

INTRODUCING

Threat Removal Plus

cross domain security that can't
be beaten


Threat Removal Plus

INTRODUCTION

Threat Removal Plus is a combined software & hardware solution. That can be used for:

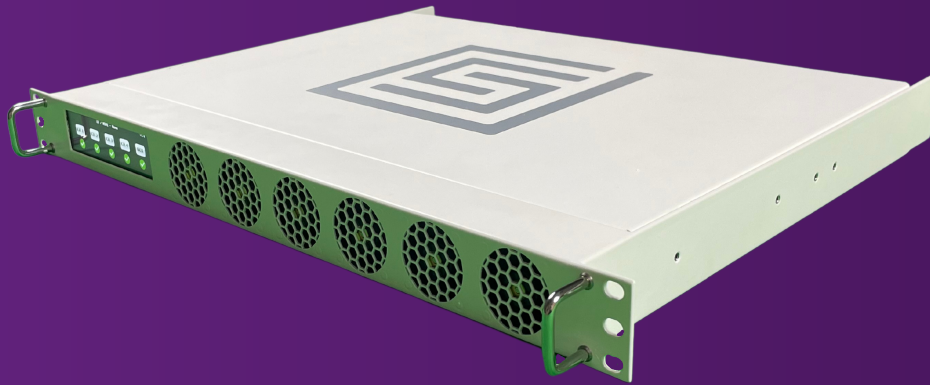
- Securing cross domain **file sharing**, file transfer & file import.
- Securing cross domain **web services** & web applications.
- Securing cross domain **Command & Control (C2)** data.
- Securing cross domain **instant messaging**.



 Combat the threat of inbound malware

Threat Removal Plus

HIGH SPEED VERIFIER



The High Speed Verifier (HSV) uses hardware logic (FPGAs) to verify the data passing across the air gap. Because this is performed via hardware **it cannot be compromised by an attacker.**

	Diode	Cross Domain Guard	Threat Removal Plus
Supports bi-directional communication	X	✓	✓
Supports native application protocols	X	✓	✓
Uses transformation to ensure attacks cannot cross the air gap	X	X	✓
Verifies data is safe in hardware logic	X	X	✓

Don't risk your data with insufficient security

Threat Removal Plus

TECHNICAL SPECIFICATIONS



..... ● Bi-directional Verifier

..... ● Dual Power Supplies

..... ● 3 Network Interfaces
- Low
- High
- Management

..... ● 3 FPGAs

..... ● Up to 4 Cards in 1U

..... ● 1 Security Processor

..... ● 3 Network Processors

Threat Removal Plus

FEATURES & BENEFITS

Feature	Benefit
Compact form factor with support for virtualised proxies	Easy to install and configure
Front panel status display with remote firmware updates	Easy to manage
Supports bi-directional application traffic	Easy to integrate into existing infrastructure
Supports standard protocols	(Deep Secure file sharing protocols, HTTPs, JSON, Protocol Buffers)
Uses separate uni-directional links for inbound & outbound traffic	Prevents cross-contamination, ensures the outbound channel cannot be used as a backlink into the trusted network
Enforces inbound and outbound protocol breaks	Minimises the attack surface by ensuring network-level traffic cannot travel "end-to-end" over the air gap
Ensures none of the original data is allowed to cross the electronic air gap. transforming it, rendering it threat-free	Prevents malware concealed in everyday office files & attacks concealed in data from crossing the air gap.
Verifies that everything crossing the electronic air gap is correctly structures using hardware FPGAs	Creates an incredibly small attack surface. Hardware logic cannot be remotely manipulated or compromised
Tamper detection	Enhanced physical security

Threat Removal Plus

HARDWARE-ENFORCED ZERO-TRUST
SECURITY

Request a demo

+44 (0)203 950 5116

contact-us@deep-secure.com

www.deep-secure.com/contact-us