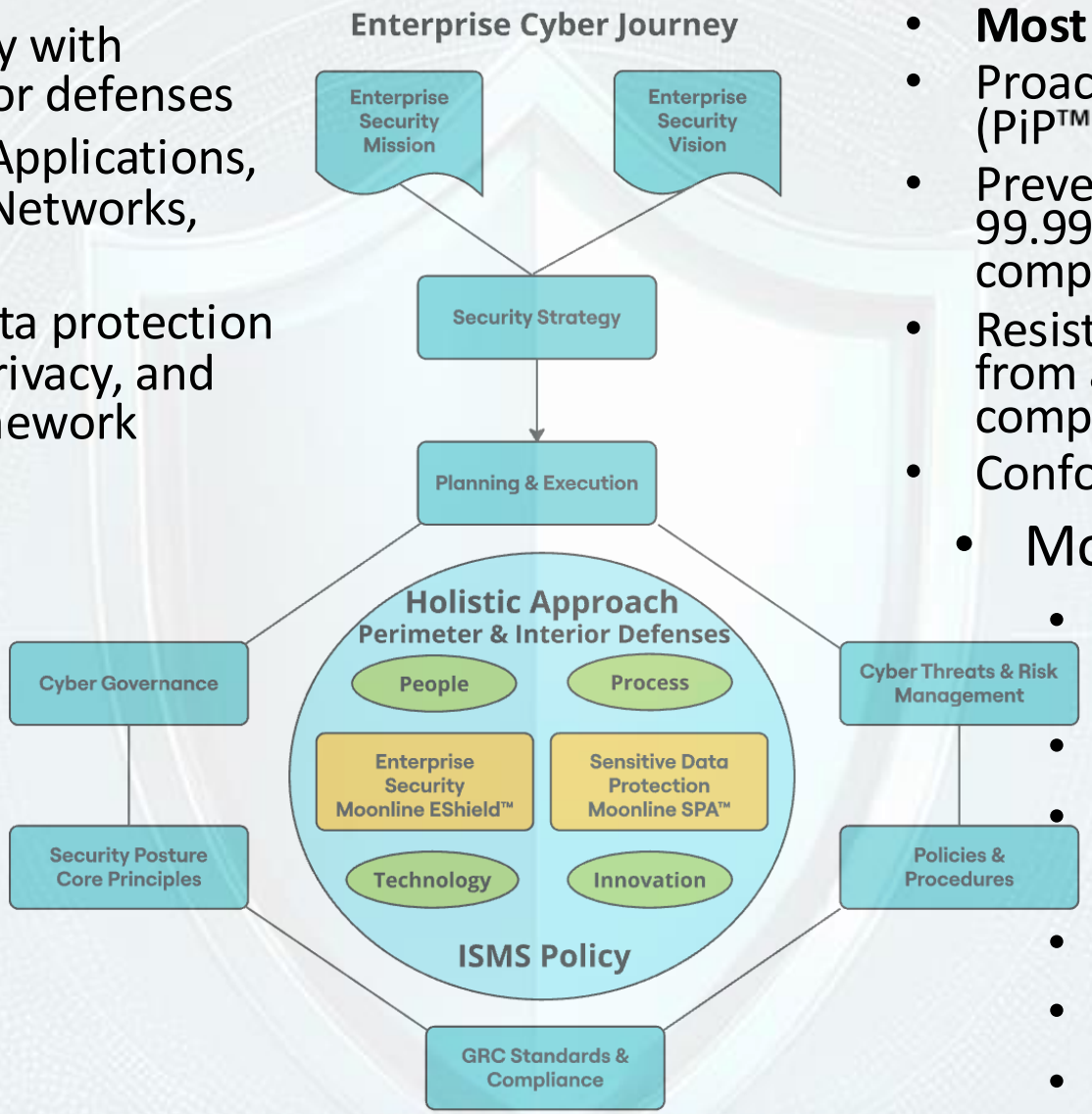
C-Shield™
Proactive identity Protection (PiP™)

C-Shield™

- What is C-Shield?
  - Holistic Cybersecurity with perimeter and interior defenses
  - Perimeter: Protects Applications, Servers, Databases, Networks, and Resources
  - Interior: Sensitive data protection with SPA (Security, Privacy, and Anonymization) framework
  - Identity Provider
- Easy Deployment
  - Authenticator App
  - Admin Portal
  - C-Shield Service

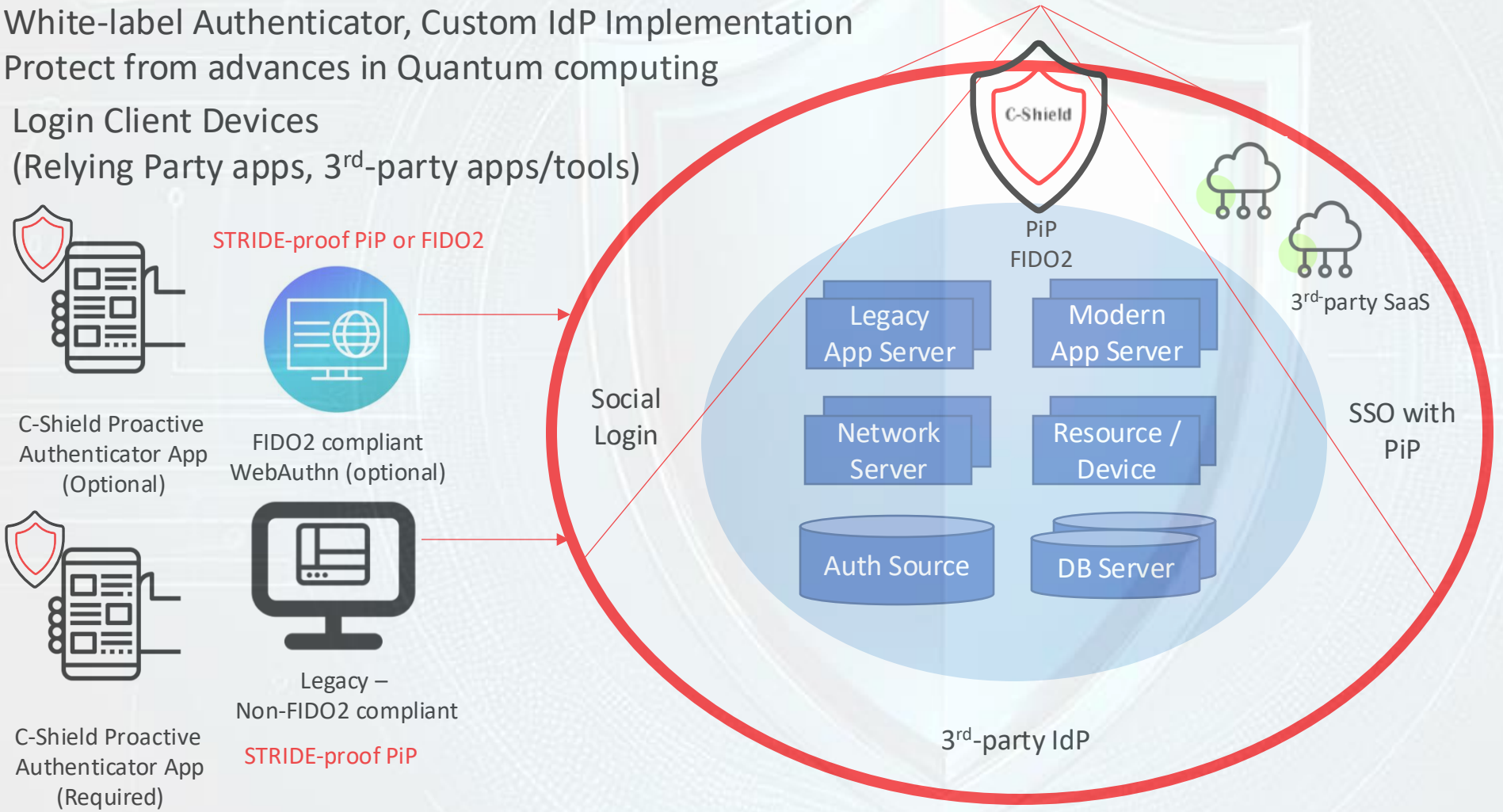


- Impeccable Defense
  - **Most secure in the world**
  - Proactive Identity Protection (PiP™)
  - Prevent MFA Fatigue by 99.999999999998% compared to FIDO2
  - Resistant to security threats from advances in quantum computing
  - Conforms to regulations
- Most secure and practical
  - Better than prevalent standards
  - Less Expensive
  - Zero-code, Easy Integration
  - Support Legacy Apps
  - Phishing and STRIDE-proof
  - Thwart malicious attacks

COSMIC KAYKA
GRAND SOLUTIONS IN HARMONY

C-Shield™

- STRIDE-proof Proactive identity Protection (PiP™): **secure & practical** than 2FA, MFA, U2F, UAF, FIDO2
- Protect applications, tools, servers, databases, networks, resources with PiP and/or FIDO2
- Avoid phishing-prone 2FA, MFA. Supports both modern and legacy apps/platforms
- Zero-code, easy integration. Enhance protection on top of 3rd-party IdP solution
- White-label Authenticator, Custom IdP Implementation
- Protect from advances in Quantum computing



Moonline™ C-Shield™ Enterprise Security

Proactive identity Protection™
Zero Trust
Zero Code / Easy Integration
STRIDE-proof, also supports FIDO2
Detection and Response
Numerous Impl Options
High Interoperability
Cost Effective Optimal Solution
Compliance & Governance
Impeccable Defense

Security Posture
Security Policy Strategies

KP - Keep your Password
KPX - KP Extended
KPX2, KPX2' - KP Extended 2
DP - Dynamic Password
DPX - DP Extended
DPX2, DPX2' - DP Extended 2
PL - Password Less
PLX - PL Extended
PLX2', PLX2'' - PL Extended 2
CA - Continuous Authentication
CAX - CA Extended
BTE - Blue Tooth Enabled
More secure than FIDO2, U2F, CBA with PiP and Mobile Phone as Dongle

Security Posture
Scope & Interoperability

Shield internal or 3rd party IdP
Shield Legacy Apps
Shield Modern Apps
Shield 3rd party SaaS Apps
SSO with PiP
Shield Social Login
Shield App Servers and DB Servers
Shield Network Resources
Act as your Enterprise IdP

Main Features

- Proactive identity Protection (PiP™), a **more secure and practical** STRIDE-proof strategy than MFA, U2F, FIDO2. Pushing for PiP™ as a future standard.
- On-device authentication with WebAuthn (FIDO2) or authentication with C-Shield authenticator app (PiP™)
- Flexible proactive authenticator tied to one or more physical devices and available as mobile app or accessible from browsers
- Supports STRIDE-proof login with PiP™ while allowing various types of user experiences: password-less, with password, OTP, dynamic password
- Secures logins to modern and legacy applications, database and network servers, resources, and 3rd party-SaaS applications
- Works with all types of authentication sources and stores including Social Logins
- Integrates using zero-code or low-code based on selected options – through configuration, single-line code changes and minimal UI changes
- Works seamlessly with existing Enterprise Authentication Servers and IdPs

Benefits

- ✓ Enable more secure and practical STRIDE-proof authentication with no or minimal changes (optional) to applications and servers
- ✓ Support clients running on non-FIDO2 compliant devices
- ✓ Enable FIDO2 login to compliant applications and servers
- ✓ Avoid implementing and maintaining less secure, phishing-prone, fatigue-prone 2FA and MFA techniques based on SMS, phone, email and TOTPs
- ✓ Thwart or discourage DOS efforts on login accounts
- ✓ Ease enabling and rollout of FIDO2-level login security to legacy devices, clients and user logins
- ✓ Stop malicious actors right on their tracks – their logins using leaked but valid passwords fail right away
- ✓ Reduced reliance on smart phone or some costly device
- ✓ Simplify and reduce user anxiety with highly secure and flex-device logins
- ✓ Meet governance, risk, and compliance (GRC) requirements

Comparison with Others

Criteria	C-Shield Proactive Authenticator	Authenticator Apps (Duo, 2FAS, Okta, Microsoft, Google, Aegis)	FIDO2 Servers (HYPER, etc.)
Quantum-proof security	Yes	No	No
Modern login devices with FIDO2 support	STRIDE-proof PiP, FIDO2	FIDO2, phishing-prone 2FA, MFA	FIDO2, phishing prone FIDO1 2FA, MFA
Legacy login devices without FIDO2 support	STRIDE-proof PiP	Phishing prone 2FA, MFA, TOTP	Phishing prone FIDO1 2FA, MFA
Requires a smart device?	Only for non-FIDO2 logins	Yes	Optional
Need Internet Connection?	App device (for STRIDE-proof PiP), login client machine (FIDO2)	Depends on the login option	Login client machine
Need user action in external app to login?	Yes - for STRIDE-proof PiP, No – for login client machine (FIDO2)	Yes – for phishing prone 2FA, MFA TOTP logins	Depends
Guard existing password-based?	Yes	Phishing prone 2FA, MFA, OTP	No
Dynamic password supported?	Yes	No	No
Password-less supported?	Yes (STRIDE-proof PiP, FIDO2)	Few, FIDO2 Only?	Yes
Enhance another IdP Solution	Yes	No	No
Application changes	Zero-code or minimal changes	Yes	Yes
Account Lockout issues	No	Yes	Yes
MFA Fatigue issues? Breaks security?	Prevents 99.9999999999998%, No	Yes, Yes	Yes, Yes
Protection Coverage	Impeccable, Very High	Medium to High	High
Thwart hacking and DOS attempts	Yes – in all cases	FIDO2 only	FIDO2 only

Prevalent Standards - cons

- Cons of 2F, MFA, OTP, TOTP
  - Phishing prone, account lockouts
- Cons of Universal 2nd Factor (FIDO U2F)
  - Cost (security keys/device), carry and manage keys, limited device support, potential for loss (keys), tedious process if device is lost, advanced phishing prone, 1st factor of password is phishing prone
  - Yubico OTP subjected to realtime replay attacks when no challenge-response, account lockouts
- Cons of Fast IDentity Online (UAF, FIDO2, WebAuthn)
  - Cost, time to implement, new technology, no broader support, legacy non-compliant devices, vendor lock-in issue with keys, known hole w.r.t. non-authenticated key exchange in CTAP2, MFA Fatigue, account lockouts
- Cons of Passkeys
  - Require specific hardware, Secure Enclave. Resetting passkeys is complicated. User resistance. Synched passkeys are synched to cloud.
- Cons of SAML-based SSO for web applications
  - Complex setup at IdP and SP with certificates, Delay with Browser redirects, privacy issues with user info in SAML assertion URL, Security vulnerabilities (MitM attacks with SAML response)
- Threat mechanisms (STRIDE)
  - Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege

Is C-Shield PiP™ impeccable? How does it work?

- C-Shield uses Proactive identity Protection (PiP™) strategy
- Most secure, practical, and less expensive solution to implement
- Proactive strategy means access to resources is always locked
- Authenticator plays pivotal (pro)active role
- Prevents MFA Fatigue by 99.999999999998%. No account lockouts.
- Besides infinitesimal MFA Fatigue, C-Shield is impeccable, i.e., 100% secure
- Easier, faster, secure SSO solution for web apps compared to SAML-based
- Varied implementation options provide different levels of security to the most impeccable while all options thwart/discourage hacking attempts right away. Options for zero-code and easy integration.
- Uses protocol-based security which is most practical and secure

Is C-Shield PiP™ impeccable? How does it work?

- C-Shield uses your phone as a physical dongle
  - Authenticator app runs on user's phone acting as a dongle
  - All authorized resources are connected to user's dongle
- C-Shield Authenticator app itself is highly secure
  - Uses user biometrics (Face ID) as 1st factor and app credentials as 2nd factor
  - Uses Inference, Possession, Knowledge, Proximity, and Time factors
- C-Shield protects resources so only authorized users can access, STRIDE-proof
  - Locks authorized resources to user account, user's dongle, user's biometrics, dongle passcode, and authenticator credentials so only authorized can access
- Quantum-resistant or post quantum security
  - Encryption is modified making quantum-resistant, or does away with encryption and passkeys

C-Shied Authenticator Components

- C-Shield Admin Portal Deployment
  - ✓ On-premise
  - ✓ Cloud
- C-Shield Service Deployment
  - ✓ On-premise
  - ✓ Cloud
- External Authenticator, App-based (PiP™)
  - ✓ iOS
  - ✓ Android
- On-device Authenticator, Browser-based (FIDO2, WebAuthn)
  - ✓ Chrome
  - ✓ Safari
  - ✓ Edge
  - ✓ Mozilla

Contact

- ✓ Rama Nalla
- ✓ rnalla@ckayka.com
- ✓ customer.support@ckayka.com
- ✓ Cosmic Kayka L.L.C.
- ✓ www.ckayka.com