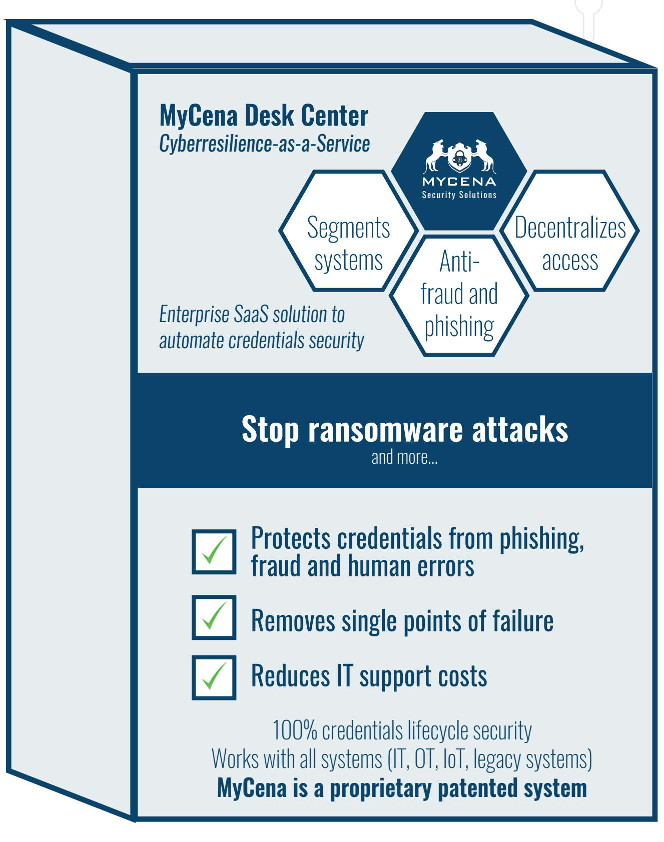
New patented system provides Cyberresilience-as-a-Service

Anti-fraud anti-phishing anti-ransomware credentials SaaS solution

MyCena Desk Center

Cyberresilience-as-a-Service (CaaS)



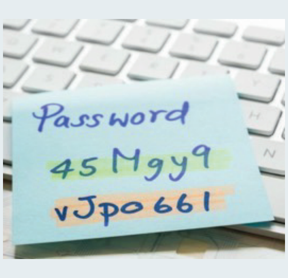
What is MyCena?
Enterprise SaaS solution to secure credentials over their entire lifecycle

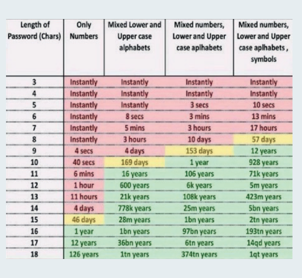
Key features
- Segments systems
- Generates strong unique passwords per system per user
- Distributes and decentralizes credentials into users' fortress
- Covers full credentials lifecycle
- System agnostic (IT, OT, IoT, legacy systems)
- Three levels of security only owner can access
- Anti-fraud anti-phishing system
- Direct access to systems with auto-filled encrypted login
- No one can see or steal passwords
- Monitor all credentials activities

Key benefits of MyCena
- Reduces up to 100% of IT helpdesk costs due to password resets
- Improves employee productivity
- Fast and economical
- Removes single, privileged access and single points of failure (SPOF)
- Breaks the supply chain of credentials used for ransomware attacks
- No modernization or change of infrastructure required
- Reduces risks of fraud inside company

Before MyCena

Employees, not the company, create the keys to access company resources



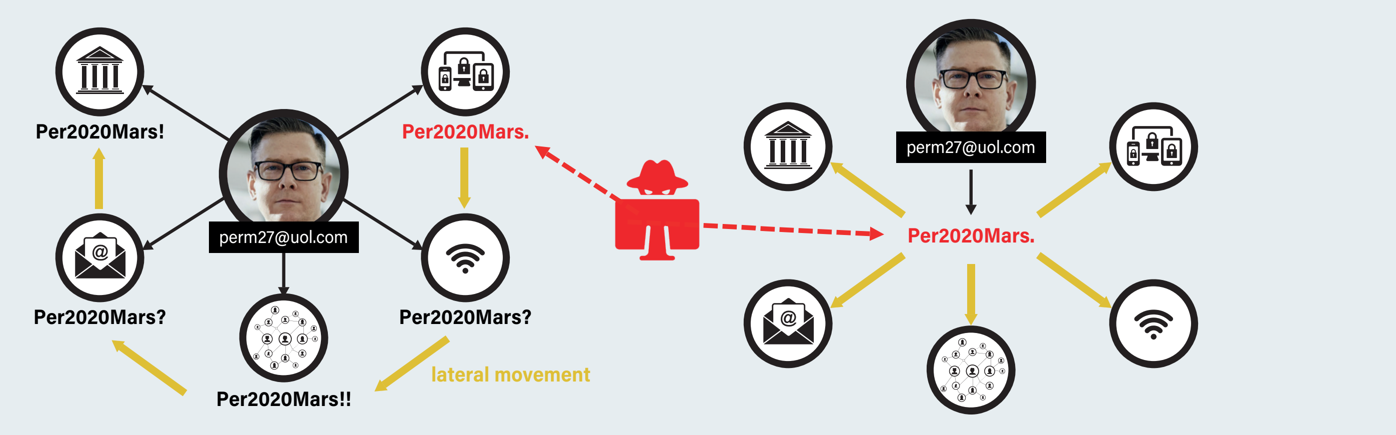


Simple passwords : name, birthday, 123456...
Reused patterns : for banking, social media, shopping, apps (123!, 123?, 123.)
Written in clear text : on post-its, paper, excel
Shared : by email, SMS, spreadsheet on cloud

Core : Servers, SOC, databases, critical infrastructure
IT : CRM, applications, chatrooms...
IoT : Printers, cameras, alarms, vehicles, radars...
OT: Machines and equipments
Call centers : Client CRM and applications

All hackers need is a password

Easy with password reuse, phishing, social engineering, credentials stuffing, brute force, dictionary attacks, dark web lists



Employee choosing passwords makes life easy for hackers

Privileged, centralised or single access makes life easy for hackers

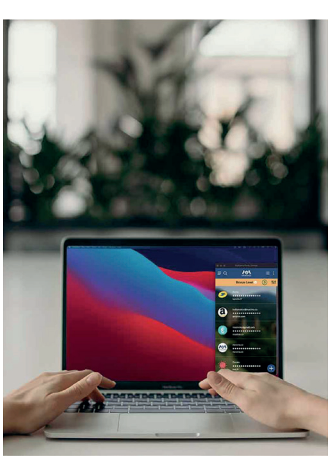
Hackers use legitimate passwords and privileged access to launch ransomware attacks

Find legitimate password	Remote Desk Protocol	Privilege escalation	Active Directory takeover	Exfiltrate data Destroy backups Deploy ransomware payload	Ransomware attack: encrypt systems and negotiate ransom

MyCena technology applies a new logic

Company, not employees, control access to company assets

Companies, not employees, create strong and unique passwords like 7D£bShX*#Wbqj-2-CiQS for every system and distribute them encrypted in real time to the right users



MyCena console
- Segment network/systems/accounts
- Manage passwords, systems rules without seeing users' passwords
- Manage roles and permissions
- Manage list of users (upload list or use Active Directory)
- Manage attributes (who receives what credentials)
- Monitor usage and potential fraud (GRC)

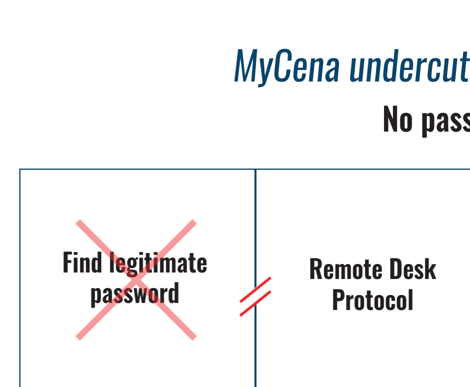
MyCena application (Mac, Windows or Linux)
- Receives preloaded encrypted passwords and systems in real time inside local fortress
- Direct access using auto-filled encrypted login

Keep systems access segmented, credentials decentralised and protected throughout lifecycle

	Creation	Distribution	Protection	Use	Expiry
Without MyCena with single master password or biometric used by password manager/ IAM / PAM / SSO	**Controlled by employee, not employer** Employee makes own passwords or master password to access company resources and assets No systems segmentation, risk of weak passwords, password pattern reuse with or without password manager/ IAM / PAM ex: Password123!, Perm2020!, Perm2021!!... No visibility on human behaviour, creates security blindspots	**Controlled by employee, not employer** Employee can share password(s) with others Risk of fraud No visibility if fraud, creates security blindspots	**Controlled by employee, not employer** Employee remembers passwords/master password, or writes on post-its, paper, notebook, excel spreadsheet in clear text Weak if using password manager/ IAM/ PAM, as passwords are centralised, creating single points of failure Risk of leak, phishing, credentials stuffing, brute force, dictionary attacks, dark web lists... No visibility if leaked or phished, creates security blindspots	**Controlled by employee, not employer** Employee types password(s)/master password Risk of phishing, keylogger, screenlogger Risks of credentials stuffing, brute force, dictionary attacks, dark web lists... No visibility if phished, creates security blindspots	**Controlled by employee, not employer** Employee can use similar password with a little change If system password not changed, employee still knows the password(s) after changing service, department, company Risks of compromising old password as with Colonial Pipeline No visibility on human behaviour, creates security blindspots
With MyCena MYCENA Security Solutions	**Controlled by employer, not employee** MyCena generates strong unique passwords for each system according to password rules for each user Auto-segment systems - No single point of failure System agnostic - Works for IT, OT, IoT, legacy systems... No one needs to see or know passwords - Not reliant on human behaviour, no security blindspot No risk of weak or reused password	**Controlled by employer, not employee** MyCena distributes encrypted preloaded passwords and systems to right users in real time No one needs to see or know passwords - No security blindspot - Manager controls permissions, passwords visibility and shareability, but does not see passwords No risk of fraud	**Controlled by employer, not employee** Encrypted passwords protected by MyCena application Private access for owner Three levels of security - accessed with token, security questions, PIN, lock pattern and passphrase Passwords are decentralised - not in the same basket User doesn't know passwords No risk of fraud, leaks, phishing, credentials stuffing, brute force, dictionary attacks, dark web lists...	**Controlled by employer, not employee** Direct access to right system using auto-filled encrypted login Employee does not type nor see passwords during use Cannot use password without direct access from MyCena No risk of fraud, phishing, keylogger, screenlogger, credentials stuffing, brute force, dictionary attacks, dark web lists...	**Controlled by employer, not employee** Manager uses 'manage attributes' feature to allocate, withdraw, expire, delete passwords when employee change service, department, company No risk of compromising old passwords
	Monitors credentials activities				

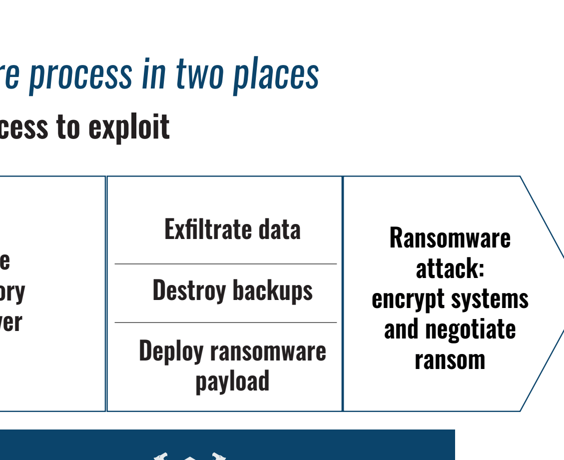
With no mental effort for users

No more login and passwords for employees to manage
MyCena provides each employee with a local fortress that only the owner can access, to use passwords they can't see or know



MyCena Fortress
Patented system
Multiple levels of security

- RECEIVE PRELOADED ENCRYPTED PASSWORDS AND SYSTEMS
- ONLY STRONG UNIQUE PASSWORDS
- THREE LEVELS OF SECURITY (BRONZE, SILVER, GOLD)
- AES-SHA 256 ENCRYPTION
- DIRECT ACCESS WITH AUTO-FILLED ENCRYPTED LOGIN
- ENCRYPTED PASSWORD SHARING IF PERMITTTED
- AUTOMATED ENCRYPTED BACKUPS



MyCena undercuts cybercriminals' ransomware process in two places

No passwords to steal, no privileged access to exploit

~~Find legitimate password~~	Remote Desk Protocol	~~Privilege escalation~~	Active Directory takeover	Exfiltrate data Destroy backups Deploy ransomware payload	Ransomware attack: encrypt systems and negotiate ransom

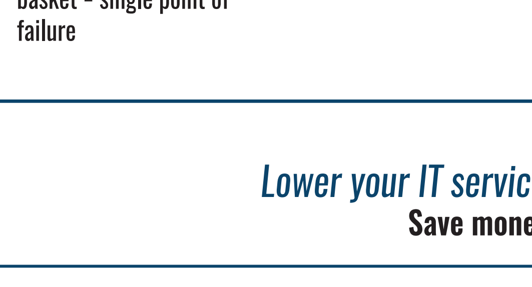
No password to steal
NO phishing, password reuse, social engineering, credentials stuffing, brute force, dictionary attacks, dark web lists

No privilege escalation
NO privileged access, centralised access, single access, single point of failure

MYCENA Security Solutions
Cybercriminals no longer have ammunition to use against your company for cyber attacks

By automating systems segmentation and credentials decentralisation, become cyberresilient by default

Without MyCena



No system segmentation
No credentials decentralisation
Reused passwords, single access, all eggs in one basket = single point of failure

No cyber-resilience
If there is a breach, can spread like wildfire

With MyCena

System segmentation
Credentials decentralisation
Strong unique passwords, no single or privileged access, not all eggs in one basket, no single point of failure

Cyber-resilience by default
If there is a breach, the breach is contained

Lower your IT service desk costs at the same time

Save money on password resets

Without MyCena	With MyCena
20-50% of all service desk calls to reset forgotten passwords (Gartner) Locked out employees, loss of productivity	No service desk calls to reset forgotten password No employee locked out, no loss of productivity

About MyCena

Who are we?
MyCena is a European company founded in 2016, specialised in credentials security.

What does MyCena do?
MyCena is a complete system of security, control and management of credentials. More than a state-of-the-art technology, MyCena incorporates a comprehensive cyber resilience strategy, automating system segmentation, creating unique and strong passwords for each system, distributing credentials to the right users in real time, providing credentials decentralization and protection, encrypted password access, credentials usage monitoring, eliminating all human risks of error, fraud and phishing without mental effort (no more passwords to create, memorize, type or see).

What changes with MyCena?
Before MyCena, people presumed there was no solution to prevent breaches in the first place. For businesses and governments, cybersecurity was about accepting cyberbreaches as a fact of life and emphasizing responsiveness: monitoring, detecting, reporting attacks, rapid response when you get breached, managing chaos and damage after breach. Solutions like IDS, IPS, WAF, DLP, MFA, EDR, BC/DR, SIEM, PAM, patch management... have made cybersecurity very expensive, yet ineffective. But as new variants appear all the time, those programs were always playing catch up, unable to prevent a single compromised password from creating havoc.

With MyCena, you tackle the source of cyberattacks rather than the symptoms, avoiding intrusions, attacks, loss of money and reputation. Cybersecurity is now about strengthening access architecture, removing single points of failure, regaining full control over your riskiest cybersecurity points, undercutting the enemy's capabilities by removing their ammunition and saving money on unnecessary costs. Indeed, as there is no password to know in the first place, you save over half of your IT helpdesk costs, which are linked to passwords reset.

info@mycena.co
www.mycena.co