DEEP SECURE

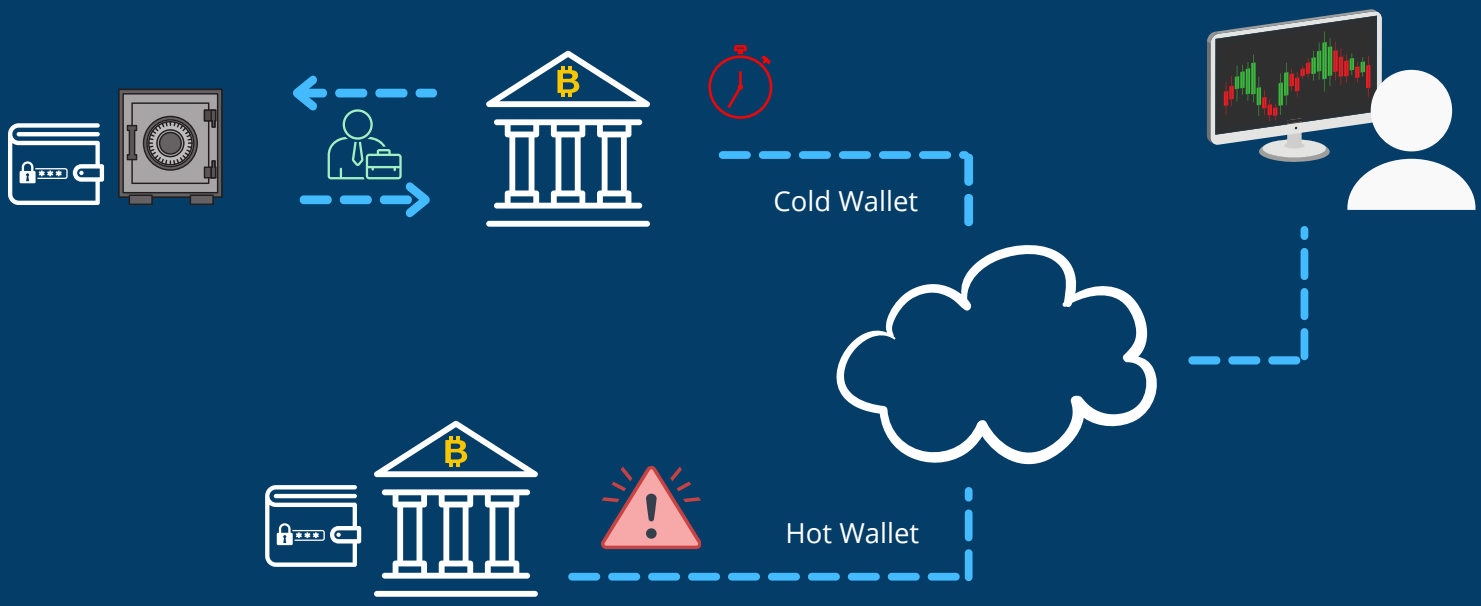
Protecting Crypto Assets

Threat protection for cryptocurrency exchange applications, custodians and networks

WWW.DEEP-SECURE.COM | INFO@DEEP-SECURE.COM

Protecting Crypto Assets

Traditional banks and other organizations offer crypto custody services to safeguard their customers' cryptocurrency assets using both hot and cold wallets.



Traditionally, organisations offering crypto custodian services have stored wallets offline from the Internet in an air-gapped vault to protect them from attack.

The best solution is a hot wallet that can be protected from the internet. Some solutions use diodes to achieve this, in order to protect valuable keys being stolen. However, diodes do not allow the 2-way communications required and ultimately do not defend against attacks concealed in data.

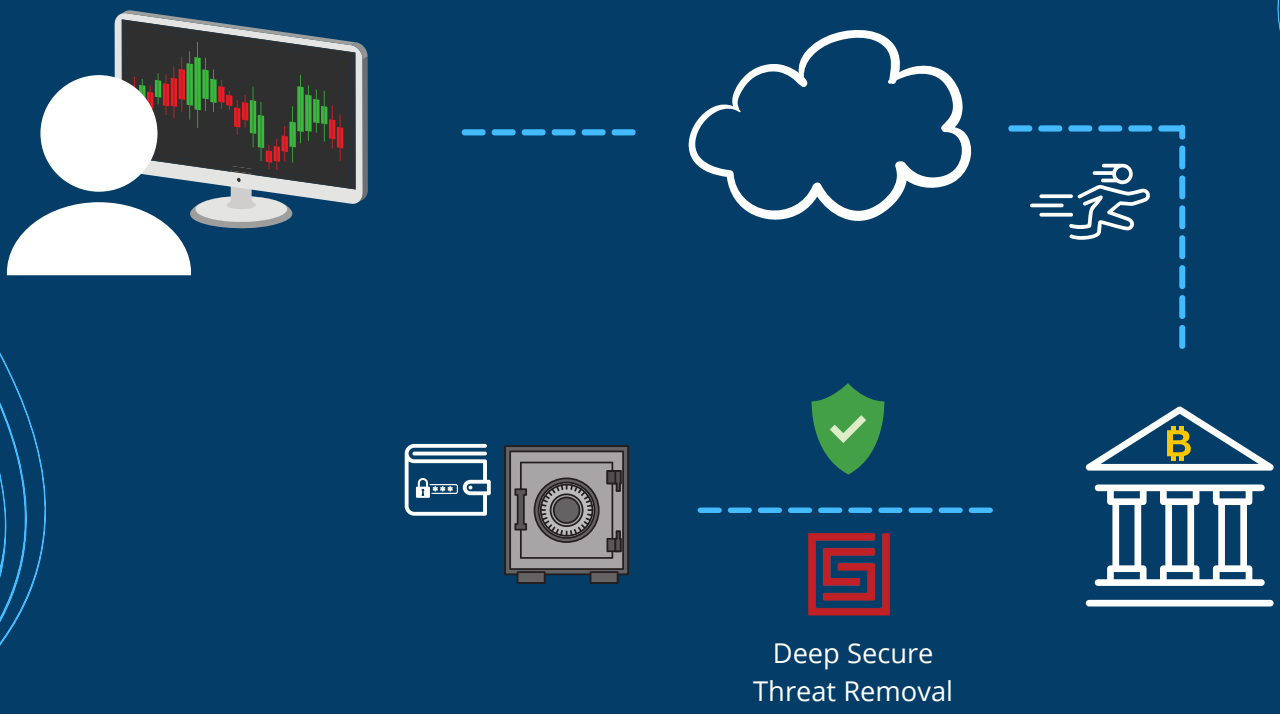
Hot wallets offer the best flexibility since they can be used immediately and so customers can take advantage of exchange rate fluctuations and the need to access funds quickly but are open to attack from the connected networks.

Cold wallets offer the best security since they are disconnected from the Internet and so not open to attack but require time consuming procedures to gain access.

Protecting Crypto Assets

The Solution for Maximum Protection

Deep Secure has innovated crypto asset protection, enabling the functionality of a hot wallet with the security of a cold wallet.



Deep Secure Threat Removal enables an HSM to be used to protect cryptocurrency assets whilst giving it online access for instant transactions.

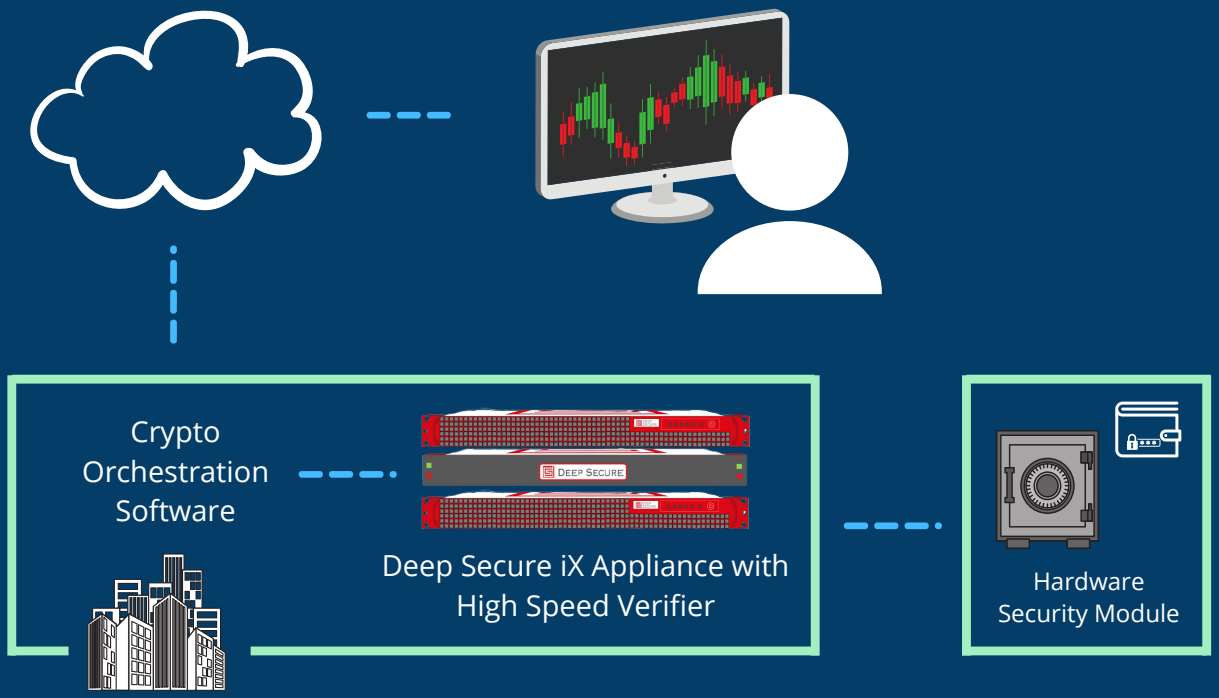
Threat Removal uses hardware-based verification to ensure all interactions with the HSM are safe and do not contain malware designed to compromise the wallets

Delivering all the convenience of a hot wallet with the security of a cold wallet

Protecting Crypto Assets

Deployment

Deep Secure iX Appliance with High-Speed Verifier (HSV) deployed as a physical on-premise appliance constrains the interface to the HSM using verification in hardware logic to ensure the HSM only receives safe, valid data to prevent a malware attack.



Threat Removal ensures the traffic flowing into an HSM does not contain any malware. The original data presented from an untrusted source is never delivered.

The information is extracted from it and used to create safe, new data to send to the HSM. The data is verified in hardware logic to ensure it is safe to deliver.

- ✓ Threat Removal ensures no malware reaches the HSM
- ✓ Hardware only High-Speed Verifier removes reliance on software
- ✓ Supports standards based crypto transaction protocols including HTTPS, JSON & Protocol Buffers
- ✓ Scales out with additional iX appliances to meet demand
- ✓ Flexible license model - Perpetual, Term, Subscription

Protecting Crypto Assets

Deep Secure Threat Removal For Crypto-Security

Threat Removal for Crypto-Security is a combined hardware and software solution, because of this it provides the following features and benefits:

Feature	Benefit
Supports standard crypto transaction protocols. (HTTPs, JSON, Protocol Buffers)	Easy to integrate into the custodian infrastructure.
Uses separate uni-directional links for inbound and outbound application traffic.	Prevents cross-contamination, ensures the outbound channel cannot be used as a backlink into the wallet.
Supports bi-directional application traffic.	Easy to integrate into the custodian infrastructure.
Enforces inbound and outbound protocol breaks.	Minimises the attack surface by ensuring network-level traffic cannot travel “end-to-end” over the air gap.
Checks transaction data against pre-defined schemas on either side of the air gap.	Prevents attacks concealed in transaction data from crossing the air gap.
Verifies transaction data is correctly structured in hardware FPGAs.	Creates an incredibly small attack surface. Hardware logic cannot be remotely manipulated or compromised.

Protecting Crypto Assets

Threat Removal For Crypto-Security - High Speed Verifier

Deep Secure's High Speed Verifier (HSV) uses hardware logic (FPGAs) to verify the data passing across the air gap. As the HSV is hardware, it cannot be compromised by an attacker.

	Single Diode	JSON/XML Gateway with diodes	Threat Removal
Supports bi-directional communication	✗	✓	✓
Supports native application protocols	✗	✓	✓
Defends against attacks concealed in data	✗	✗	✓
Verifies data is safe in hardware logic	✗	✗	✓

Ease of Integration

Threat Removal for Crypto-Security supports standard crypto transaction protocols so it can be dropped inline into the existing infrastructure without the need for costly development or re-design.

Designed in line with the UK National Cyber Security Centre's guidance on best practice for protecting high-risk systems. Deep Secure is actively working with banks and financial institutions to implement Threat Removal for Crypto-security, providing the most secure link imaginable.

DEEP SECURE

Crypto-Security

Threat protection for cryptocurrency exchange applications, custodians and networks

www.deep-secure.com
info@deep-secure.com
+44 (0)1684 892831