



TAFASHIELD

TAFAMANAGED SECURITY SERVICES

Future-Proof Endpoint Security

For years, endpoint security products' primary threat protection was based on signatures, created after patient zeros were impacted and the damage already done. Assuming all attacks had been seen before, using signatures made sense. Today, malware mutates daily, even hourly, making signature-based prevention tools obsolete, and creating the need for a stronger prevention-based approach to endpoint security.

Tafa Shield security services are powered by BlackBerry® intelligent security, which provides an AI-driven, automated, prevention-first approach to endpoint protection. BlackBerry® technology delivers the detection and prevention capabilities needed to stay ahead of attackers, keeping the business secure. It is an accurate, efficient, and effective solution for preventing advanced persistent threats and malware from executing on an organization's endpoints. Tafa Shield is cloud-enabled and can be deployed on premise, or in a hybrid form for advance desktop and mobile protection.

Features

True Zero-Day Prevention



Resilient AI model prevents zero-day payloads from executing

Device usage Policy Enforcement



Controls which devices can be used in the environment, eliminating external devices as a possible attack vector

AI-Driven Malware Prevention



Field-proven AI inspects any application attempting to execute on an endpoint before it executes

Memory Exploitation Detection and Prevention



Proactively identifies malicious use of memory (fileless attacks) with immediate automated prevention responses

Script Management



Maintains full control of when and where scripts are run in the environment

Application Control for Fixed-Function Devices



Ensures fixed-function devices are in a pristine state continuously, eliminating the drift that occurs with unmanaged devices.

Capabilities

Device Usage Policy Enforcement

- Control use of USB mass storage devices
- Prevent data theft via removable media

Role-Based Access Controls (RBAC)

- Minimize risk with more granular role management with custom RBAC
- Improve restrictions to network access based on the roles of individual users
- Limit employee access rights to only the information they need to do their jobs
- Benefit from no impact on existing users

Application Control

- Lock down fixed-function devices
- Prevent bad binaries or modification of a binary
- Lock down specified systems and restrict any changes

Script Control

- Stop unauthorized scripts from running
- Benefit from granular whitelisting and safelist capabilities
- Support MacOS®, Microsoft®, and Linux®
- Prevent execution of PowerShell one-liners







IOS® Sideloaded Application Detection

- Sideload applications are immediately scanned and detected

WHY SHOULD YOU MAKE THE SWITCH?

The algorithmic model utilized within Tafa Shield means there are no signatures, patching, system scans, or slow endpoints due to the security solution running on them. Customers who have made the switch from reactive legacy, signature-based antivirus products have seen up to a 99% ROI, a 97% reduction in the re-imaging of machines, extended hardware and battery performance, and a 90% reduction in staff hours required to manage the solution.

What we do

 <p>Rely on AI & Machine Learning</p>	 <p>Analyze malware at the DNA-level</p>	 <p>Advanced Threat Prevention</p>
 <p>Minimal Updates</p>	 <p>Work on air-grapped networks</p>	 <p>Predict & prevent</p>

What others do

 <p>Rely on Human classifications</p>	 <p>Require on-premise infrastructure</p>	 <p>Wait for threats to execute</p>
 <p>Require constant updates</p>	 <p>Signatures</p>	 <p>Heuristics</p>
 <p>Behavioral analysis</p>	 <p>Micro-virtualization</p>	 <p>Sandboxing</p>

Tafa Shield Add-on Services

01

External IT Vulnerability Assessment

Testing is performed in a 'Black box' method with no information about the services or servers provided to the test team; only confirmation of the external IP Addresses are provided. This most closely replicates threats to the organization from a malicious attacker, who would have the same information as the test team.

02

Internal IT Vulnerability

Testing internal systems will determine the level of threat to an organisation that a malicious attacker, an employee, or contractor, who has gained access to internal systems, may pose to the systems and data. The aim is to examine the security of all server's OS, applications, wireless security, segregation of restricted data, VLAN and firewall rulesets.

03

Wireless Penetration Testing

A wireless penetration test will examine security of all nominated wireless points and check for data leakage and security level. This will test the reliability of the organization's wireless network and is aimed to prevent a cyber-attack.

04

Web Application Penetration Testing

A full test on the nominated websites including OWASP most common vulnerabilities. This test employs different software testing techniques to find "security bugs" in server/client applications belonging to the organization from the Internet.

05

IoT Security Assessment and Penetration testing

A full test on critical infrastructure and IOT devices to detect vulnerabilities and examine the effectiveness of security measures in place. This is to fortify critical infrastructure and prevent malicious attacks on IOT devices.

06

Managed SOC Services

A subscription-based managed Tafa Shield threat hunting, detection and response service that merges the BlackBerry® AI cybersecurity platform with 24x7 support from best-in-class incident responders and prevention experts.