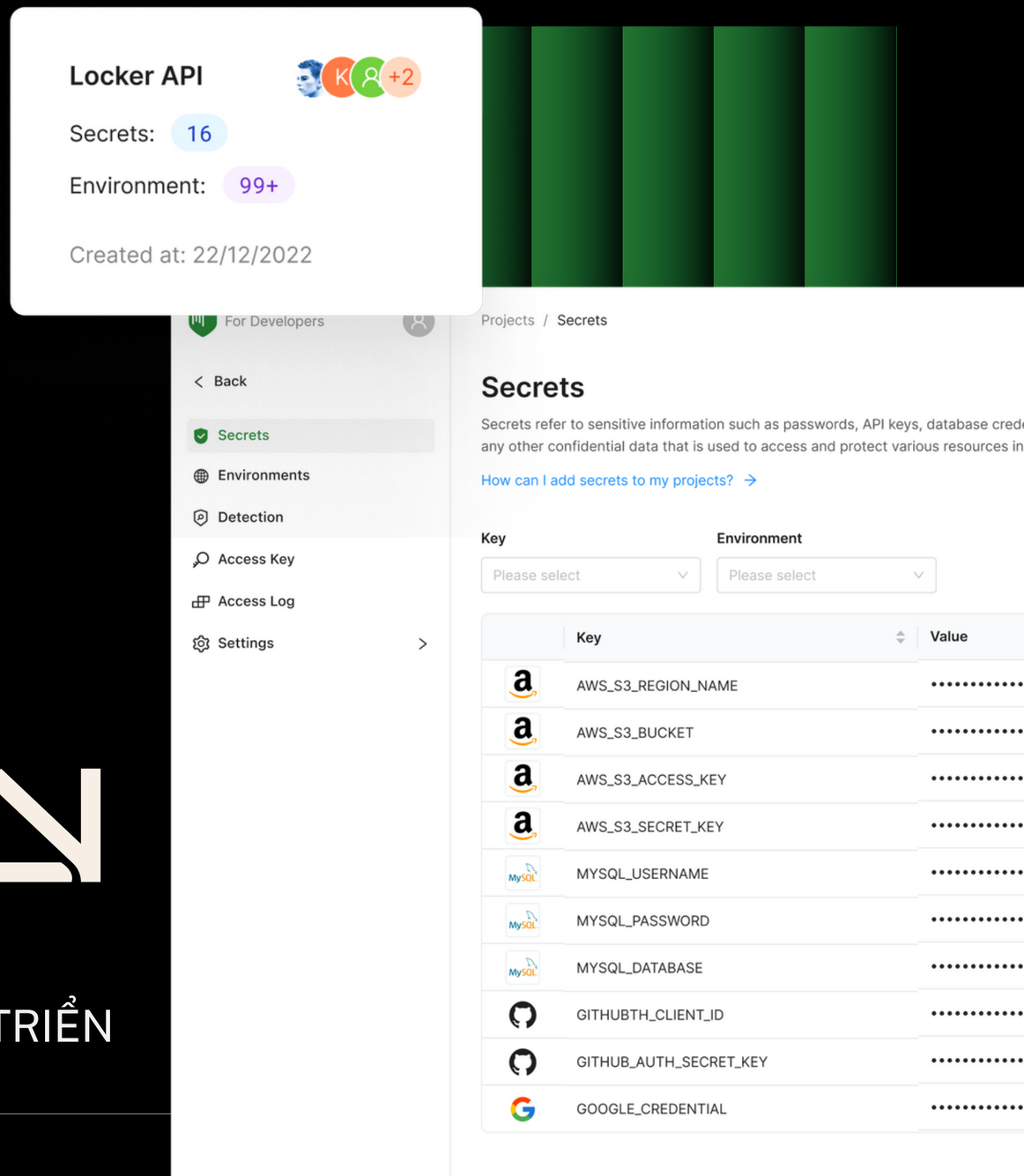
Locker

Một sản phẩm của CyStack

LOCKER SECRETS MANAGER

TRÌNH QUẢN LÝ DỮ LIỆU BÍ MẬT LOCKER
THIẾT KẾ DÀNH CHO NHU CẦU CỦA CÁC NHÀ PHÁT TRIỂN



Locker

Nội dung chính

LOCKER SECRETS MANAGER

Thách thức chung

LOCKER SECRETS MANAGER

LOCKER SECRETS MANAGER

LOCKER SECRETS MANAGER

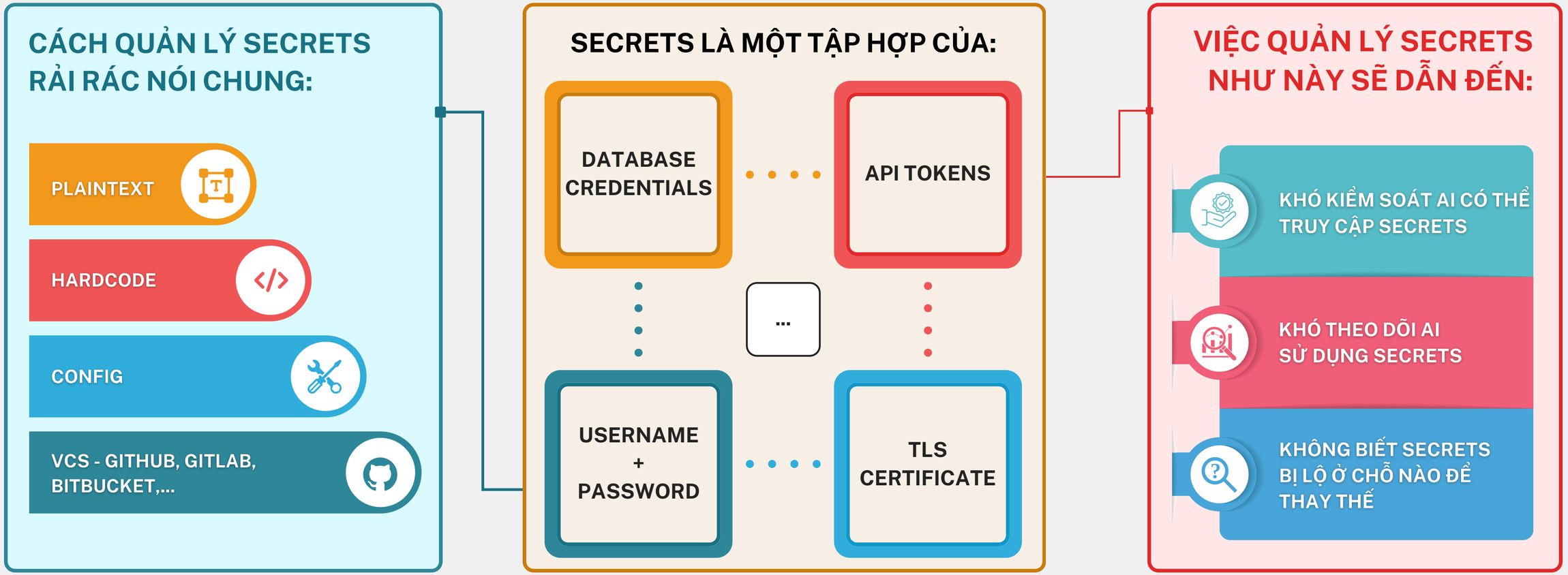
LOCKER SECRETS MANAGER

LOCKER SECRETS MANAGER

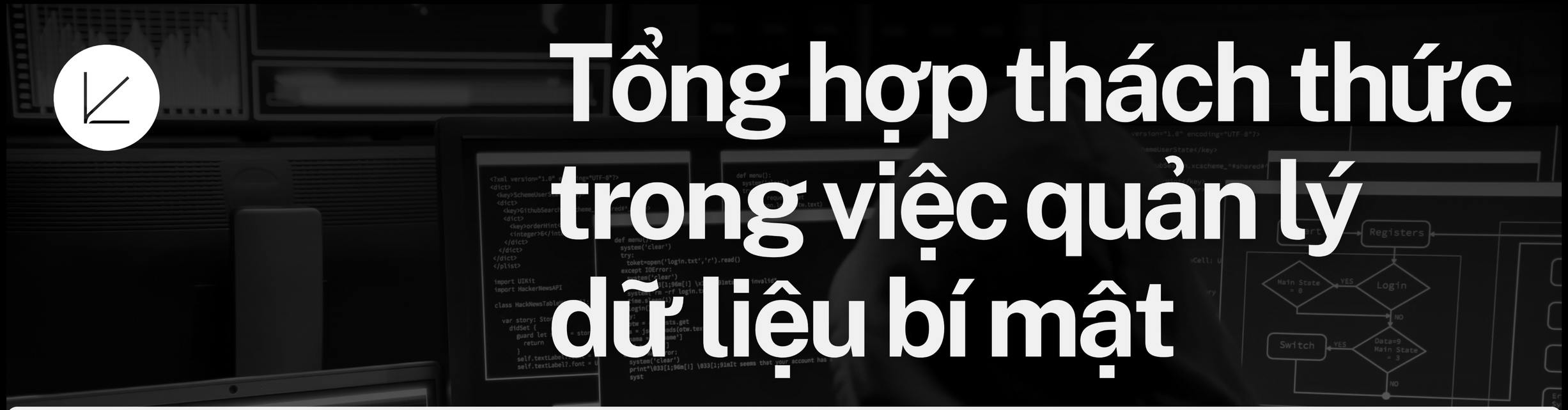
SECRETS LÀ GÌ?

Trong lập trình, "secrets" là các thông tin nhạy cảm như mật khẩu, khóa API, token truy cập, hoặc bất kỳ dữ liệu nào mà ứng dụng hoặc hệ thống cần để truy cập vào các dịch vụ bên ngoài (authorization) hoặc để xác thực người dùng (authentication). Việc bảo vệ các secrets rất quan trọng để tránh truy cập trái phép hoặc lộ thông tin nhạy cảm. Trong lập trình, thường sử dụng các công cụ và phương pháp để lưu trữ, quản lý và truy cập các secrets một cách an toàn và bảo mật.

Ví dụ về secrets và các thách thức gặp phải trong quá trình lưu trữ secrets:



VCS - Version Control System: Hệ thống quản lý phiên bản



Tổng hợp thách thức trong việc quản lý dữ liệu bí mật

01
Giữ secrets an toàn.

02
Lưu trữ secrets một cách an toàn.

03
Phải thay đổi key - mã khoá thường xuyên.

04
Kiểm soát ai có thể xem secrets.

05
Theo dõi ai sử dụng secrets.

06
Tích hợp secrets với các hệ thống hiện tại một cách tự động.

07
Chia sẻ secrets một cách an toàn.

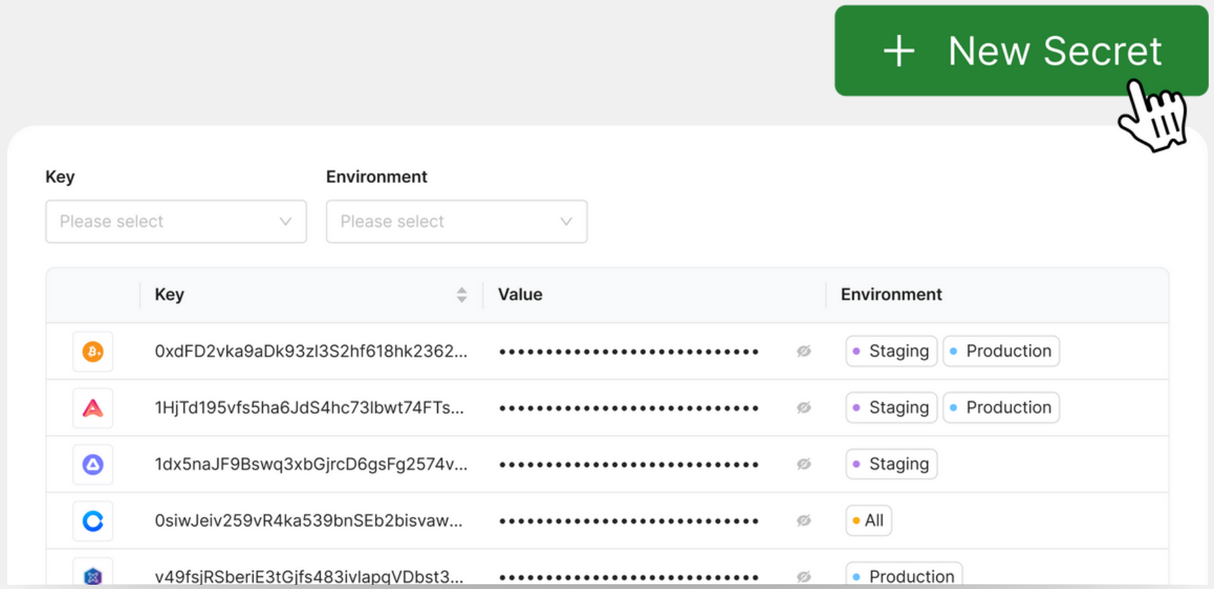
08
Thay đổi secrets tự động.

09
Nâng cao nhận thức cho các nhà phát triển về cách bảo mật secrets.

10
Không phụ thuộc quá nhiều vào một giải pháp.

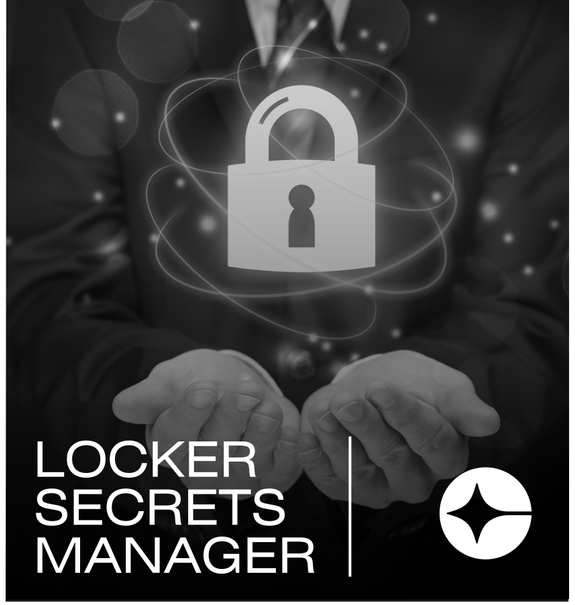
Giới thiệu về trình quản lý dữ liệu bí mật Locker

Trình quản lý dữ liệu bí mật Locker đơn giản hoá việc lưu trữ và quản lý các dữ liệu phục vụ vòng đời phát triển phần mềm (gọi là secrets) như SSH key, API key, mật khẩu cơ sở dữ liệu... Nhà phát triển có thể truy cập secrets thông qua CLI và SDK lập trình được tích hợp vào mã nguồn của dự án.



LOCKER - MỘT SẢN PHẨM CỦA CYSTACK

Cách Locker SM hoạt động



01

Locker lưu trữ secrets vào một kho dữ liệu tập trung được gọi là secrets vault.

02

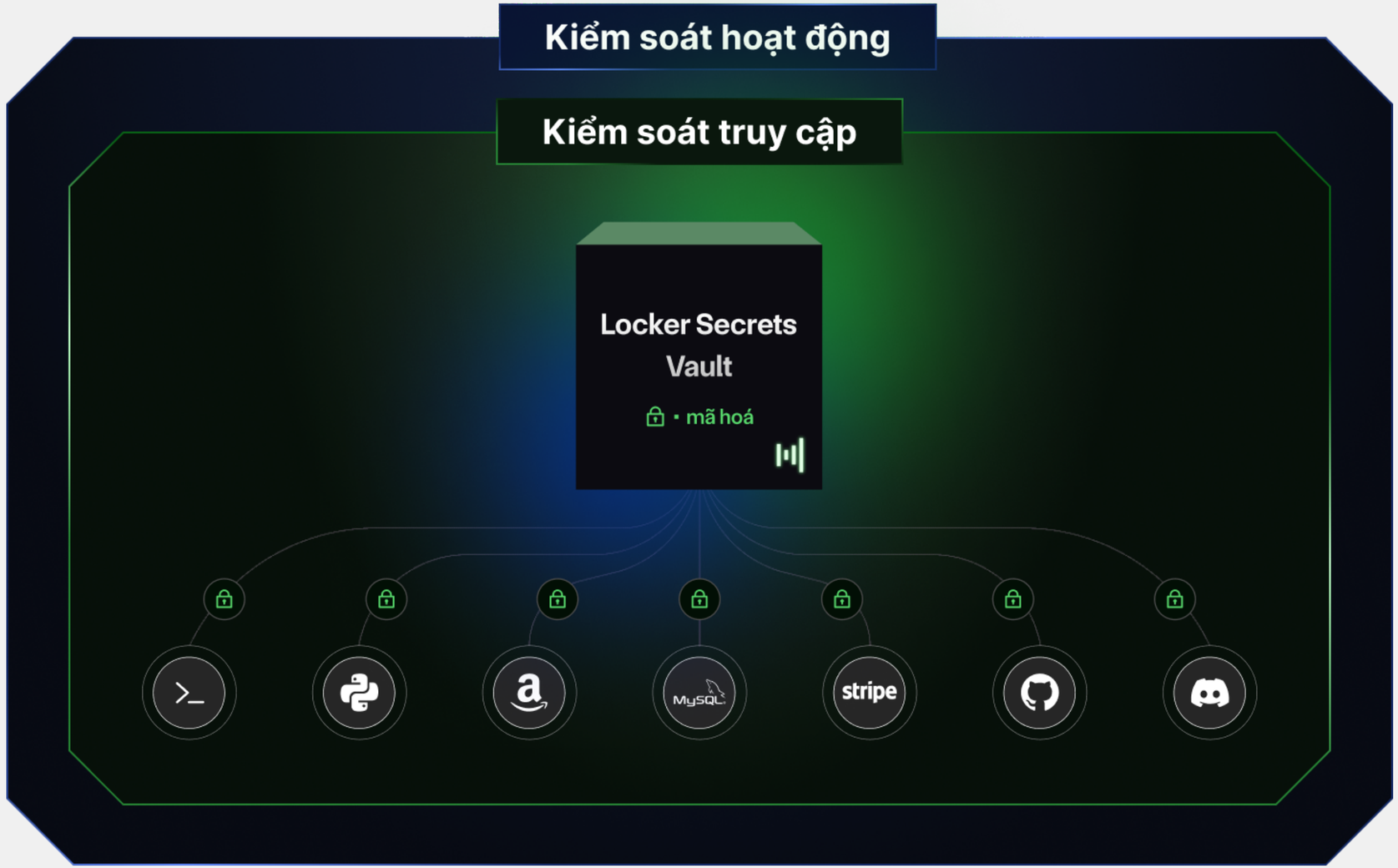
Dữ liệu trong Locker được bảo vệ hoàn toàn an toàn bằng cách sử dụng mã hóa đầu cuối, mã hóa không thông tin và mô hình không tin tưởng.

03

Các ứng dụng thứ ba muốn truy cập đến secrets được lưu trong Locker, hoặc ngược lại, Locker truyền secrets đến các ứng dụng thứ 3 để cấp quyền, đường truyền đều được mã hoá tuyệt đối.

- *Mã hóa đầu cuối (end-to-end encryption): đảm bảo rằng dữ liệu được mã hóa và giải mã an toàn chỉ trên thiết bị của người dùng.*
- *Mã hóa không thông tin (zero-knowledge encryption): đảm bảo rằng chỉ có người dùng mới có khóa mã hóa cho hòm an toàn của họ.*
- *Mô hình không tin tưởng (zero trust model): đảm bảo mọi mọi hoạt động và người dùng đều được xem xét và xác thực một cách kỹ lưỡng.*

Sơ đồ giải thích cách Locker SM hoạt động



https://locker.io/

Lợi ích của việc dùng Locker SM

01 - TĂNG CƯỜNG BẢO MẬT

Bằng cách sử dụng Locker, các thông tin nhạy cảm như mật khẩu, khóa API, token truy cập được lưu trữ và quản lý một cách an toàn hơn. Điều này giảm thiểu rủi ro truy cập trái phép và lộ thông tin, giúp bảo vệ dữ liệu của bạn.

02 - QUẢN LÝ SECRETS DỄ DÀNG HƠN

Các secrets được lưu trữ tập trung trong một nơi, giúp quản lý và theo dõi chúng trở nên thuận tiện hơn. Bạn có thể dễ dàng thêm, sửa đổi hoặc xóa secrets mà không cần phải thực hiện thủ công trên nhiều hệ thống.

03 - MÃ HÓA MẠNH MẼ

Dữ liệu trong Locker được mã hóa một cách mạnh mẽ, bảo vệ chúng khỏi sự truy cập trái phép. Thậm chí khi có một sự tấn công xâm nhập, thông tin nhạy cảm vẫn được bảo vệ.

04 - KIỂM SOÁT TRUY CẬP CHẶT CHẼ

Locker cung cấp các cơ chế kiểm soát truy cập tinh tế, cho phép bạn chỉ định rõ ràng ai có quyền truy cập và sử dụng các secrets. Điều này giúp ngăn chặn truy cập không cần thiết và tăng cường bảo mật hệ thống.

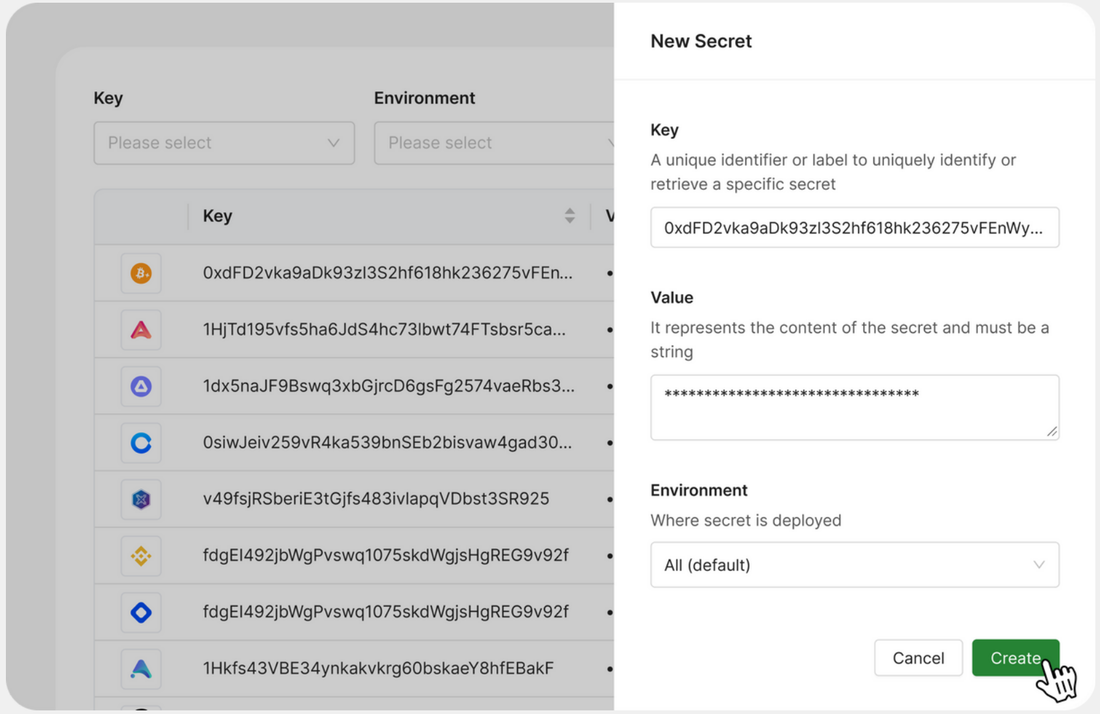
05 - THEO DÕI VÀ KIỂM TRA HOẠT ĐỘNG

Locker cung cấp chức năng audit trail, cho phép bạn ghi lại và theo dõi các hoạt động liên quan đến secrets. Bạn có thể dễ dàng kiểm tra và xác minh việc sử dụng của các secrets này.

06 - TÍCH HỢP LINH HOẠT

Locker tích hợp tốt với các công cụ và dịch vụ phổ biến trong quy trình phát triển phần mềm như AWS, Azure, và các dịch vụ cloud khác. Điều này giúp bạn dễ dàng tích hợp và sử dụng secrets trong các ứng dụng và hệ thống của mình mà không gặp phải sự cản trở lớn.

Tính năng của Locker SM



01

Lưu trữ và quản lý secrets được mã hoá.

02

Phân loại secrets theo môi trường phát triển: dev, staging, production...

03

Hỗ trợ SDK lập trình: với các ngôn ngữ lập trình phổ biến như Python, Go, JS, C#

04

Hỗ trợ CLI: thuận tiện cho quá trình CI/CD và DevSecOps.

05

Kiểm soát chia sẻ, truy cập secrets cho thành viên theo từng cấp độ.

06

Kiểm tra nhật ký truy cập qua thời gian, vị trí, địa chỉ IP của người sử dụng

07

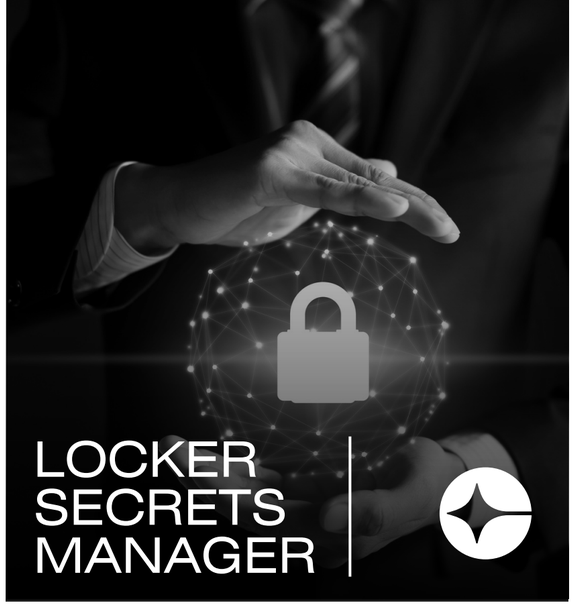
Tự động phát hiện secrets được sử dụng không an toàn trong mã nguồn, tự động thay thế bằng Locker SDK, và xoá lịch sử Git.

08

Tự động thay đổi khoá bí mật định kỳ.

BẢO MẬT & MINH BẠCH

Giá trị cốt lõi của Locker SM



MÃ HOÁ NÂNG CAO

Locker sử dụng **mã hoá đầu cuối** và **mã hoá không thông tin** đảm bảo quyền truy cập độc quyền kho lưu trữ. Dữ liệu được mã hoá và giải mã ngay trên thiết bị của bạn, đảm bảo ngay cả Locker cũng không thể truy cập.

MÃ NGUỒN MỞ

Sử dụng mã nguồn mở là cách chúng tôi chứng minh cam kết mang đến một sản phẩm minh bạch và đáng tin cậy. Thông qua công bố mã nguồn của mình, chúng tôi đảm bảo rằng bất kỳ ai cũng có thể xem, báo cáo lỗi và đóng góp các thay đổi để cải thiện Locker.

KIỂM THỬ ĐỘC LẬP

Locker thường xuyên trải qua các cuộc kiểm thử độc từ nền tảng săn lỗi nhận thưởng WhiteHub và các chuyên gia bảo mật tại CyStack, giúp phát hiện và giải quyết các lỗ hổng tiềm ẩn đồng thời tăng cường các giao thức và quy trình bảo mật của chúng tôi.

Tính khả dụng của Locker SM

Linh hoạt và thích ứng thông qua hỗ trợ các ngôn ngữ lập trình phổ biến

BẢO MẬT VÀ MINH BẠCH

BẢO MẬT VÀ MINH BẠCH

BẢO MẬT VÀ MINH BẠCH

BẢO MẬT VÀ MINH BẠCH

BẢO MẬT VÀ MINH BẠCH

https://locker.io/

Các use cases phổ biến

LƯU TRỮ BIẾN NHẠY CẢM

01 - THÁCH THỨC

Loại bỏ thông tin đăng nhập, khóa, và token được hardcode cứng trên các đám mây và môi trường khác nhau.

02 - VẤN ĐỀ

Hardcode, lưu thô secrets trong file config hay biến môi trường khiến bất kỳ ai truy cập được vào mã nguồn, tệp hoặc biến môi trường đều có thể đọc và trích xuất secrets. Nếu mã nguồn bị rò rỉ hoặc bị xâm phạm, secrets có thể dễ dàng bị trích xuất và sử dụng cho mục đích xấu, gây tổn hại cho hệ thống.

LOCKER SECRETS MANAGER

03 - GIẢI PHÁP

- Sử dụng Locker thay cho biến môi trường để kiểm soát secrets dễ dàng, kể cả trong quá trình hoạt động của chương trình.
- Locker ứng dụng công nghệ **mã hóa đầu cuối** và **mã hoá không thông tin** để lưu trữ, đảm bảo rằng secrets được bảo mật tuyệt đối và không ai khác có thể truy cập được vào kho dữ liệu của người dùng ngoại trừ họ.
- Cho phép người dùng sắp xếp các nhóm secrets vào các dự án và môi trường để quản lý và truy cập một cách có hệ thống.
- Cho phép quản trị viên quản lý được tất cả secrets trong hệ thống. Khi hệ thống tăng quy mô, việc quản lý tập trung secrets giúp các dữ liệu quan trọng này vẫn được phân phối, cập nhật và đồng bộ một cách an toàn và hiệu quả.

Các use cases phổ biến

LOCKER SECRETS MANAGER

MÃ HOÁ DỮ LIỆU

01 - THÁCH THỨC

Quản lý các khóa mã hóa ở quy mô lớn là công việc khó khăn và tốn thời gian.

02 - VẤN ĐỀ

Nhiều nhà cung cấp cloud cung cấp dịch vụ quản lý khóa (KMS), nơi các khóa mã hóa có thể được phát hành và lưu trữ để duy trì một nguồn tin cậy. Tuy nhiên, điều này thường dẫn đến công việc quản lý vòng đời thủ công khi bạn muốn sử dụng các khóa của riêng mình.

03 - GIẢI PHÁP

- Locker có thể dùng như một trình quản lý khóa (KMS) để tạo và quản lý các khóa mã hóa như AES, RSA, DES, XChaCha20... phục vụ việc mã hóa dữ liệu.
- Quản lý tập trung và tự động mã hóa các khóa mã hóa các môi trường khác nhau.

Các use cases phổ biến

LƯU TRỮ KHOÁ RIÊNG TƯ CỦA VÍ CRYPTO

01 - THÁCH THỨC

Đảm bảo an toàn, bảo mật cao nhưng vẫn phải dễ dàng tiếp cận để truy cập và sử dụng một cách dễ dàng và thuận tiện.

02 - VẤN ĐỀ

- Truyền thống, việc lưu trữ khoá riêng tư của ví crypto thường gặp phải nguy cơ bị tấn công từ các hacker hoặc phần mềm độc hại, đặc biệt là khi lưu trữ trên các thiết bị kết nối internet.
- Quản lý và bảo vệ khoá riêng tư có thể trở nên phức tạp và đòi hỏi nhiều công việc.

LOCKER SECRETS MANAGER

03 - GIẢI PHÁP

- Locker là nơi an toàn để lưu trữ dữ liệu nhạy cảm như khoá bí mật của một ví crypto và có thể truy xuất thông qua công cụ tích hợp của Locker.
- Mã hóa điểm cuối (End-to-end encryption): Áp dụng mã hóa điểm cuối để bảo vệ dữ liệu trong quá trình truyền và lưu trữ, đảm bảo rằng dữ liệu chỉ có thể được giải mã bởi người được ủy quyền.

Các use cases phổ biến

HOẠT ĐỘNG NHƯ MỘT KEY-VALUE DATABASE

01 - KHÁI NIỆM

Cơ sở dữ liệu key-value là một loại cơ sở dữ liệu không cấu trúc, trong đó dữ liệu được lưu trữ và truy xuất dựa trên một cặp key (khóa) và value (giá trị) tương ứng. Mỗi key là duy nhất và được liên kết với một giá trị cụ thể.

02 - VÌ SAO LẠI CẦN DÙNG KEY-VALUE DATABASE THAY VÌ DÙNG RELATIONAL DATABASE?

Lợi ích lớn nhất của việc dùng key-value database là truy xuất thông tin nhanh. Với cơ sở dữ liệu truyền thống, nếu muốn truy xuất thông tin, tốc độ truy xuất thông tin sẽ rất chậm.

03 - SỬ DỤNG LOCKER SM NHƯ LÀ MỘT KEY-VALUE DATABASE

Với những dữ liệu bí mật cần truy xuất nhanh, như access key để truy cập vào hệ thống, thì việc dùng Locker SM như là một key-value database sẽ đảm bảo được cả hai yếu tố bảo mật và nhanh chóng.

Giới thiệu về CyStack

CyStack

CyStack là công ty an ninh mạng hàng đầu tại Việt Nam, được biết đến với khả năng nghiên cứu chuyên sâu và xây dựng các giải pháp tiên phong về bảo mật.

Sản phẩm và dịch vụ của chúng tôi tập trung vào quản lý lỗ hổng, phát hiện mối đe doạ, bảo mật cộng đồng, và bảo mật dữ liệu. Locker là một sản phẩm được phát triển bởi CyStack.

ĐƯỢC TIN TƯỞNG BỞI NHIỀU TỔ CHỨC LỚN

CAKE by VPBank · Sendo · ACB · momo · mitsubishi.com

vntrip.vn · AGRIBANK · OpenCommerce · One Mount

LOCKER
SECRETS
MANAGER

Liên hệ

Locker Secrets Manager

Bản cloud

Locker Secrets Manager

Bản self-hosted tự triển khai và quản lý

ĐIỆN THOẠI
02471099656

ĐỊA CHỈ
Toà nhà Tân Hồng Hà Complex,
317 Trường Chinh, Ngã Tư Sở,
Thanh Xuân, Hà Nội

WEBSITE
https://locker.io/

EMAIL
contact@locker.io

Thank you

LOCKER
SECRETS
MANAGER

2024

LOCKER.IO

WHERE SECRETS
STAY SAFE!