Secure Endpoints

Cybersecurity
BIOS-SHIELD®

◀ BIOS-SHIELD® L100
(Laptop version)

▼ BIOS-SHIELD® D100 (Desktop version)

Performs seamless network isolation and eliminates insider threats

Secure Endpoint series provides security at users' convenience through virtualisation to isolate the OS and strengthen security at the firmware level to guard against cyber exploitations. It allows users to work in both trusted (Intranet) and untrusted (Internet) environments securely without compromising productivity. The SECURE BROWSER enables users to freely browse the internet and safely screenshot and move graphics, photos and PDF files without the fear of importing malicious code.

It is complemented by CLOUD MANAGEMENT SYSTEM to empower IT administration capabilities.

Key Features

Enhanced endpoint protection

- Secure Browser blocks malicious websites and enables users to use the internet, safely screenshot and move graphics, photos and PDF files without the fear of importing malicious code.

Stronger protection with fast file restoration

- Data Encryption: It has hard drive encryption to protect data from both malicious insiders and hackers.
- Time Machine Restoration: Users can save a point-in-time "snapshot" of their hard drive. Should the user encounter a virus or malware attack, users can select a previous snapshot and initiate a rollback to quickly recover their corrupted or missing data.
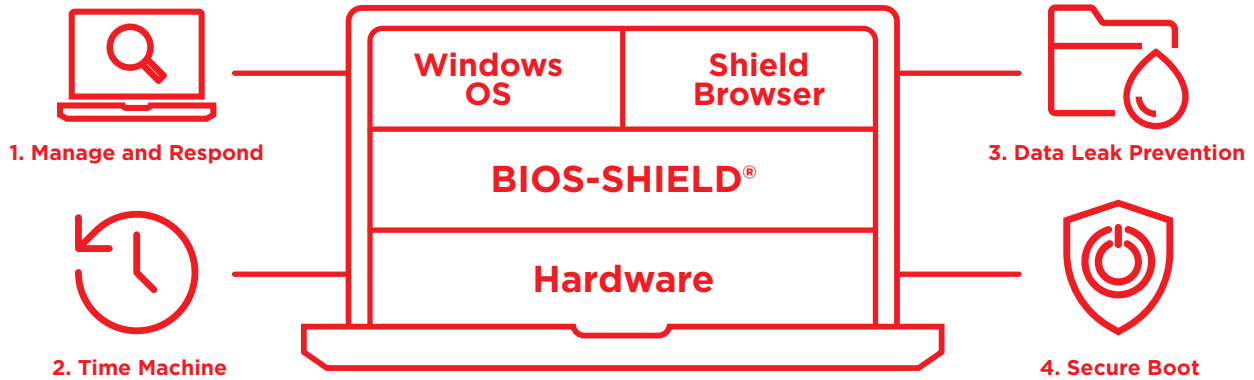
Take control of your endpoints

- Reset Windows®: Administrators can revert PC state to previous backup "golden" OS image.
- Cloud Management: Administrators can remotely force a reboot or a shutdown to limit access to the corporate network. Should a user lose a PC, administrators can remotely disable it.

Prevent unauthorized access

- USB encryption limits access so that data can only be read on a pre-authorized PC. Should a USB thumb drive go missing, the data is encrypted and cannot be read in any unauthorized device. Administrators can disable storage devices.
- Disable networking devices and printers to prevent unauthorized data leakage while allowing audio/video devices so that user can access video calling.

ST Engineering

Deployment Use Cases

1. Manage and Respond

2. Time Machine

Windows OS | **Shield Browser**

BIOS-SHIELD®

Hardware

3. Data Leak Prevention

4. Secure Boot

Specifications

BIOS-SHIELD® L100 (Laptop Version)

Processor	8th Generation Intel® Core™ i7-8550U
Memory	16GB
Storage Drive (NVMe)	512GB
Integrated Graphics	Intel® UHD Graphics 620
Operating System	Windows 10 Pro
Weight	~1.1kg
Display	13.3" Full HD (1920x1080)
Audio	Built-In Speaker Combo headphone output
Connectivity	1x Ethernet LAN 1x Wireless LAN (802.11a/b/g/n/ac)
Interfaces	1x USB 3.0 with Charge 2x USB 3.0 1x HDMI 1x VGA
Battery	Built-In Lithium Polymer

BIOS-SHIELD® D100 (Desktop Version)

Processor	8th Generation Intel® Core™ i5-8500
Memory	8GB DDR4 RAM
Storage (SATA SSD)	256GB
Integrated Graphics	Intel® HD Graphics 530
Graphics Card	nVidia GT1030
Operating System	Windows 10 Pro
Dimensions (W x D x H)	280mm x 305mm x 102mm
Form Factor	Small Desktop
Audio	Built-In Speaker Mic In, Speaker Out, Line In
Connectivity	1x Ethernet LAN
Interfaces	4x USB 3.0 2x USB 2.0 1x HDMI, 1x DP, 1x VGA (Integrated) 1x HDMI, 1x DP (Graphics Card)

www.stengg.com/cybersecurity
cybersecurity@stengg.com