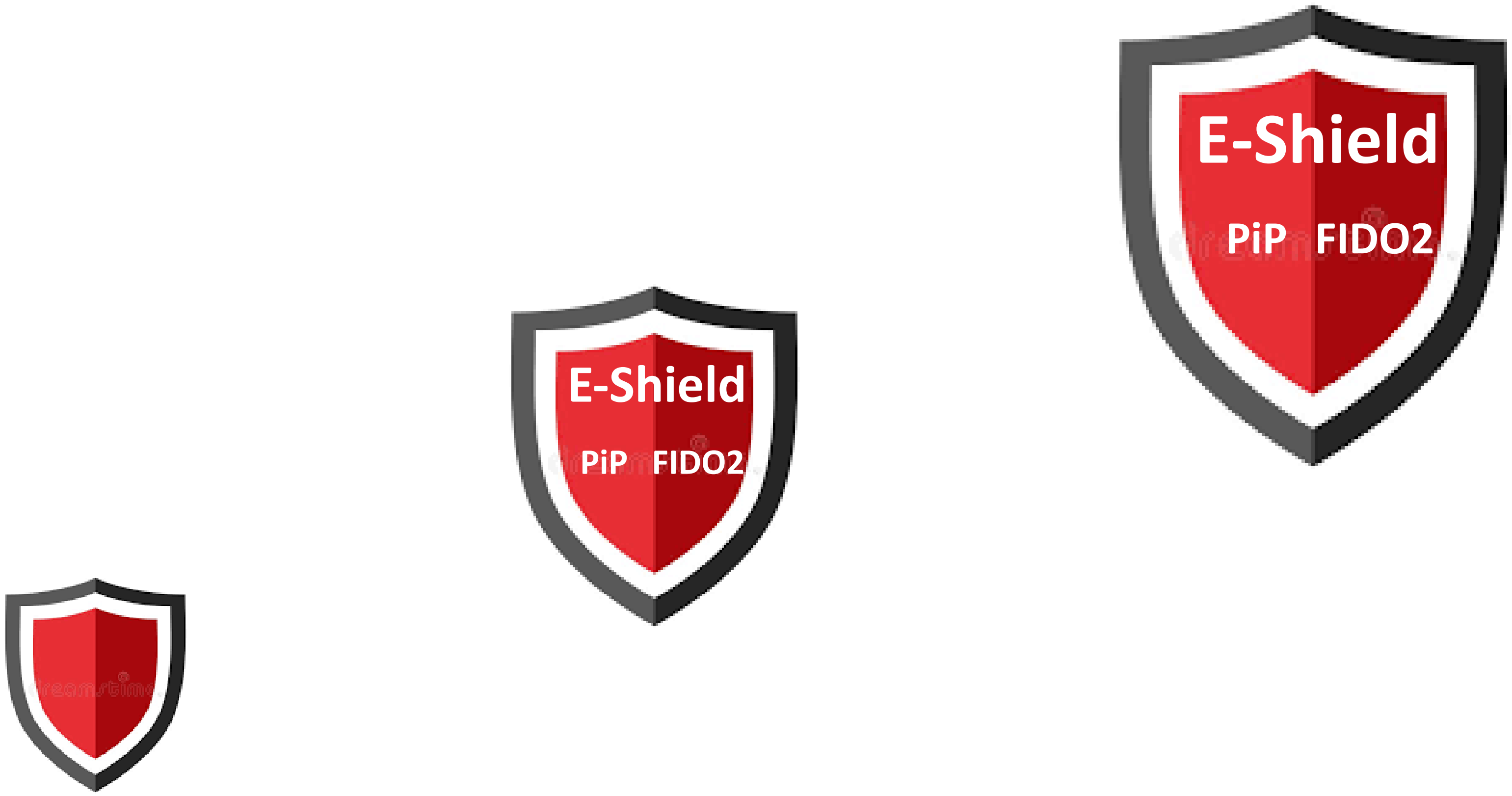
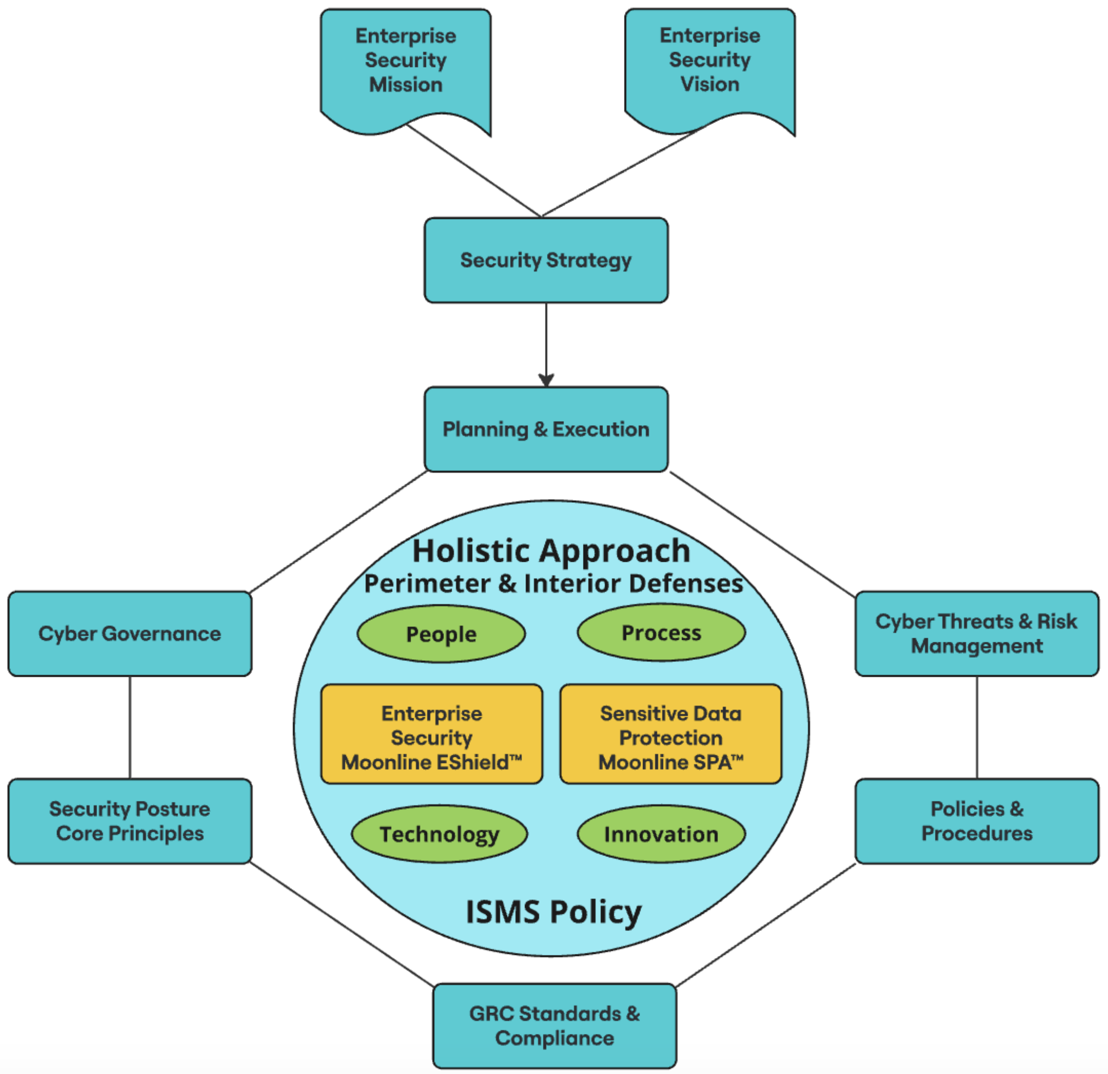
E-Shield™ Proactive Authenticator



Enterprise Cyber Journey



Enterprise Security Mission

Enterprise Security Vision

Security Strategy

Planning & Execution

Holistic Approach

Perimeter & Interior Defenses

People

Process

Enterprise Security Moonline EShield™

Sensitive Data Protection Moonline SPA™

Technology

Innovation

ISMS Policy

Cyber Governance

Security Posture Core Principles

Cyber Threats & Risk Management

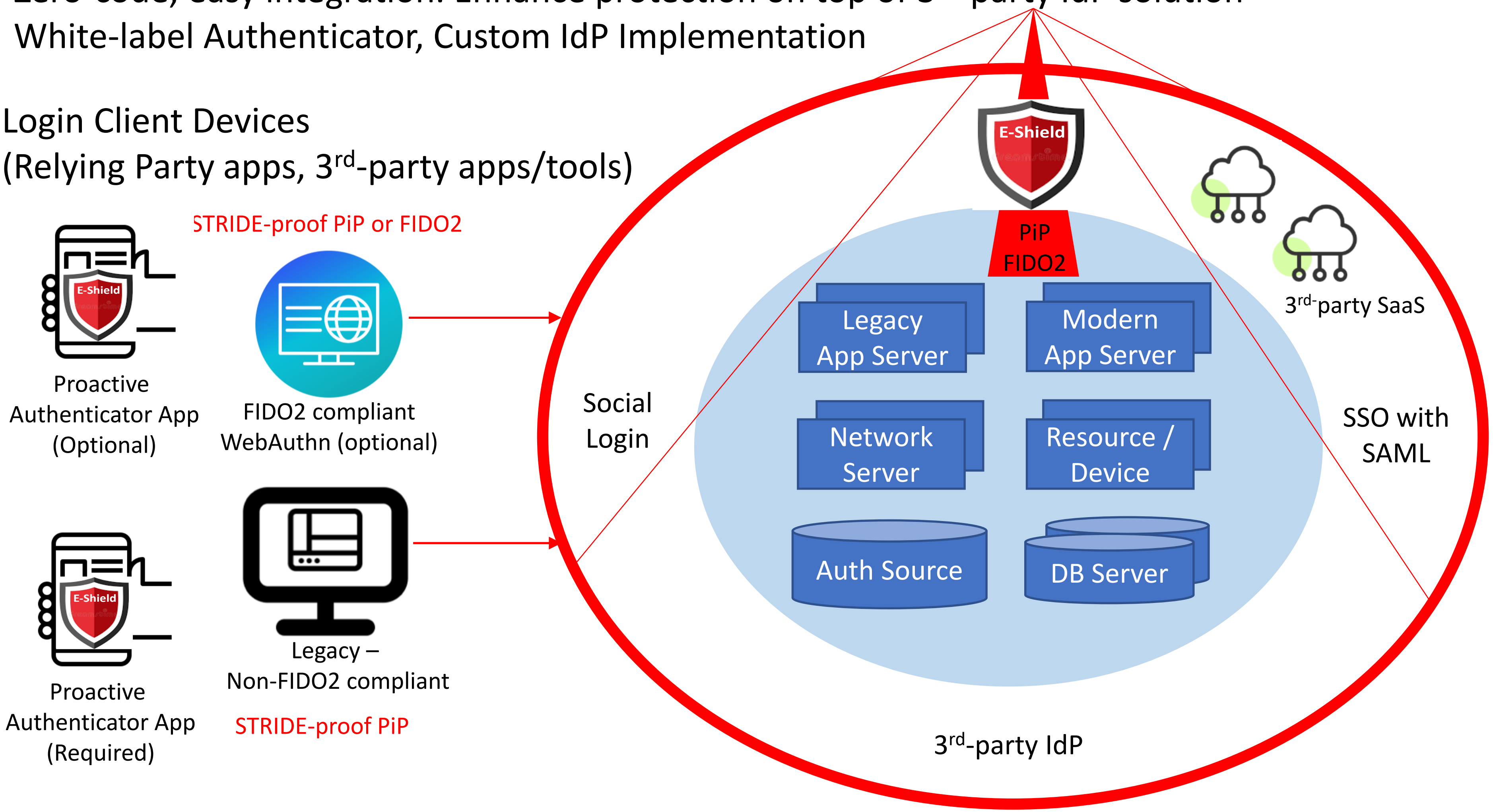
Policies & Procedures

GRC Standards & Compliance

E-Shield™ Proactive Authenticator

- STRIDE-proof Proactive identity Protection (PiP™): **secure and practical** than 2FA, MFA, U2F, 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

Login Client Devices
(Relying Party apps, 3rd-party apps/tools)



STRIDE-proof PiP or FIDO2

Proactive Authenticator App (Optional)

FIDO2 compliant WebAuthn (optional)

Proactive Authenticator App (Required)

Legacy – Non-FIDO2 compliant

STRIDE-proof PiP

© 2024 Cosmic Kayka

Moonline™ EShield™ 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

P - 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 SAML
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 E-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 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	E-Shield Proactive Authenticator	Authenticator Apps (Duo, 2FAS, Okta, Microsoft, Google, Aegis)	FIDO2 Servers (HYPER, etc.)
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 – depends on options selected	Yes	Yes
Protection Coverage	Impeccable, Very High	Medium to High	High
Thwart hacking and DOS attempts	Yes – in all cases	FIDO2 only	FIDO2 only

E-Shied Authenticator Components

- E-Shield Admin Portal Deployment
  - ✓ On-premise
  - ✓ Cloud
- E-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