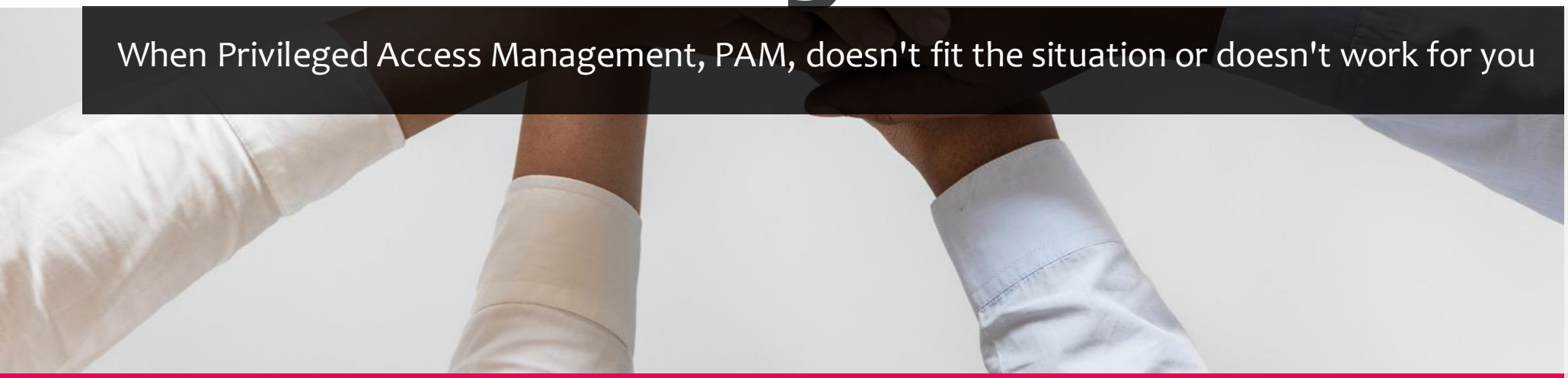
Gratitech Incorporated

Keep your credentials safe in source code, applications, and configuration files

When Privileged Access Management, PAM, doesn't fit the situation or doesn't work for you



Gratitech©

s3cr3tx ©

Gratitech safeguards technology across the entirety of applications.

Based in Chicago and serving US and multinational clients, Gratitech specializes in end-to-end protection across your entire ecosystem, from the front-end to the back-end and the code that connects the two.

We accomplish this by architecting and engineering highly secure risk-controlled software tailored to your business. Whether you're B2B, B2C, or in the public sector, cyber security and application security needs to be on top of your mind to protect your organization, your clients, your employees, your business partners, and you.

Our innovative approach protects against cyberattacks and gives you peace of mind.

About Us

Gratitech safeguards technology across the entirety of applications.

s3cr3tx

Solution to protect credentials in source code in any language

Gratitech's founder, Patrick Kelly,

Created s3cr3tx to provide a solution to one of the most difficult to remediate critical vulnerabilities in Application Security, which is protecting credentials in code. This critical vulnerability leads to major breaches and successful attacks on confidentiality, integrity, and availability if not protected or remediated appropriately

- Application Security Testing tools normally identify this complex vulnerability as "Insecure Credential storage", "Clear-text Credentials stored in code or configuration files", or "Hard coded credentials".
- S3cr3tx is a solution to protect you and your organization from this critical vulnerability that can exist in any application in any coding language and is considered one of the most difficult vulnerabilities to remediate. If you are not protected against this critical vulnerability, hackers or digital adversaries can gain access to the keys to your kingdom, which most likely will lead to critically negative impact on confidentiality, integrity and availability and may cause severe financial costs or fines in some cases.
- Gratitech's founder, Patrick Kelly, created the s3cr3tx solution to enable anyone developing applications in any language to remediate this vulnerability and protect credentials for organizations simply and securely. Patrick created and maintains a public repo: https://github.com/patrickkelly20/s3cr3tx_API for this solution and support, maintenance and Software Assurance is available from Gratitech. If you are interested in support, maintenance, or software assurance for s3cr3tx, please contact Gratitech at sales@gratitech.com or call or text Gratitech at +1(312)961-0174

Why choose to protect credentials with s3cr3tx?

Comparing existing solutions with s3cr3tx API to protect your credentials

Comparison

Before we show you how to use **s3cr3tx** let's compare it to other competing solutions in the market that have been used to try to solve the same problem

Gratitech's s3cr3tx

- Trusted, simple, custom, tailor made, specialized, easy to implement, open-source, field-tested and production AppSec solution to protect credentials stored in source code or configuration files
- Created by an AppSec SME, senior software engineer, and trusted senior technology and security advisor to remediate vulnerabilities simply and securely in any environment (ex: development thru production environments).
- Trusted solution and risk control of global enterprises, application security unicorn startups with valuations over a billion dollars and US federal government agencies with multibillion dollars and multi trillion dollars in assets.
- Backed by a company and AppSec SME that has been trusted to protect over $5 trillion in assets for global organizations, Application Security unicorn startups with valuations over a billion dollars, and US government agencies.
- Platform and language agnostic

PAM (Privileged Access Management)

- PAM is a complex, error-proned, difficult to implement, frustrating, unintended, non-specific solution to this problem for developers AppSec SMEs and infrastructure engineers
  - In practice, PAM normally ends up being a mirage or labyrinth for the goal of protecting credentials stored in source code or configuration files for developers, infrastructure engineers and AppSec SMEs.
  - Developers, Application Security Architects/Engineers, Infrastructure Engineers, and DevSecOps Engineers experience a lot of red tape and digital blockers when trying to use PAM to solve the problem they are facing in modern DevSecOps processes and organizations these days which leave organizations and individuals open to this critical vulnerability.

Protect credentials with s3cr3tx

Getting up and running with s3cr3tx API

Pricing and Gratitech's projected profit scenarios for s3cr3tx:

S3cr3tx can be used in applications on-premise, in the cloud, and on endpoint devices and IoT devices to protect credentials. Prices listed below are for annual software assurance subscriptions.

	Licensed Users	Licensed Devices	Developers	Included Support Tickets/Calls	Cost	Itemized Projected Annual Profit from individual unit sale
Open-source Community Edition	Free	5	2	0	$0	$0
Starter	10	100	50	3	$6,999	$1,013
Professional	50	500	60	30	$33,999	$5,063
Premium	200	2000	100	100	$143,000	$20,250
Enterprise	400	4000	220	500	$270,000	$40,500
Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	$750,000 - $?*	$50,000

*cost may vary reasonably if Gratitech's resource needs change in order to support an unlimited plan


It's reassuring to us knowing that you are interested in protecting your credentials with Gratitech s3cr3tx

Gratitech ©
Incorporated

ThankYou

Patrick Kelly
+1(312)961-017487
Patrick@Gratitech.com
https://Gratitech.com