SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Solution Innovation Case Study:

Eliminating People and Asset Protection Fatigue with One Trusted Biometric Logical and Physical Access Control Assurance Credential

The SEC's Solution Innovation Partner (SIP) program evolved to help security practitioners expedite choosing a trustworthy risk mitigation vendor with confidence given the myriad of viable options in the marketplace. Proven Solution Innovation Practice Case Studies help evaluate performance claims and differentiate security solution providers for business outcomes including risk mitigation, return on investment, and security assurance.

This case study demonstrates Sentry Enterprises Contracting's innovative capabilities in biometric logical and physical security for information systems for its client Phase II Staffing and Contracting, Inc (Phase II). This proven practice was validated by the Security Executive Council and Phase II's end user.

Risk Issues and Mitigation Opportunities:

Phase II is an emerging Small Business Service-Disabled Veteran-Owned Small Business (SDVOSB) that provides solutions and hardware to both government and commercial clients. Almost exclusively comprised of veterans and military spouses, Phase II provides cutting-edge technology solutions that improve efficiency and reduce complexity for its government customers.

Many employees of Phase II were burdened by having to carry multiple credentials to access IT systems and physical security installations. Complying with federal cyber security requirements, its own network required multiple password and PIN changes every year, which presented users with challenges and created credential fatigue. Using a single sophisticated and converged authentication token of any kind would allow Phase II to provide a compelling and innovative solution to government customers, improve its own cyber security, and increase employee productivity.

Solution Requirements:

- Phase II had to improve security efficiency for its Microsoft 365-based enterprise for its internal operations.
- Affordable and robust compatibility with standard Microsoft infrastructure, Phase II's existing physical security systems as well as client (US government) facilities was imperative.
- Employees/contractors needed to be authenticated/ identified within 1 second and in the least intrusive manner.
- No private information could be stored in the cloud or on Phase II's servers, protecting the privacy of Phase II and its key government clients.
- Comply with Executive Order 14028, NIST-compliant authentication standards.

SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Solution Innovation Case Study:
Eliminating People and Asset Protection Fatigue with One Trusted Biometric Logical and Physical Access Control Assurance Credential

Delivered:

- Phase II evaluated other solutions based on its extensive experience with smart cards (CAC/PIV) and determined that an innovative modern identity and authentication capability would be less complex, more secure, and easier to implement.
- Phase II implemented Sentry Card FIDO2 tokens with HID EV2 technology for password less computer access and physical security solutions. This solution was fully compliant with Executive Order 14028.
- Phase II was impressed by Sentry Enterprises' commitment to security by design, open standards such as FIDO2, and the cards lightweight and editable form factor.
- Phase II comprehensively secured its Microsoft 365 solution and access security systems at client facilities.
- Novel use cases were also identified for the biometric FIDO2 card solution by utilizing its extensive contacts within the federal government, particularly the Department of Defense.
- Phase II is now offering a private-label version of the Sentry Card, which they call the Sentinel Card. Phase II's expertise in government cyber security requirements, transparent GSA pricing, and a proven track record of outstanding customer service will complement Sentry's technology expertise.

Outcome and Benefits of Service Including ROI:

- Phase II increased its security posture confidence from a 7 out of 10 to a 10 out of 10 by eliminating password phishing opportunities and password and PIN changes.
- Reduced log-in and password change complexity has allowed the company to regain 100+ hours per employee per year.
- Saved its customers thousands of dollars in security system upgrades by ensuring that only Phase II personnel could access required areas and were biometrically identified.
- Reduced privacy concerns while achieving efficiency and enhanced security by eliminating any biometric data that could be stored off-card.
- Gained experience integrating Sentry Card (and Sentinel) into the information technology infrastructure of a customer, improving the ability to provide value to them.

End user quote – “Forget about zero trust, we now have absolute trust.”

SIP Case Study Authentication Process

This process was overseen by a Security Executive Council subject matter expert with 20+ years of experience in developing and leading people and asset protection programs as trusted security advisor for global, multinational organizations. Client end-user authenticated **March 2023 by the Security Executive Council.**

Note: *The Security Executive Council's Solution Innovation case study represent a snapshot in time to demonstrate a solution to a specific organization's issue. End-user diligence, trial and measurement are strongly recommended for any contemplated risk mitigation activity.*

SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Solution Innovation Case Study:
Eliminating People and Asset Protection Fatigue with One Trusted Biometric Logical and Physical Access Control Assurance Credential

A General Comparison of Competition

Client Service/Resource Attributes or Capabilities	Sentry Card	Common Badge	FIDO FOBS	Mobile Devices
Convenient and Portable	YES	YES	YES	YES
Easy to Use	YES	YES	YES	YES
Hardware & Software Security Configurations	YES	NO	YES	YES
66% Less Costly Than Current High Security Options	YES	NO	NO	NO
Disconnected from a Network/Internet	YES	YES	YES	NO
No Cameras or Recording Devices	YES	YES	YES	YES
Multi-function/Supports Custom Apps	YES	NO	NO	NO
Decentralized Security Architecture	YES	NO	NO	NO
Highest Levels of Security	YES	NO	NO	NO
Solely Biometric (No PINs or Passwords)	YES	NO	NO	NO
Permanent Biometric Bond to Holder	YES	NO	NO	NO
Tamper Proof	YES	NO	NO	NO
No Charging or External Power Required	YES	YES	NO	NO

See other case studies and learn more about the SIP Program here:
https://www.securityexecutivecouncil.com/solutions/vendor-innovations