA/Browser Forum) is a voluntary gathering of Certificate Issuers and suppliers of Internet browser software and other applications that use certificates (Certificate Consumers).

More information for about the forum and information for [Site Owners](#), [Developers](#), [Auditors and Assessors](#), and [Potential Members](#) can be found in the [About](#) section of this website.

Recent posts

[Ballot SMC011 - Add EUID as Registration Reference](#)

March 31, 2025 by [Stephen Davidson](#) [Ballot](#) [S/MIME](#)

IPR Review of Ballot SMC011: Add EUID as Registration Reference This Review Notice is sent pursuant to Section 4.1 of the CA/Browser Forum's Intellectual Property Rights Policy (v1.3). This 30-

Type her

Search

LATEST RELEASES

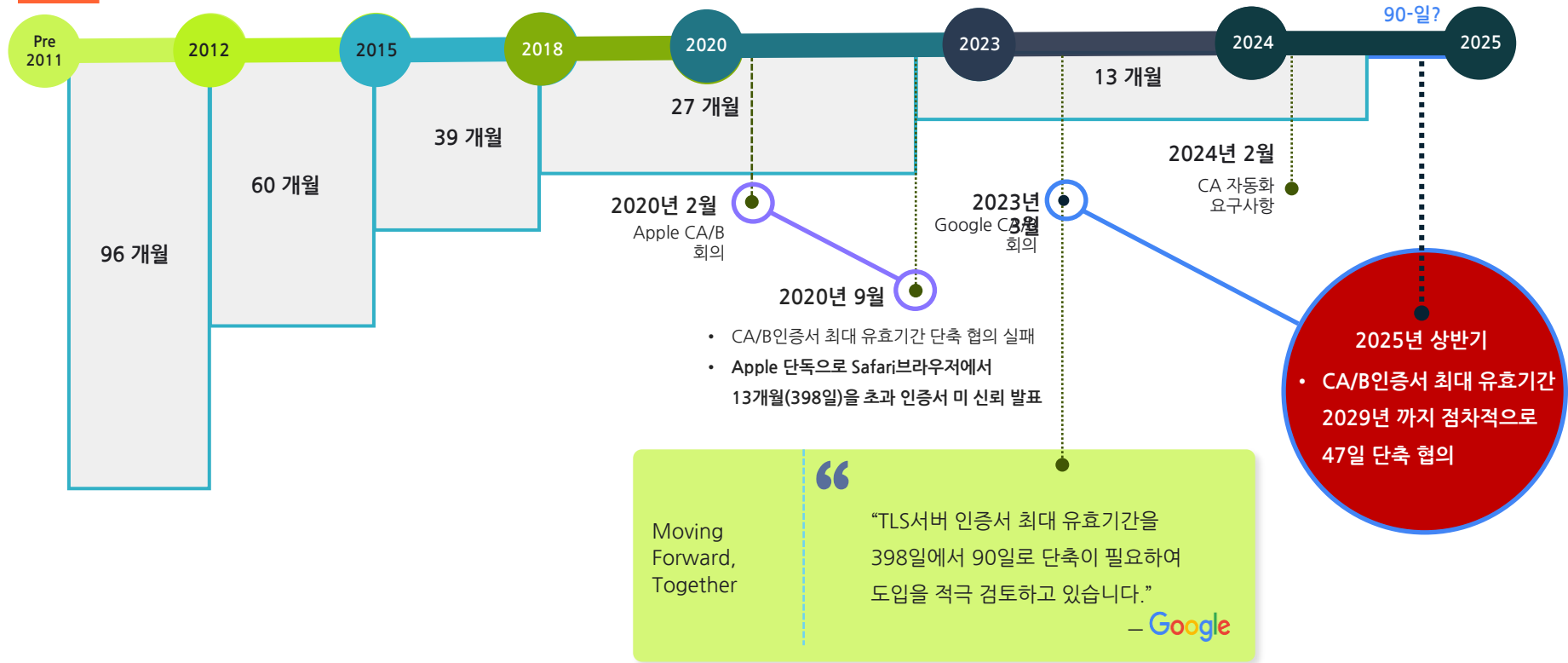
Server Certificate Requirements

[SC-084: DNS Labeled With ACME Account ID Challenge \(#566\)](#) - Mar 13, 2025
BRs release version 2.1.4

Code Signing

<https://cabforum.org/>

Google & Apple 주도로 바뀌는 인증서 정책 대응



Google & Apple 주도로 바뀌는 인증서 정책 대응

Industry to Shift to 47-Day SSL/TLS Certificate Validity by 2029

Starting in 2026, SSL/TLS certificate lifespans will be reduced from the current maximum of 13 months. By 2029, all public SSL/TLS certificates will have a 1.5-month maximum validity. Here's what you need to know.

On April 11, 2025, the CA/Browser Forum (CA/B Forum) approved **Ballot SC-081v3**, a proposal from Apple that aims to dramatically reshape how organizations manage digital certificates and keys by reducing the lifespans of certificates and validation-related data.

But this update to the SSL/TLS Baseline Requirements isn't just another technical change — it's a fundamental shift that will require organizations to rethink their certificate management approach and strategies.

Here's what you need to know about the coming changes to SSL/TLS certificate validity and data reuse periods and how they'll affect your organization.

Let's hash it out.

💡 Download: [Certificate Lifecycle Management 15 Best Practices Guide \(Free PDF\)](#).

TL;DR: A Breakdown of the Changes to Come Starting in March 2026

- The industry is moving toward shorter SSL certificate lifespans (i.e., 47 days). The goal of the ballot's phased reduction is to make the proposed changes "reasonable and attainable."
- Google originally proposed 90-day validity. Apple said, "hold my beer" and proposed half the lifespan (45 days), but the negotiated validity period ultimately settled on 47 days. (Check out the [FAQs](#) at the end of the article to learn more about the changes in certificate validity periods over the years.)
- The certificate lifespan
 - ~6 months (starting March 2026)
 - ~3 months (starting March 2027)
 - 1.5 months (starting March 2029)

주요 외신 기사

<https://www.thesslstore.com/blog/47-day-ssl-certificate-validity-by-2029/>

📅 2026년 3월 15일

- 최대 TLS 인증서 유효기간: 200일
- 약 6개월 주기로 갱신 필요
- 도메인 소유 검증(DCV) 재사용 기간: 200일

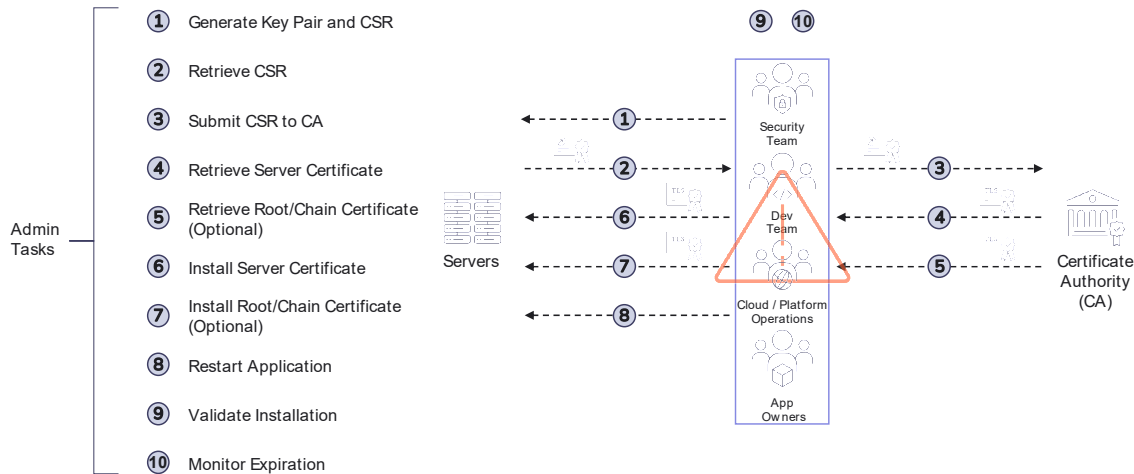
📅 2027년 3월 15일

- 최대 TLS 인증서 유효기간: 100일
- 약 3개월 주기로 갱신 필요
- DCV 재사용 기간: 100일

📅 2029년 3월 15일

- 최대 TLS 인증서 유효기간: 47일
- 약 1개월 주기로 갱신 필요
- DCV 재사용 기간: 10일

인증서 수동 요청 프로세스



복잡하며, 높은 휴먼 에러 발생 확률



인증서 유효기간 47일 시대 준비과정

Fast-track your enterprise to **47-Day Ready**.

현황 파악

- 범위와 비즈니스에 미치는 영향 평가

설계

- 빠른 도입과 성공을 위해 맞춤형 시스템 검토

솔루션 도입

- 47일 TLS표준을 신속하게 구현하기 위해 핵심 자동화 전문 서비스 연동
- 사람, 프로세스, 기술의 조정을 요구하는 47일 TLS 시대 대응

시스템 구성 요소



사람 & 프로세스

- 준비 상태 평가
- 기업 영향도 평가
- 구현 가이드
- 기업 로드맵



기술

- 인증서 탐지
- 핵심 워크플로우
- 핵심 자동화



준비 상태 점검

- **전문가에 의한 90(47)일**
준비상태 점검 및 컨설팅

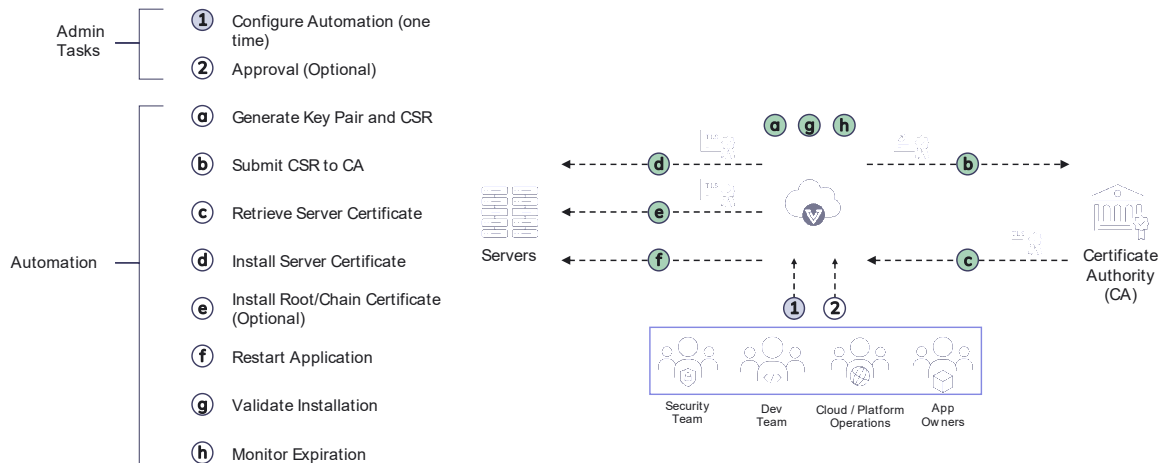
조직적 준비

기술적 준비

준비 완료



자동화 완료 & 준비 완료



<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-16.pdf>

NIST 1800-16



“자동화는 인증서의 등록, 설치, 모니터링, 교체가 가능한 모든 곳에서 사용되어야 한다...”

NIST 1800-16 “Venafi TLS서버 인증서의 보안 및 운영 리스크를 해결할 수 있도록 지원한다”

인증서 서비스 팀

인증서 관리를 자동화할 수 있도록 리소스 소유자를 지원하는 중앙 시스템을 제공

리소스 소유자

본인 소유의 인증서 관리 자동화

"인증서 수명 주기 관리(Certificate Lifecycle Management)

솔루션은 조직이 **디지털 인증서를 탐지, 발급, 갱신, 폐기, 감사 등**
전체 수명 주기에 걸쳐 **자동화**되고 정책 기반으로 관리할 수 있도록
지원합니다.”

— *Gartner Market Guide for CLM, 2023*

Certificate Lifecycle Management 7대 핵심



중앙 집중 식 거버넌스 및 분산 발급

- 중앙에서 정책 및 통제를 운영
- 다양한 부서나 팀이 인증서 발급할 수 있도록 지원



인증서 탐지

- 모든 인증서를 자동 탐지
- 위치, 만료일, 소유자 등 메타데이터 수집



리포트 및 경고

- 인증서 상태 실시간 리포트
- 만료 임박, 비정상 발급 등 이벤트 경고



승인 워크플로우

- 인증서 발급, 갱신, 폐기에 대한 승인 절차 정의
- 무단 변경 방지

Certificate Lifecycle Management 7대 핵심



자동화

- ACME, SCEP, EST등의 표준 프로토콜 뿐만 아니라 다양한 API를 통해 인증서 수명주기 자동화



위임된 관리 및 셀프서비스

- 그룹별 인증서 관리 권한 위임
- 셀프서비스 포털 제공



정의된 프로세스

- 인증서 관리에 대한 정책, 절차, 역할을 명확히 정의

사이버아크 머신 아이덴티티 솔루션



Venafi
TLS Protect



Venafi
TLS Protect for Kubernetes



Venafi
Firefly



Venafi
SSH Protect



Venafi
CodeSign Protect



Venafi
Zero Touch PKI



탐지



인텔리전스



정책



자동화



머신 아이덴티티 보안

멀티 클라우드

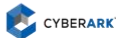
하이브리드

IDC



amazon
WEB SERVICES™

kubernetes



servicenow



HashiCorp



Azure



citrix



ORACLE



Google Cloud



Venafi
Ecosystem

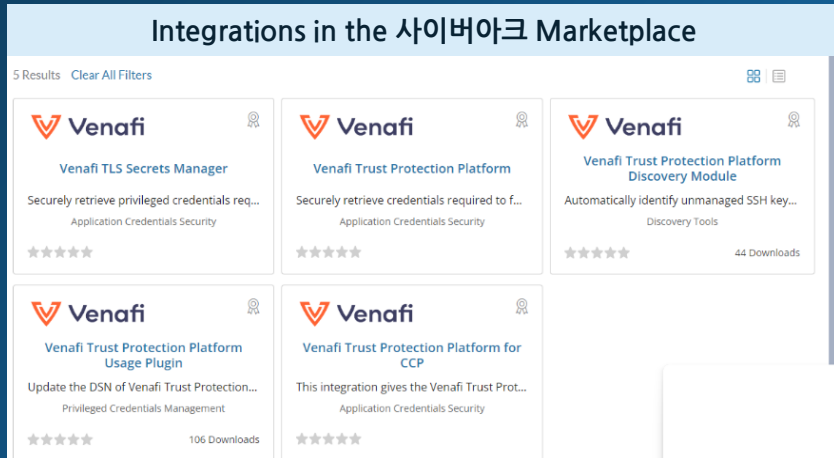
사이버아크 CLM

1. 인증서 탐지, 갱신 및 보안자동화

2. SaaS 및 구축형 솔루션

3. 사람, 머신 아이덴티티 볼트 통합
(비밀번호 로테이션 통합)

✓ CLM, PAM, Secret
Manager



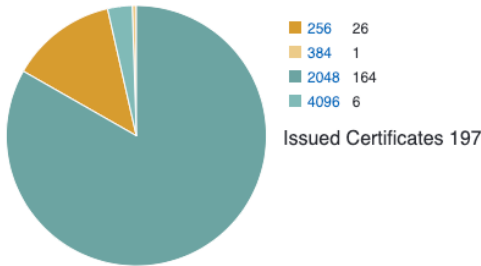
All Certificates Dashboard

Add Widget ▾

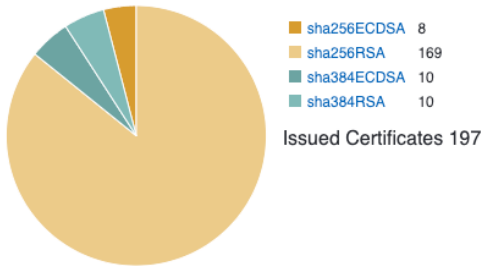
Certificate Totals +

My Certificates	Expiring within 30 days	In Error	Key Size < 2048 RSA keys	Weak Signing Algorithm	Validity Period > 397 days	Unapproved Issuer	Pending My Approval	Distrusted Entrust
197	31	2	0	0	2	189	0	0

Key Size

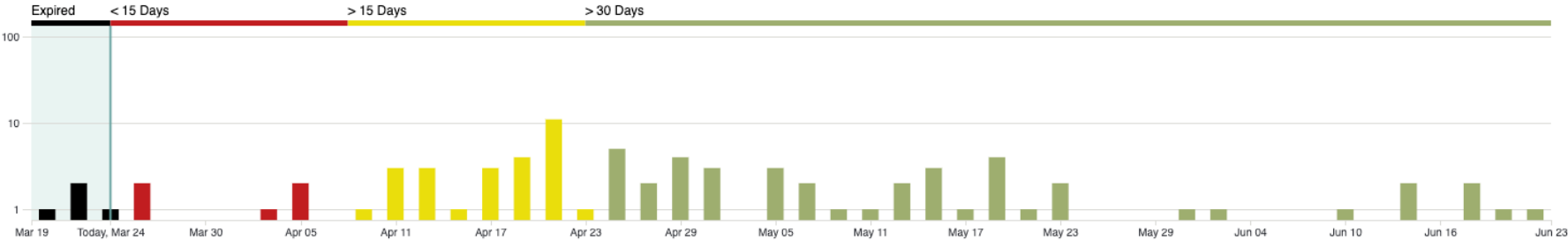


Signing Algorithm



Expiration

3/19/2025 - 6/23/2025



Certificates

Create a New Certificate

☐	a248.e.akamai.net	4	4	4/20/2025	2048	Expiring Soon	No Owner Assigned, Unapproved Issuer, Validation Disabled	Download	
☐	a2hosting.com	2	2	4/17/2025	2048	Management Type Unassigned	No Owner Assigned, Unapproved Issuer, Validation Disabled		
☐	abc.net.au	2	2	11/26/2025	256		No Owner Assigned, Unapproved Issuer, Validation Disabled		
☐	accessify.com	1	1	3/27/2025	2048	Expired - Short Term	No Owner Assigned, Unapproved Issuer, Validation Disabled		
☐	accounts.google.com	2	2	4/21/2025	2048	Management Type Unassigned	No Owner Assigned, Unapproved Issuer, Validation Disabled	Import	
☐	acervo.extra.globo.com	1	1	4/25/2025	2048	Expiring Soon	No Owner Assigned, Unapproved Issuer, Validation Disabled	Download	
☐	acnpic.accenture.com	1	1	10/22/2025	2048		No Owner Assigned, Unapproved Issuer, Validation Disabled	Download	
☐	adage.com	1	1	4/29/2025	256	Management Type Unassigned	No Owner Assigned, Unapproved Issuer, Validation Disabled	Import	
☐	adam.law.harvard.edu	1	1	5/11/2025	2048	Expiring Soon	No Owner Assigned, Unapproved Issuer, Validation Disabled	Download	
☐	ad-server.soo.com	0	0	2/8/2026	2048		No Owner Assigned, Validation Disabled	Download	
☐	affiliate-program.amazon.com	2	2	10/18/2025	2048	Management Type Unassigned	No Owner Assigned, Unapproved Issuer, Validation Disabled	Import	
☐	airtable.com	8	8	2/14/2026	2048	Management Type Unassigned	No Owner Assigned, Unapproved Issuer, Validation Disabled	Import	
☐	alexandergerst.esa.int	1	1	12/25/2025	2048		No Owner Assigned, Unapproved Issuer, Validation Disabled	Download	
☐	all.content.cirrus.bloomberg.com	2	2	7/14/2025	2048		No Owner Assigned, Unapproved Issuer, Validation Disabled	Download	

Download

Renewal Details

Import

Add Installation

Retire

Revoke

Check Revocation

Delete

CLM도입 효과와 운영 전략# 도입 단계



인증서 탐지



인증서 모니터링



인증서 발급



인증서 배포

CLM 성숙도 단계 – 인증서 배포 자동화

CLM도입 효과와 운영 전략# 인증서 탐지 & 모니터링

네트워크 및 디바이스 분석을 통해 사용중인 인증서 탐지



Onboard Discovery: 특정 네트워크 애플리케이션에서 사용 중인 인증서를 탐지



CA Import: CA연동을 통해 인증서 탐지



네트워크 탐지: 네트워크 포트 분석을 통한 인증서 탐지

CLM도입 효과와 운영 전략# 인증서 발급 (생성)

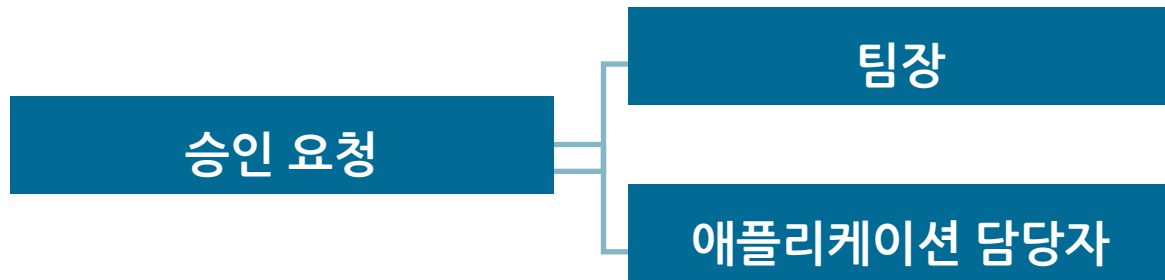
- 개인 키와 CSR은 CLM에 의해 생성
- CSR을 직접 업로드, CLM는 키 길이, 알고리즘 등 보안 정책에 준수하였는지 확인

Create a New Certificate

Folder	Certificate Signing Request	Additional Information
CSR Generation Generate a CSR for me		
Common Name ⓘ		
Organization		
Organizational Units Organizational Units		

CLM도입 효과와 운영 전략# 인증서 발급 (생성, 삭제 승인)

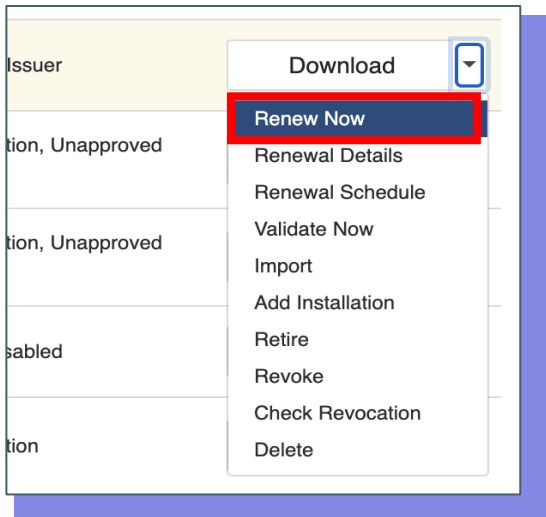
인증서 생성 처리 과정에 추가되는 승인 단계



Requesting - Pending Someone Else's Approval
This certificate is waiting for an external approval.

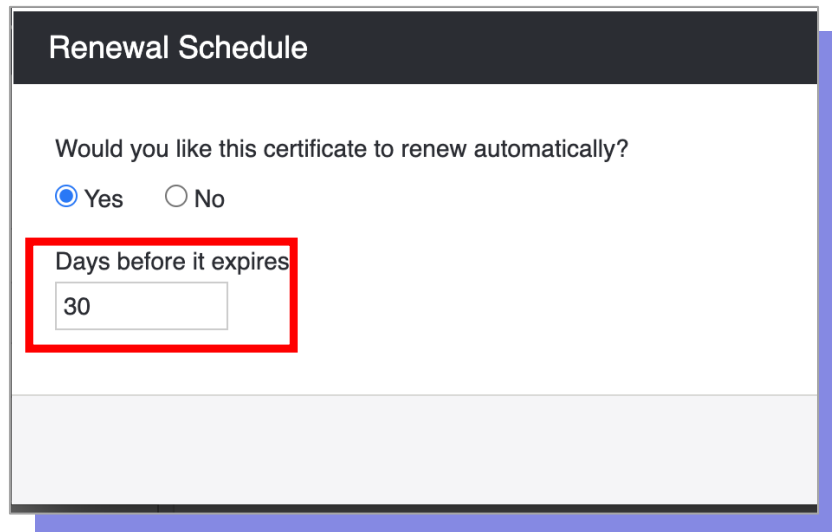
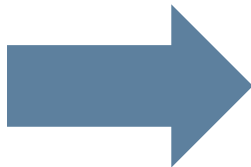
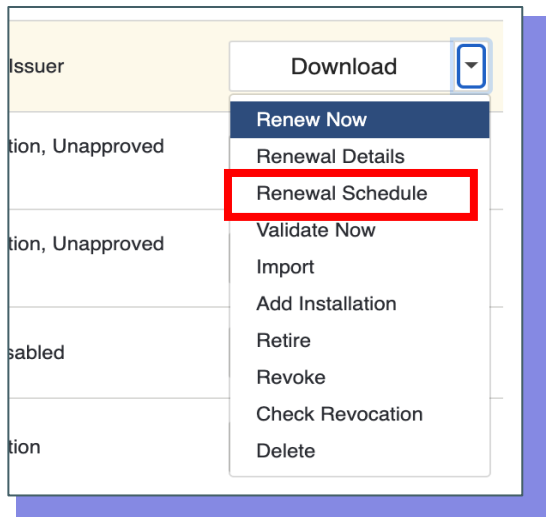
CLM도입 효과와 운영 전략# 인증서 발급 (갱신)

인증서 생성부터 폐기까지 완전 자동화



- 기업 인증서 보안 정책의 적용 지원

CLM도입 효과와 운영 전략# 인증서 발급 (갱신 자동화)



CLM도입 효과와 운영 전략# 인증서 배포

The screenshot displays a certificate management dashboard. On the left, there are filter sections: 'Quick Filters' and 'Common Filters'. The 'Common Filters' section includes a 'Status' filter set to 'Managed', a 'Risks' filter, and a 'Certificate Name' filter. The main area shows a table of certificates with columns: Nickname, Installations, Valid To, Key Size, Status, and Risks. Two certificates are listed: 'labs.venafi.com' and 'validate.lab.venafi.com'. The 'labs.venafi.com' certificate is highlighted in yellow. A context menu is open for this certificate, showing options: Download, Renew Now, Renewal Details, Renewal Schedule, Import, Add Installation (highlighted with a red box), and Retire. A blue box with the text '인증서 적용' (Certificate Application) is overlaid on the bottom right of the interface.

Nickname ▲	Installations	Valid To ▼	Key Size ▼	Status	Risks
labs.venafi.com	0	4/13/2019	2048		Validation Disabled
validate.lab.venafi.com	0	3/29/2018	2048	Pending Someone Else's Approval ⓘ	Failed Validation

2 Certificates | [Edit Columns](#)

Quick Filters >

Common Filters ▼

Status

Managed x

Risks

Certificate Name ⓘ

Move to ...

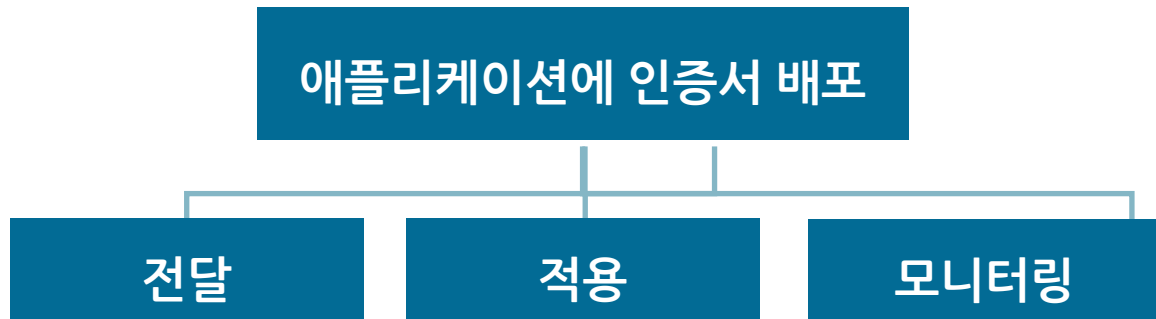
Download ▼

- Renew Now
- Renewal Details
- Renewal Schedule
- Import
- Add Installation
- Retire

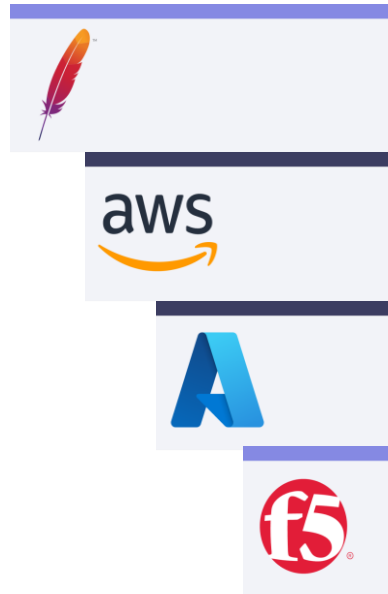
인증서 적용

CLM도입 효과와 운영 전략# 인증서 배포

TLS인증서 관리



- 상용 애플리케이션 드라이버 및 완전 자동화 지원
- 스크립트 이용 추가 드라이버 작성



CLM도입 효과와 운영 전략# 인증서 배포 (폐기)

The screenshot displays the Venafi console interface for a server certificate. The left sidebar contains navigation links: Overview, Installations, SSL/TLS, and Previous Versions. The main area shows the 'Server Certificate Template' details for the domain *.happyfuncorp.com. A table lists the certificate's attributes, including Issuer (traininglab-Root-CA), Common Name (*.happyfuncorp.com), Organization (Venafi, Inc.), and Organizational Unit (EssentialSSL Wildcard, Domain Control Validated). The 'Previous Versions' button is highlighted with a blue callout box stating: 'Previous Versions (이전) 버튼을 통해 모든 버전의 인증서 폐기 여부 확인'. The 'Actions' menu is open, showing options like Download, Renew Now, Renewal Details, Renewal Schedule, Retire, and Revoke. The 'Revoke' button is highlighted with a red border and a blue callout box stating: 'Revoke(폐기) 버튼 클릭'. At the bottom, a 'VALIDATION' section shows a warning icon and the text: 'SSL/TLS: No validation results' and 'Installations: No validation results'.

*.happyfuncorp.com
Policy\10\Internal\Infrastructure\Load Balancers\

Overview
Installations
SSL/TLS
Previous Versions

Server Certificate Template

Issuer	Common Name	Organization	Organizational Unit	City/Locality	State/Province	Country
traininglab-Root-CA	*.happyfuncorp.com	Venafi, Inc.	EssentialSSL Wildcard, Domain Control Validated			

Key Usage
Digital Signature, Key Encipherment (c0)

Enhanced Key Usage
Server Authentication (1.3.6.1.5.5.7.3.1)

Actions

- Download
- Renew Now
- Renewal Details
- Renewal Schedule
- Retire
- Revoke

Previous Versions (이전) 버튼을 통해 모든 버전의 인증서 폐기 여부 확인

Revoke(폐기) 버튼 클릭

VALIDATION ⓘ

SSL/TLS: No validation results
Installations: No validation results

CLM도입 효과와 운영 전략# 리포트 및 경고

Action Required: Certificate Expiring Contact

The certificate for [DemoCert2.tpp.local](#) is going to expire in 33 days.
This certificate must be renewed and installed before it expires.

[See a list of available actions and get additional information.](#)

If you need assistance, contact your Administrator.

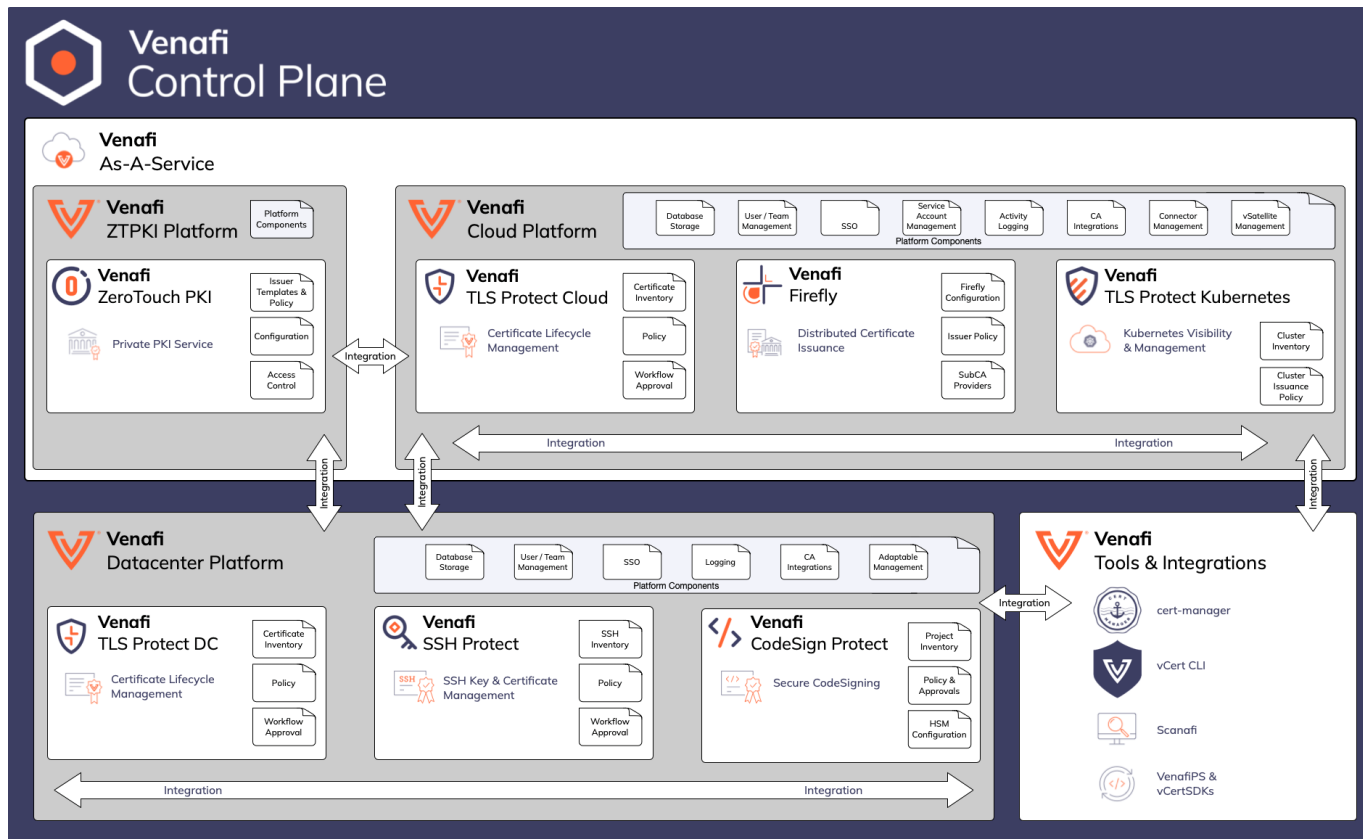
This email is being sent to you by Venafi Trust Protection Platform because you are named as a contact on this notification.

일일 작업 실행 시 이메일로
알림 표시

인증서가 곧 예정을 알리는 알림

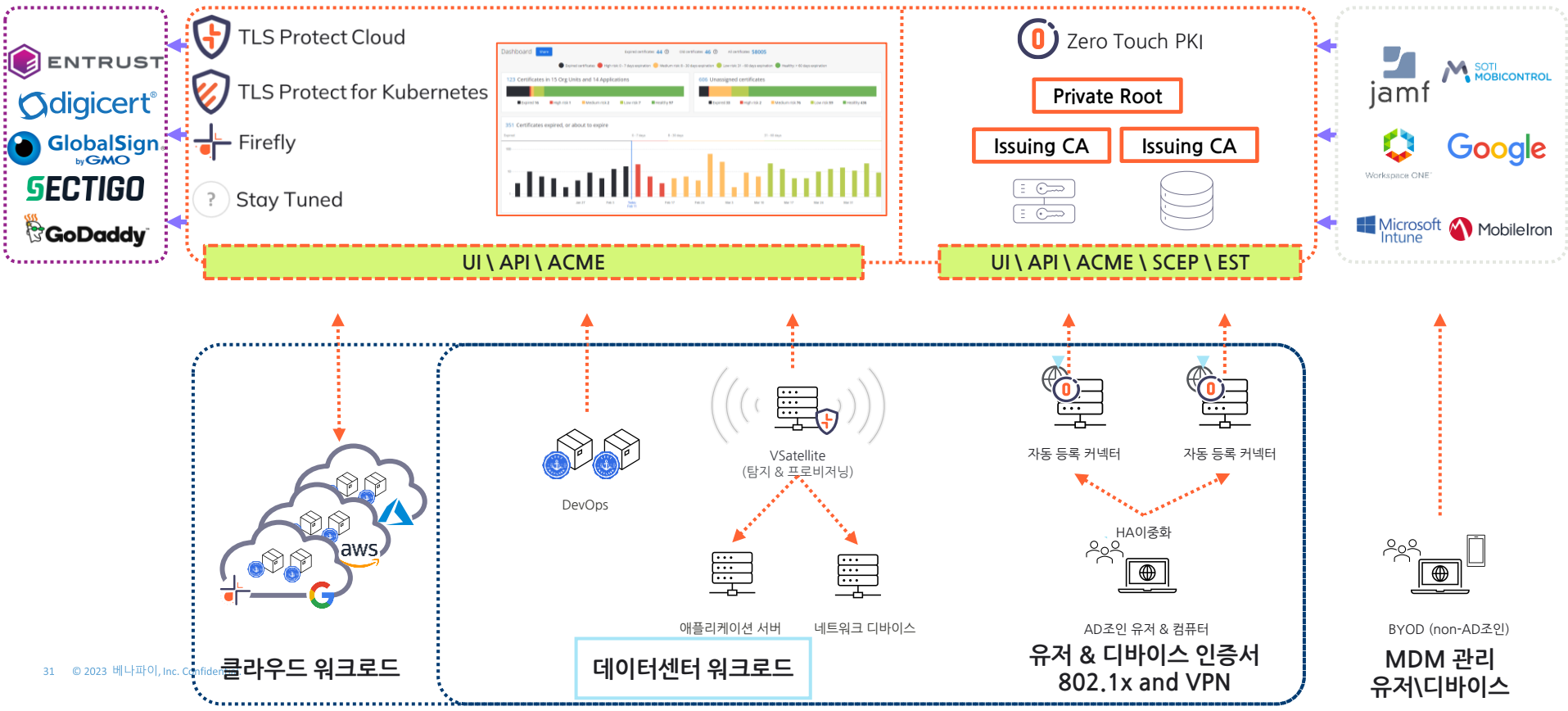
관리자에게 전송

On-prem 구성



SaaS 구성

Venafi Control Plane



사람, 머신 아이덴티티 통합

통합 운영, 보안 정책,
분석 통합



CYBERARK®
The Identity Security Company™

아이덴티티 보안분야
글로벌 리더



Venafi
A CyberArk Company

현대적이고 신뢰할 수 있는
머신 아이덴티티 관리

다양한 산업군의 도입 배경과 기대효과

“사이버아크 솔루션을 통해 시스템 강화 및 **인증서 설치를 즉시 자동화**할 수 있습니다. 자동화를 통해 인증서 수명 주기 및 설치에 대한 노력을 줄입니다.

Michael Flanders,
Senior Cybersecurity Engineer,
Southwest Airlines

Southwest[®]

[Southwest](#)

“사이버아크 없이 인증서 관리를 전혀 할 수 없었습니다. 솔루션 도입이후 가장 큰 효과를 본 것은 인증서를 **관리하는 리소스를 대폭 낮추고** 다른 업무에 집중 할 수 있게 된 것 입니다.”

Alan Morton
Technical Lead for Certificate
Services, BP



“사이버아크는 인증서 미 갱신, 만료로 인해 **서비스가 중단**되지 않을 것 이라는 확신을 제공합니다. 덕분에 우리팀은 환경 보안에 집중할 수 있었습니다. 의심 여지없이 사이버아크 솔루션을 추천합니다.

Scott Barronton
CISO, Diebold Nixdorf



[Diebold Nixdorf](#)

SSH 키 관리 시스템

많은 조직에서 **인지하지 못하는 SSH 키 쌍, 통제되지 않은 SSH 키 설정, SSH 정책 시행의 어려움**, 그리고 **무단 접근의 위험성이 증가**합니다.

SSH 키를 수동으로 관리할 경우, 조직은 보안 침해를 방지하는 데 필요한 가시성 및 인텔리전스가 결여 됩니다. 결과적으로, **SSH 키는 보안 부담이 되어 조직이 감사에 취약**해지고, 악의적인 공격자가 취약한 보안 관행을 이용하여 **중요한 시스템에 무단으로 접근할 수 있는 위험에 노출**되게 됩니다

SSH Protect 주요 기능



가시성

- SSH 키 탐지 및 정확한 인벤토리를 생성하고, 모니터링 제공.
- 에이전트 기반 및 에이전트 없는 스캐닝 도구 사용.
- 키 및 메타데이터를 폴더로 조직.
- AD와 연동



자동화

- SSH 키 정책을 수립 및 적용하며 모니터링과 키 로테이션 제공
- 정책 위반에 대한 맞춤형 수정 작업 자동화.
- 키가 언제 사용되었고, 누가 사용했는지 기록
- SIEM 등과 통합
- 셀프 서비스 UI를 통해 모든 장치에서 프로비저닝 자동화

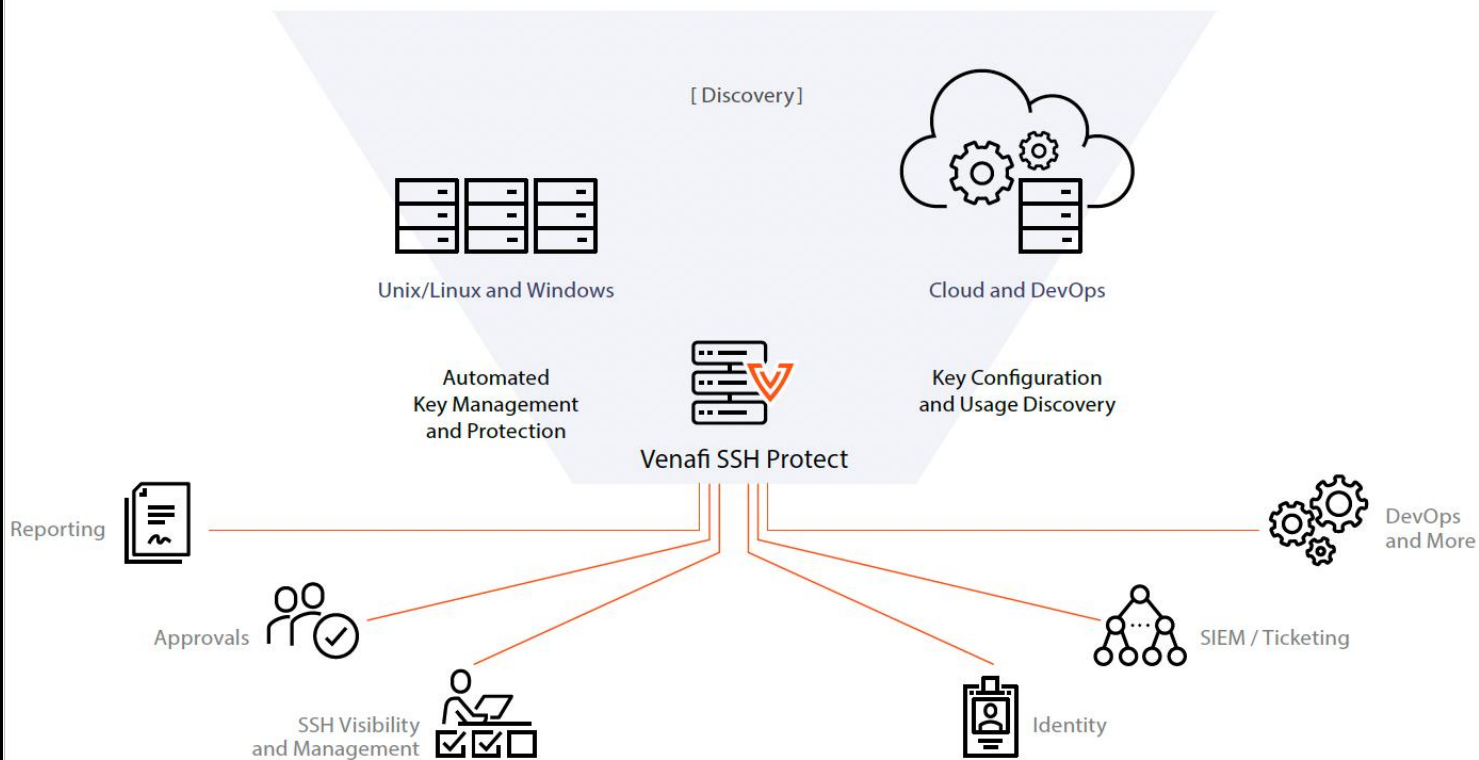


인텔리전스

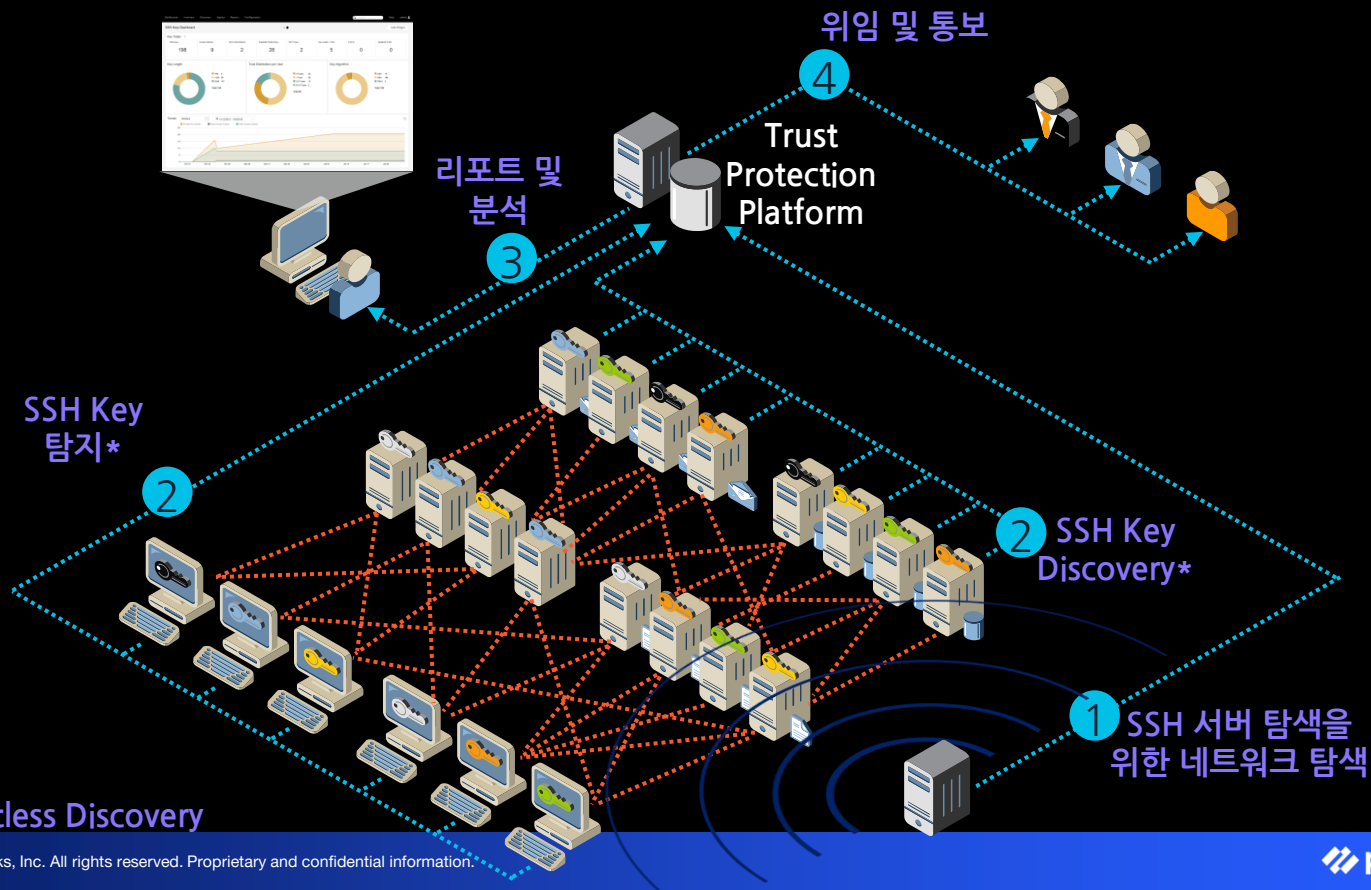
- 정책 위반 및 취약점을 식별하고, 단일 대시보드에서 권장 조치 확인.
- 서버, 사용자 및 접근 권한에 대해 보고서 제공.
- SSH 키 정책 위반 사항을 NIST 800-53에 매핑.
- 불안정한 구성과 포트 포워딩 식별.

SSH Protect

How SSH Protect Secures Your Keys



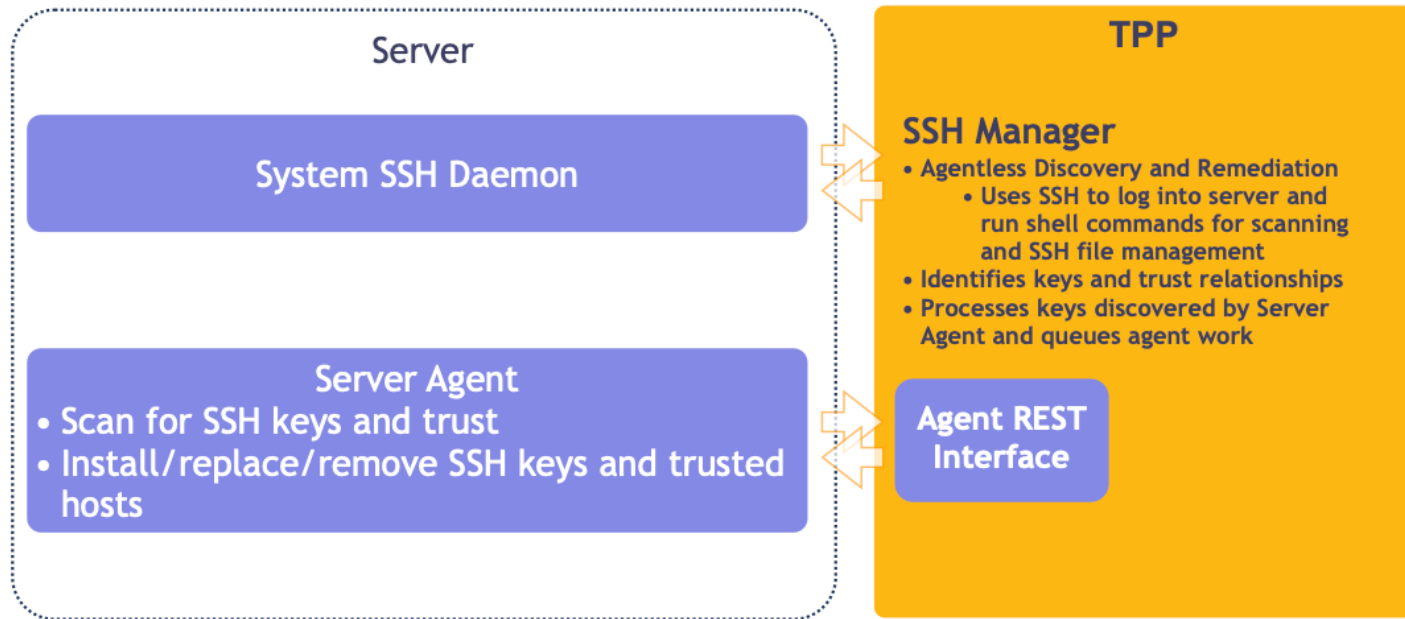
SSH Key 관리를 위한 SSH Protect



*Agent or Agentless Discovery

SSH Protect 구성 모듈

SSH Protect Components



SSH Keys Dashboard



SSH Protect

Dashboards ▾

SSH Keys

Inventory ▾

Folders

Reports ▾

Configuration ▾

Clients ▾

Workflow ▾

Logs

Search...



SSH Keys Dashboard

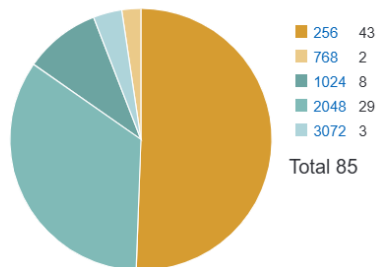


Add Widget ▾

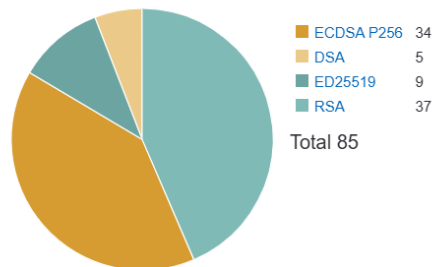
Key Totals +

Total Keys	Access Orphans	Assigned To Me	Authorized Key Control	Duplicate Client Private Keys	Duplicate Host Private Keys	In Error	Key Older than Allowed
87	15	0	18	5	0	0	0
Key Size < 1024	Key Smaller than Policy	Key Type Violations	NIST Noncompliant Keys	Passphrase Unknown	Pending My Approval	Private Key Orphans	Root Authorizations
2	10	3	22	2	0	3	5
SSH1 Keys	Unknown Client Access	Untracked Keys	Unused Authorized Keys Last 365 Days				
0	0	0	22				

Key Size

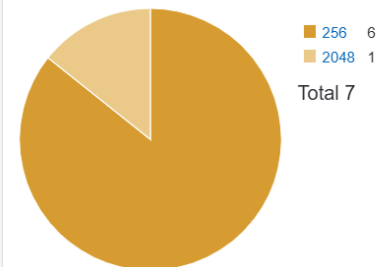


Key Algorithm



Network Discovery - Key Sizes

Last 365 Days



SSH Keyset Inventory

[Dashboards](#)[SSH Keys](#)[Inventory](#)[Folders](#)[Reports](#)[Configuration](#)[Clients](#)[Workflow](#)[Logs](#)

SSH Keyset Inventory

[Create New Keyset](#)

Common Filters

Status

Risks

NIST Control Number

Folder

☐ Include Subfolders

Device

Account

Rotation Date

Key Usage

[Clear all](#)

Properties

[Move Keysets](#)39 Keysets | [Edit Columns](#)

☐	Access	Type	Key Type	Private	Public	Last Rotated	Risks	Status	NIST Control Number	FingerprintSHA256	FingerprintMD5	Keyset ID
☐	unknown → Brian@ip-10-1-0-31	Client	RSA 2048	0	1		Client Access Orphan Missing Options	OK	AC-2, AC-6, AC-20, CP-2	uO/KESSsJOIIS...	95:46:89:a2:5d:...	05455BCB0F410
☐	unknown → many	Client	RSA 2048	0	2		Root Access Orphan, Client Access Orphan Missing Options	OK	AC-2, AC-6, AC-20, CP-2	TIEUAbNNqZoU...	c1:96:da:44:ad:...	28F9A72A6163D
☐	Sandra@ip-10-1-0-31 → Sandra@ip-10-1-0-30	Client	RSA 2048	1	1		Missing Options	OK	AC-20, CP-2	aXUlrQumjDTez...	09:98:5d:46:2d:...	325EA0C1B8583
☐	unknown → Bob@ip-10-1-0-30	Client	RSA 1024	0	1		Key Smaller Than Required, Client Access Orphan Missing Options	OK	AC-2, AC-6, AC-20, CP-2, SC-12	uti+/mPJyBt/9dd...	78:59:t2:fa:8a:1:...	52FEEA04C12C1
☐	Pat@ip-10-1-0-32 → Pat@ip-10-1-0-30	Client	RSA 2048	1	1			OK		OdgNydA2QTJ...	21:79:40:fb:fe:3f:...	546EFABBBF971
☐	unknown → Joe@ip-10-1-0-30	Client	RSA 2048	0	1		Client Access Orphan Missing Options	OK	AC-2, AC-6, AC-20, CP-2	fMle+7CFmRsf...	ee:7b:20:3d:cc:...	6A5EB9F7039F0
							Key Smaller Than					

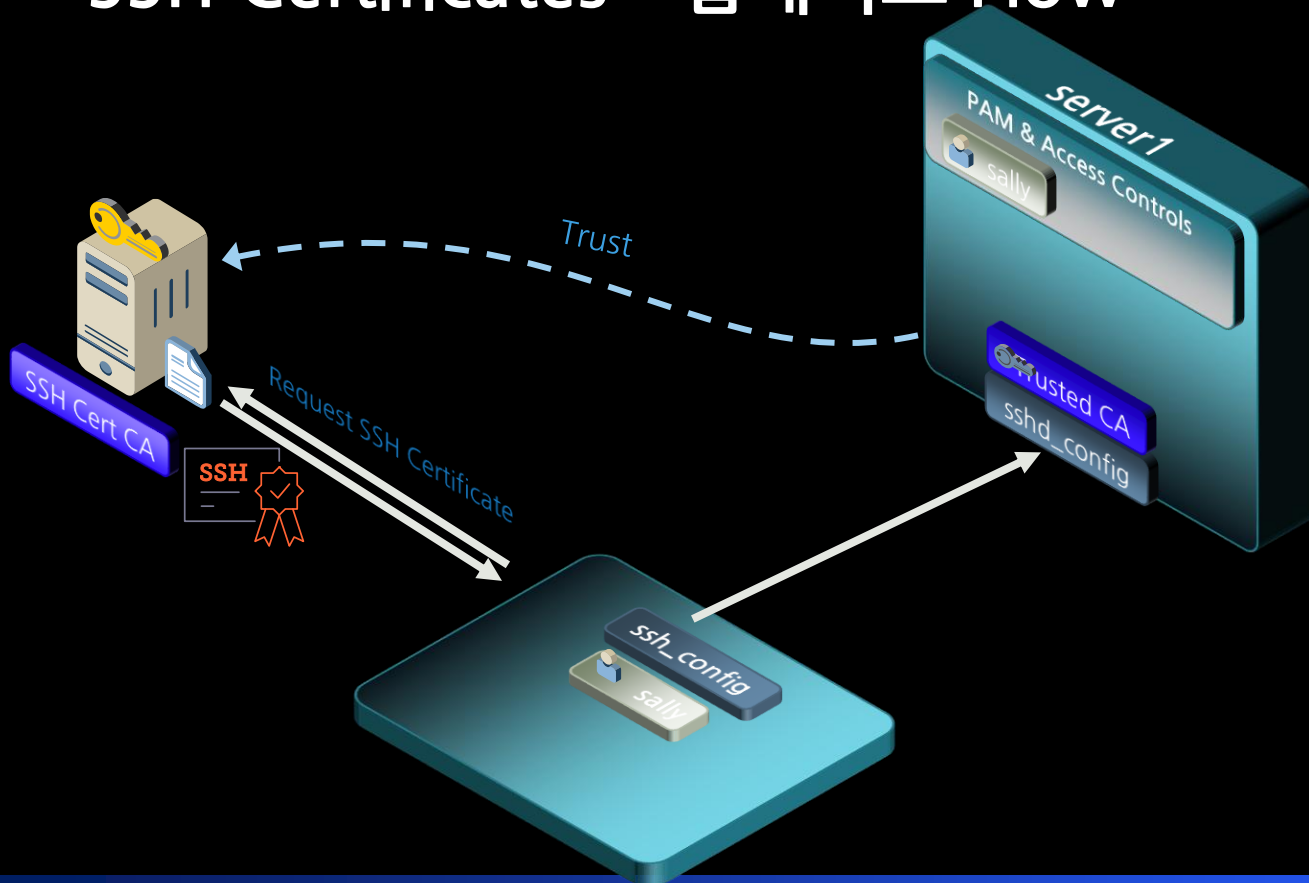
SSH Certificate & CA

- 기업에서는 Venafi SSH Protect를 사용하여 클라이언트 및 호스트 인증을 위한 SSH 인증서를 발급받고 관리할 수 있습니다.
- SSH 인증서는 SSH 키와 달리 만료 날짜를 포함한 메타데이터가 내장되어 있어 보안을 크게 향상시키고 정책 시행을 강화합니다.
- 또한, SSH 관리가 간소화되며, 일시적인 자격 증명도 지원



- 새로운 SSH CA(인증 기관) 설정
- “문(doors)” 인벤토리 작성
- 새로운 잠금 장치 설치
- SSH 인증서 발급 활성화
- SSH 인증서 프로세스 간소화
- SSH 키 “잠금 장치” 체계적으로 제거”

SSH Certificates - 업데이트 Flow



SSH 인증서를 활용한 서버간 인증

1. CA 키 쌍 생성 및 배포
2. 인증서 생성 및 서명
3. 서버에 인증서 설치.
4. 서버 간 SSH 연결 시 인증
5. 유효성 검사
6. SSH 연결 확립

Thank You

paloaltonetworks.com