Valmistettu Ruotsissa

Mousetrapper®

Mousetrapper Core Protect

Kehitetty ympäristöihin, joissa vaaditaan erityisen korkeaa turvallisuustasoa – Core Protect on rakennettu samalla testatulla alustalla kuin myydyin tuotteemme Advance 2.0+ ja tarjoaa saman luotettavan toiminnallisuuden ja ergonomian, mutta siinä on lisäksi ylimääräinen tietoturvakerros soveltumaan organisaatioihin, joissa tietoturva on ratkaisevan tärkeää.

Core Protectin edut

Core Protect on rakennettu samalle testatulle alustalle kuin myydyin tuotteemme Advance 2.0+ ja tarjoaa saman luotettavan toiminnallisuuden ja ergonomian, mutta siinä on ylimääräinen tietoturvakerros sopimaan organisaatioihin, joissa tietoturva on ratkaisevan tärkeää. Tuote on kehitetty tiiviissä yhteistyössä johtavien turvallisuusluokitelluissa ja arkaluonteisissa ympäristöissä toimivien toimijoiden kanssa, ja se on mukautettu heidän korkeiden vaatimustensa täyttämiseksi.

Core Protect on varustettu kaksinkertaisesti salatuilla muistoilla, ja fraasimuisteja on poistettu, mikä tarkoittaa, että valmiita tekstijonoja ei voi syöttää tai tallentaa laitteeseen. Tämä luo tiukan ja kontrolloidun konfigurointiympäristön, joka täyttää korkeat turvallisuusvaatimukset.

Kahdeksan painiketta antaa useita mahdollisuuksia mukauttaa Mousetrapper juuri haluamallasi tavalla. Painikkeiden toimintojen muuttaminen onnistuu helposti selainpohjaisen MT Keys -ohjelmiston avulla.

Tiedot

- Leveys: 480 mm
- Korkeus: 20 mm
- Syvyys: 110 mm
- Paino: 715 g
- Tuotenumero: MT124

Avainominaisuudet

- Erittäin ohut ergonominen muotoilu
- Ohjausalusta, jossa klikkaus- ja vieritystoiminto
- Kaksinkertaisesti salatut muistot ja fraasimuisti poistettuna vastaamaan korkeimpia turvallisuusvaatimuksia
- 8 ohjelmoitavaa painiketta, jotka voidaan helposti mukauttaa MT Keys -ohjelmiston avulla
- Valmistettu kierrätysmuovista
- Vaihdettavat rannetuet, jotka voidaan puhdistaa pintadesinfiointiaineilla
- Säädettävä korkeus taitettavalla kitkapohjalla
- 2400 dpi

Technical Security Overview

Core Protect is engineered for deployment in high-assurance

environments where strict security
controls, minimized attack surface, and deterministic behavior are required. The device architecture
is intentionally constrained to eliminate non-essential functionality and reduce exploitable vectors.

Security Architecture

1. Layered Encryption Model: Implements double encrypted memories to protect data integrity and
confidentiality across operations.
2. Dedicated Cryptographic Domain: Separate memory secured with independent key
(AES-CBC-128).
3. Key Isolation: Unique cryptographic keys per memory segment prevent lateral compromise.

Memory & System Segmentation

1. Firmware and configuration stored in physically/logically separated memory areas where Firmware and configuration are stored.
2. Independent key management per memory block.

Data Handling Policy

1. No Persistent Text Storage: Phrase memory functionality removed entirely.
2. No capability to store, cache, or replay sensitive input.

Compliance & Deployment Context

1. Suitable for classified and regulated environments.
2. Supports strict IT governance and security policies.
3. Designed for defence, avionics, government, and critical infrastructure.
4. The firmware can be upgraded to ensure it remains equally capable over time.