DATA SHEET

Isla® Web Malware Isolation System

The Enterprise Malware Problem

The web browser is the most strategically important application in today's Internet-powered enterprise. But the browser is inherently insecure, and has become the #1 vector for cyber attacks on your organization.

Benefits to Your Organization

- Stops browser-borne malware
- Simplifies endpoint security complexity
- Simplifies SSL administration
- Reduces risk of business disruption
- Saves money on forensics and remediation
- Empowers your employees with web freedom.

The power of the web browser is that it provides employees with access to virtually any content on the Internet, which can be invaluable for both personal and business productivity. But the browser also provides a clear path for cyber criminals to deposit targeted, undetectable malware on endpoint devices and launch stealth attacks on internal business resources to cause significant disruption to operations and reputation.

The conventional method of stopping these threats is to deploy various detection-based security technologies outside the gateway, in the network, or at the endpoint to hopefully identify and block any potentially malicious activity. But cyber attacks continue to become more advanced, more complex, and often completely undetectable. Gone are the days when a gateway security appliance or endpoint AV product could simply match a threat against its database of attack signatures. Sandboxes and micro VMs on the endpoint are an improvement, but they introduce unnecessary deployment complexity and still carry the risk of malware escaping endpoint containers.

Browser vendors have made sincere, continuous efforts to resolve some of their vulnerabilities. But more patches means more code, which also increases the already-massive attack surface and provides a bigger target for hackers. In addition, flash, Java and other browser plug-ins further increase browser vulnerabilities. Finally, human behavior can never be controlled when it comes to web browsing, and all it takes is one "click" on a bad web link to initiate an attack on your business.

Isla Web Malware Isolation

The only way to eliminate all browser-borne malware from the enterprise is to shift the focus from malware detection – which can never be 100% accurate - to malware isolation - which literally prevents all rendered web content (and all web malware) from entering the corporate network. This is the strategy employed in the innovative Isla Web Malware Isolation system.

Isla (Spanish for island) physically separates and isolates the web browser - and all potential web malware - on its own "island" (a specialized Isla appliance) deployed in the DMZ outside your network. To access web content, users inside your network can continue to use their favorite commercial browser, or a lightweight Isla client viewer (which behaves just like a browser). In either case, these browsers are connected to the external Isla appliance, rather than being connected directly to the Internet.

Users request web content through their browsers as they normally would. But with Isla, the appliance first authenticates and encrypts each user connection, then launches a private, hardware-isolated VM for each user session. Isla fetches and renders all web content securely inside each user's VM, then applies patent-pending technology to instantly and continuously transform all content (audio, video, text, and graphics) into a benign, malware-free format that is delivered to internal users.

Isla works with all major browsers across all major platforms, including Windows, OSX, and Linux. This includes protection for mobile users working off-premise on IOS, and Android smart phones or tablets.

Isla is an ideal solution for virtually any organization because it meets and exceeds business requirements for security, performance, and scalability. Each of these is summarized below.

- **Security** – Isla is built with Spikes Security's patent-pending AirGap isolation technology, which integrates multiple levels of protection and isolation. For example, the browser is physically isolated from the end user on a specialized server that is running only the browser and a hardened Security-Enhanced Linux OS – no other applications or sensitive business data are on the appliance. All end user browser sessions are fully encrypted and executed in individual isolated VMs, which are automatically destroyed after each session. If malware does enter a VM on Isla, it finds only a very small, isolated browser attack surface, with no access to network resources, and no ability to deliver its payload to the end user device or other systems on your secure network. In short, malware has nowhere to go and is automatically destroyed when the VM session is ended.
- **Performance** – If not properly designed, remote browsing technology can suffer from high latency and low performance. But the engineering team at Spikes Security has architected Isla to deliver the same end user experience and performance as traditional desktop browsers. To accomplish this, all the "heavy lifting" in terms of processing web requests is done on the appliance. The content presented to the end user then leverages intelligent compression algorithms that automatically sense content type to ensure maximum performance and minimum latency. The result is an elegant end user experience with no significant latency – this is true even for bandwidth-intensive audio and video content. The appliances themselves can be deployed in active/active high availability configuration to ensure non-stop performance for all users.
- **Scalability** – The Isla client-server architecture makes it easy to deploy appliances, add users, and rapidly scale capacity based on the needs and growth of the customer organization. Spikes Security offers Isla models with various web session capacities, and all can scale linearly across multiple locations while being managed as a single system. And because Isla web content integrates transparently into all major commercial browsers (across all platforms including mobile devices), there is no need for time-consuming endpoint administration or installation of complex endpoint software.

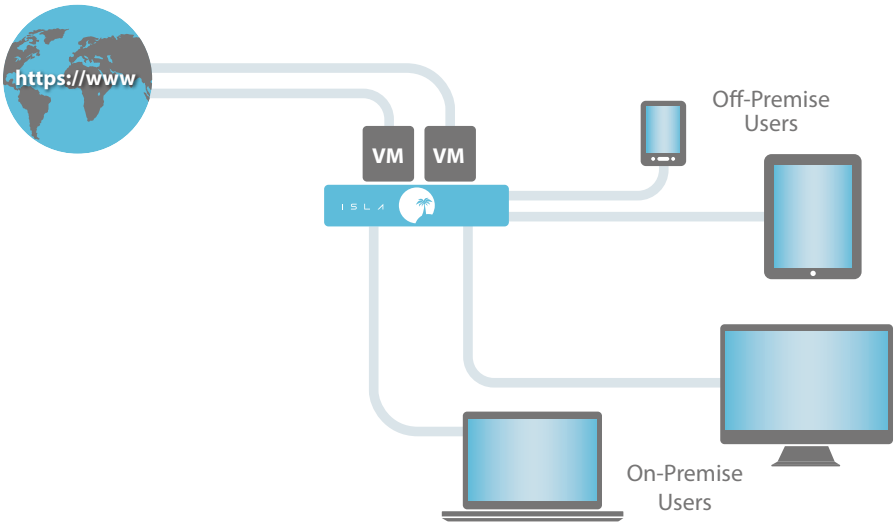
Benefits to Your Organization

The Isla solution delivers tremendous value throughout the enterprise. Here are five key benefits.

1. **Stops browser-borne malware.** Isla isolates and eliminates the #1 threat vector for malware attacks on the enterprise – regardless of whether the malware is a known threat, a complex APT, or a new, previously unknown zero-day attack. It will never penetrate the network or infect end user devices, regardless of where they are working.
2. **Simplifies endpoint security complexity.** Because browser-borne malware will never reach the end user device, desktop managers don't have to worry about deploying complex desktop sandboxes and micro VM technologies in an effort to contain and control complex attacks. Also, Isla eliminates the need to deploy potentially vulnerable plug-ins (such as Java, Flash or QuickTime) on endpoint devices to be able to browse the web. These plug-ins now run on the Isla appliance.
3. **Simplifies SSL administration.** With SSL tunnels increasingly being used for malware delivery, IT organizations wrestle with decisions to decrypt and inspect all SSL connections, or respect employee privacy. With Isla, the problem is eliminated because all connections are terminated on the appliance, and no embedded SSL malware ever gains access to internal networks.
4. **Reduces risk of business disruption.** By isolating the browser and eliminating the primary threat vector for malware, Isla customers reduce their risk of being victims of successful attacks by cyber criminals. Reduced attack risk means there is also far

less risk of disruption to operations, lost user productivity, theft of confidential data, or damage to brand reputation.

5. **Saves money on forensics and remediation.** According to Gartner, the average IT cost for laptop remediation is $653 every time a device is infected by malware. In addition, according to a 2015 Ponemon report sponsored by Spikes Security, the average organizational cost of a data breach as a result of a web-based malware attack is estimated at $3.1 million. By eliminating browser-borne malware, Isla helps companies avoid these unnecessary costs.



6. **Empowers your employees with web freedom.** When Isla is deployed, there is no longer a reason to be concerned about employees visiting web sites – even trusted web sites – that may have been infected by malware. With Isla, malware will never penetrate the network or infect endpoints. So employees can safely and fearlessly embrace the full power of the web, without the need for restrictive Internet controls or policies. Isla also allows easy access to internal applications or other specific trusted sites that may require direct browser access.

Network Integration and Deployment Options

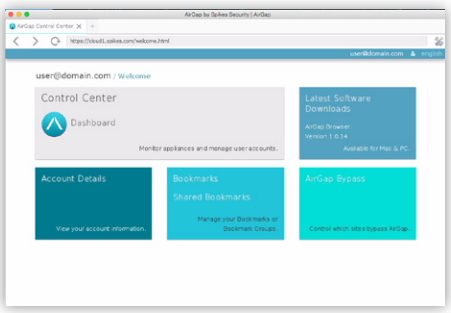
Network agnostic – Any network topology or existing security infrastructure can coexist with the Isla solution. Existing layers of security systems simply serve to improve the overall security, though upstream malware filters may be deemed unnecessary.

Multi-site deployment – Deploying Isla across multiple locations is not a problem, and can be beneficial to traveling/remote users because they can automatically be routed to the nearest Isla appliance to ensure optimal performance and highest security.

Isla Control Center

The Isla solution includes the Isla Control Center, which provides IT security managers with the tools required for fast deployment and management of Isla appliances across the enterprise. Key administrator tools include the following:

- **Reporting** – Intuitive dashboard displays reports on browsing activity, various security events and alarms, and top trends in users and groups.
- **System performance management** – Quickly provision new users or interoperate with your existing user authentication tools; measure and manage system performance across your enterprise; easily see gaps in coverage; monitor resource utilization and plan for growth.
- **Single pane of glass** – All enterprise controls are in one place, with reporting that helps guide policy decisions for customers that require more granular controls. Configuration and health alerts are also controlled centrally.



Secure browser connections – All connections and data streams between user devices and the Isla appliance are protected using advanced 256-bit AES encryption and authenticated using PKI.

Integration with SWG – Customers can deploy Isla with their existing secure web gateway, allowing Isla to secure all browser content, while enabling the SWG to handle DLP and URL filtering processes that may be required for compliance reasons.

Intrusion prevention – Because the Isla browser is the only application on its server, sensitive tripwires immediately identify any unexpected behavior, terminate the VM and all malware, and provide users with a clean session.

Isla System Requirements and Specifications

Isla Client for Windows
32-bit and 64-bit Windows XP/Vista/7/8/10
Intel 500 MHz Pentium class processor or better
30MB of available disk storage; 250MB of available memory

Isla Client for Mac
MAC OS X 10.7 or higher
Intel Core Duo class processor or better
30MB of available disk storage; 250MB of available memory

Ilsa Client for Linux
Check with Sales representative for all Linux versions supported
30MB of available disk storage; 250MB of available memory

Isla Appliance Model SAS-1030	
Rated Capacity	90 concurrent sessions (typical usage)
Chassis Form Factor	1U, rack mounted
Chassis Dimensions	1.75" x 16.93" x 27.95"
Chassis Weight	40 lbs (18.4kg)
Rack Rails Included	Yes
Required Ethernet Ports	1 x 10/100/1000 mbps
Power Supply	750W AC
Power Supply Type	110-220 AC
# of Power Supplies	2
Redundant Fans	Yes
Redundant Power	Yes

Isla Appliance Model SAS-4030	
Rated Capacity	360 concurrent sessions (typical usage)
Chassis Form Factor	2U, rack mounted
Chassis Dimensions	3.47" x 17.25" x 28.50
Chassis Weight	85 lbs (38.6kg)
Rack Rails Included	Yes
Required Ethernet Ports	4 x 10/100/1000 mbps
Power Supply	2000W AC
Power Supply Type	110-220 AC
# of Power Supplies	2
Redundant Fans	Yes
Redundant Power	Yes

Customer Support

Standard customer support is available during normal business hours, 8am – 6pm PT. Please consult your Spikes Security sales representative if you require a customized support program.

For more information on the innovative Isla web malware isolation system – or to arrange a demo or trial for your organization – please call or contact us at (855) 287-7453 or sales@spikes.com.

Spikes Security, 536 N. Santa Cruz Ave., Los Gatos, CA 95030 | Tel: +1 855-287-7453 | Email: sales@spikes.com | www.spikes.com