Absolute Trust

with SentryCard®

Thank you for downloading this Sentry's data sheet. Carahsoft is the master government aggregator and distributor for Sentry's solutions available via SEWP, The Quilt, NASPO, and other contract vehicles.

To learn how to take the next step toward acquiring Sentry's solutions, please check out the following resources and information:

For additional resources:
carah.io/sentry-enterprises

For upcoming events:
carah.io/sentry-enterprises

For additional Sentry solutions:
carah.io/sentry-solutions

For additional cybersecurity solutions:
carah.io/sentry-solutions

To set up a meeting:
Sentryenterprises@Carahsoft.com
844-214-4790

To purchase, check out the contract vehicles available for procurement:
carah.io/sentry-contracts

For more information, contact Carahsoft or our reseller partners:
SentryEnterprises@carahsoft.com | 844-214-4790

Absolute Trust

with SentryCard®

WITH SENTRYCARD, ORGANIZATIONS CAN QUICKLY & SEAMLESSLY:

Harness biometric multi-factor authentication for physical entry, logical access, and a whole lot more.

Biometric Logical Access

Biometric Physical Access

Passive Proximity Detection

SENTRY

Multi-factor codes are NOT proof of identity!

UNIQUE

SentryCard is the first open-architected biometric platform of its kind; self-contained and disconnected from any network, server, or software, making it undiscoverable.

PRIVACY-DRIVEN

The biometrics are enrolled, stored and matched solely within the SentryCard, alleviating a broad range of privacy concerns, including GDPR & BIPA.

LEADING-EDGE

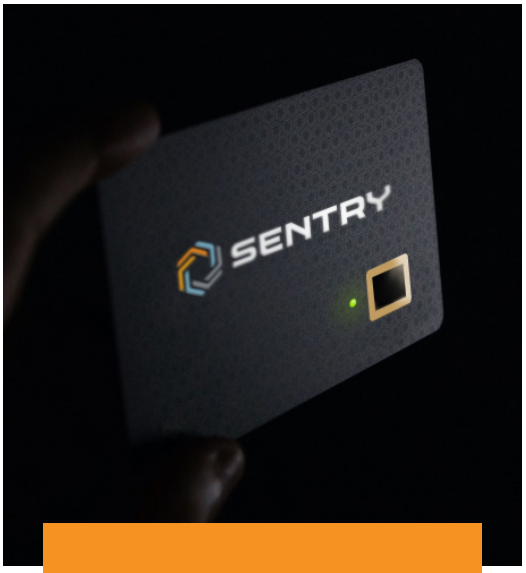
SentryCard is now equipped with FIDO2 security keys, an unphishable standards-based passwordless authentication method. (FIPS 140.2 Certification pending).

COMPATIBLE

SentryCard integrates with all leading industry platforms and readers; eliminating the need to rip and replace existing infrastructure, while being easily phased-in.

CONVERGED

SentryCard was built to address the requirements of Information and Operational Technology, as well as Physical Security; providing multi-factor biometric proof-of-identity for building and systems access.



SentryCard is designed for organizations seeking an indisputable assurance of who is entering their facilities, accessing their computers and devices or logging into their websites.

SENTRY
Identification Without Question.

Leveraging the SentryCard Platform

and its multiple use cases

BIOMETRIC LOGICAL ACCESS

SentryCard biometric authentication quickly provides indisputable proof-positive identification for every computer and server login, whether on-site or working remotely. When used in conjunction with FIDO2, or any third-party logical software, SentryCard provides the path to a zero trust architecture. SentryCard enables your organizations move to a passwordless future, reducing the risks of phishing scams and keyboard logging. Eliminate the high cost of your Password Reset Helpdesk!

BIOMETRIC PHYSICAL ACCESS

SentryCard can work in conjunction with existing physical access control infrastructure, replacing standalone biometric solutions. SentryCard and its data is undiscoverable until the user is biometrically authenticated, protecting the privacy of the user and the potential liability to the organization.

PASSIVE PROXIMITY DETECTION

With embedded UHF technology, SentryCard can be leveraged to track the location of the credential holder while they are in the office. That's critical when determining who is inside in the event of a mandatory evacuation. Importantly, in the COVID era, it enables organizations to implement contact tracing and determine how the illness might spread in the unfortunate occurrence of an outbreak. That can be the difference between a site-wide quarantine or targeted quarantining of only the individuals who were exposed.

Sampling of supported technology platforms

Azure Active Directory

Microsoft 365

digitalPersona.

VERIDIUM

PingIdentity

okta

IBM Security

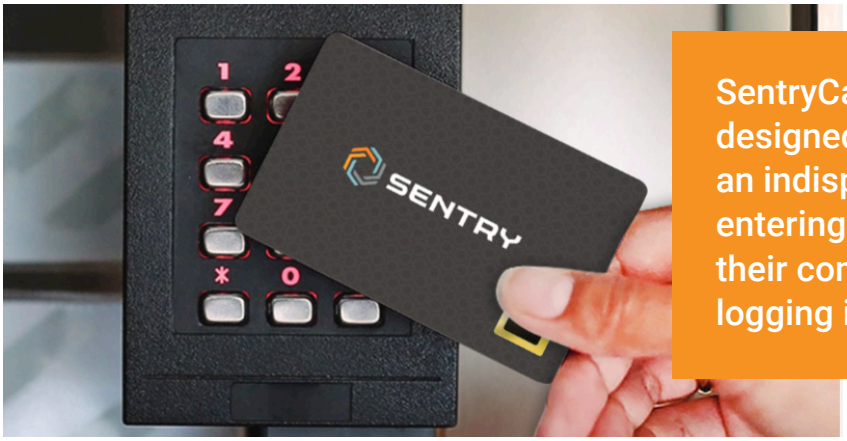
citrix

Google

SENTRY

Identification Without Question.

SentryCard Is Absolutely Compatible



SentryCard is a biometric platform designed for organizations seeking an indisputable assurance of who is entering their facilities, accessing their computers and devices or logging into their websites.

SentryCard is universally compatible with existing infrastructure—no need to rip and replace!

	Sentry Enterprises **Biometric Proximity**	Sentry Enterprises **Biometric iClass**	Sentry Enterprises **Biometric SEOS**	Sentry Enterprises **Biometric EV2/FIDO2**	Sentry Enterprises **Biometric EV2/FIDO2 non-biometric proximity**
Enroll biometrics on card	●	●	●	●	●
Biometric Data Encrypted AES256 and Security Key	●	●	●	●	●
Enrollment of two different fingers	●	●	●	●	●
FIDO2				●	●
Compatible with Passwordless software & computer login	●	●	●	●	●
Reader Compatibility					
Proximity	●			●	●
iClass		●		●	●
SEOS			●	●	●
EV2				●	●
LEAF EV2				●	●
LEGIC EV2				●	●
Des/Fire/MiFare EV2				●	●

Sample of Compatibility with Access Control Systems. No additional software, API or Integrations Required.

Genetec · LENEL·S2 · Software House · Honeywell · openpath · brivo

SENTRY
Identification Without Question.

SentryCard: Addressing Privacy Concerns

The protection of biometric data is of paramount importance. Any breach exposing this ultra-sensitive personal data poses significant risks and liabilities to the organization as well as to the affected person.

In order to keep organizations accountable, several U.S. States have passed legislation regarding the collection, storage and use of biometric data. Internationally, the E.U.'s General Data Protection Rights (GDPR) legislation, along with the rules in the UK and India provide a strong stance on biometric data protection and the associated liabilities.

The potential liabilities for the mishandling of biometric data are considerable. Illinois' Biometric Information Privacy Act (BIPA) is viewed as the most rigorous, imposing a $1,000 to $5,000 penalty for each violation, per employee, until remedied. In 2018–19, over 200 BIPA lawsuits were filed targeting employers utilizing biometric technology in the workplace.

> **"Utilizing the SentryCard will demonstrate to regulators your commitment to protecting your employee's sensitive biometric information."**
>
> **David Ross**
> **Chief Privacy Officer**
> **GreyCastle Security**

Sentry Enterprises is committed to having a Data Processing Agreement (DPA) in place with each of its resellers by mid-2021.

KEY PRIVACY ATTRIBUTES: The SentryCard eliminates most of the risks associated with using biometric authentication by removing all human access to the biometric data.

1. **DECENTRALIZED:** Biometric data is enrolled, stored and matched solely within the SentryCard platform, never touching an external database or server. With SentryCard there is no large "honeypot" of biometric data for hackers to pursue.
2. **UNIQUE:** Each SentryCard generates its own unique inaccessible encryption key used to protect the biometric data stored within the card.
3. **NON-TRANSFERABLE:** The SentryCard is a single-use solution. Once a person's biometrics are enrolled only that person can ever use the credential.
4. **CONTROLLED:** Once issued, the holder maintains control of their biometric data, stored securely within the credential.
5. **IRRETRIEVABLE:** Enrollment of the holder's biometrics are one-way and irreversible once set. The credential's only output is an affirmative or negative authentication.

SENTRY
Identification Without Question.

Can You Afford Not to Use The SentryCard?

An immediate ROI while increasing security, mitigating risk and reducing complexity.

REDUCTION CATEGORY	AVERAGE COMPANY SPEND	BUSINESS OUTCOME
Eliminate secondary multi-factor authentication, i.e. soft and hard tokens.	$40 per employee annually plus token cost.	Sentry Payback: **Just over 18 months.**
Significant reduction in Helpdesk Support.	1.2 helpdesk interactions per year at $70 per employee.	Sentry Payback: **Less than 12 months.**
Eliminate password and phishing training.	$75 per employee annually.	Sentry Payback: **Immediate** as SentryCard eliminates the need to use usernames and passwords for logical access.
Eliminate the need to upgrade or replace existing readers or add new biometric devices.	$3,000 to upgrade existing readers or $7,500 to install new readers and infrastructure.	Sentry Payback: **Immediate** as Sentry credentials automatically turn existing readers into biometric readers.
Eliminate internal IT cost for servers and support for a biometric software solutions.	$50,000–$100,000 annually per server.	Sentry Payback: **Immediate** as biometrics are enrolled, stored and matched on the SentryCard. No databases, servers or workstations required.
Eliminate the risks associated with the storing employee biometric data.	$10,000 fine per instance for GDPR violations related to the mishandling of biometric data.	Sentry Payback: **Immediate** as biometrics are enrolled, stored and matched on the SentryCard. No databases, servers or workstations required.

The SentryCard will “plug & play” with your existing infrastructure to provide a secure and touchless solution while addressing today’s hygiene and privacy concerns.

SENTRY
Identification Without Question.

Absolute Trust

with SentryCard®

SENTRY

To learn more: info@sentryenterprises.com