Island

Balance Business Group

Self Protecting Browser | Overview

The Enterprise Browser offers enterprise users a meaningful security improvement over consumer browsers. Not because those browsers are insecure, but because their security model is focused on consumer usage patterns. Island goes further with the *Self Protecting Browser* that protects against a wide range of threat modes, both external and local.

For organizations who need to protect sensitive applications and data — even when accessed on unmanaged or BYOD devices — the Enterprise Browser offers a unique security model. Consumer browsers operate under a model where the device and local user is always trusted, leaving the door open to data leakage or insider threats. Island adds unique innovations that protect the browser footprint and adds policy controls for how data is allowed to move within or outside the browser. This gives the Enterprise Browser an active role in enterprise security.

Innovative Self-Protection in a Natural Browsing Experience

External Threat Protection

- **MitM Protection** to protect data over the network from interception
- **Attack Surface Reduction** to disable JIT & browser APIs for untrusted sites
- **Extension Guard** to govern browser extensions and disable extensions for sensitive applications
- **Safe Browsing** protects against phishing, malware, and risky content

Local Threat Protection

- **Tamper Prevention** to detect & report tampering and disable browser
- **Encryption of Browser Stores** to protect passwords, cookies, cache
- **Keystroke Logging Prevention** to disarm malicious keystroke loggers
- **Hardened Browser Policy** to protect settings and disable developer tools
- **Process, Memory, and File Protection** to protect local resources. This is enhanced with the *SPM Driver*

Application & Data Protection

- **Last-Mile Controls** to govern data movement by policy
- **Screen Capture Controls** to govern screen recording by policy
- **Device Posture Assessment** to enforce local device security settings
- **Browser Enforcement** to require application access via Island
- **Complete visibility** of browser activity to aid in incident response and security researchers

Consumer Browsers

The web browser was born as a passive application to render HTML documents over the network. Over time, it's gained massively powerful capabilities to become an application platform. Legacy security solutions attempt to protect the web browser externally — the Enterprise Browser applies a *secure by design* approach by adding security controls to the browser itself.

Consumer browsers are generally good at protecting against web-based threats, but do not protect local resources from insider threats or malware like keyloggers.

Interested in learning more?

Check out our website to learn more about our solutions, and be sure to check our "Industry News" page for up-to-date reports of ransomware attacks and more.

Website: https://www.bbg-mn.com

SPM Driver for Windows

Every Island user benefits from the wide range of protections outlined above. For organizations with particularly sensitive data where maximum protection from insiders and APTs is needed, Island offers the **SPM Driver**. This is a Windows kernel driver that prevents advanced attacks on the endpoint itself. If a malicious attacker attempts to inject a DLL, dump system memory, or manipulate OS-level APIs to circumvent Island protections, the SPM detects and defends the browser. No other process on the system is allowed to obtain a handle to the Island Enterprise Browser and any attempt to load a library is blocked unless it's signed by Island, Microsoft, or Google.

Once the Enterprise Browser is configured to use the SPM Driver, any attempt to disable or disrupt communication between the browser and the SPM Driver will immediately cause the browser to log out and shut itself down. Island administrators can install the SPM along with the initial browser installation, or require existing users to install the SPM Driver by policy.