Isla® Q&A

General

What is Isla?

Isla is an innovative, enterprise-class web malware isolation system that prevents all browser-borne malware from penetrating corporate networks and infecting endpoint devices. Isla delivers this by rendering all web content on a specialized appliance deployed outside the corporate firewall, then presenting all text, graphics, audio, and video in a benign, malware-free format.

To access the web, users inside the network can use their normal browser or a dedicated Isla client viewer. In either case, they communicate directly with the Isla appliance instead of the Internet. The appliance processes all web content requests within an isolated VM created for each user session, then transforms the requested web content into a benign format and delivers it to the endpoint devices connected to the Isla appliance.

Any malware contained in the original web content remains isolated in the VM and is automatically destroyed when the session ends. The result is complete protection against all web malware attacks.

I already have a strong security infrastructure. Why do I need Isla?

Each year, businesses worldwide collectively spend billions of dollars to create a strong, multi-layer security architecture that includes firewalls, secure web gateways, network AV, content analysis engines, endpoint software, and more.

The problem is that all of these products rely on some form of detection technology to determine if web content is safe or not. Advanced targeted attacks are becoming increasingly undetectable – even if suspicious traffic is executed in a sandbox - ,which makes all of these products increasingly ineffective. They, of course, cannot detect what is undetectable. For that reason, IT organizations are now integrating isolation technology into their security architecture as a means to prevent all web malware attacks.

In addition, today's strong infrastructure does not guarantee security in the future. There must be acknowledgment of trends defining the state of information security. These trends include:

- Sophistication of attacks will keep improving, especially APT and zero-day exploits
- Network breaches are not stopped by the continuous additional layers of legacy security technologies
- Cyber criminals will increasingly target web browsers, as they are un-securable

Isla plays an important role in protecting businesses because it is a gateway appliance that isolates the web browser and stops web content from infecting endpoint devices and your network. Isolation technology is innovative and is designed to shut down the #1 threat vector for cyber attacks on the enterprise—browser-borne malware.

Why should I use isolation technology to secure my existing browser?

The web browser is the most strategically important application in today's Internet-powered enterprise. But the browser is inherently insecure, and a target for cyber attacks on the enterprise. It has become impossible to secure. Add to this the fact that web malware is increasingly undetectable, and you have the requirement for browser isolation. The question to focus on, given today's security environment, is: why would you want to trust browsers running on endpoints in your enterprise?

Isolating the browser eliminates a primary attack vector and lowers cyber attack risk. Web browsers were never designed to be security tools. Although browser vendors continue to deliver security enhancements to their browsing platforms (with sandboxing, virus detection, etc.), the fact remains that every desktop browser has a large attack surface loaded with vulnerabilities that can be easily exploited.

Adding browser plug-ins such as Java, Flash, Silverlight, etc., makes these browsing platforms even more vulnerable to attacks. By isolating the browser from the endpoint, you completely eliminate that attack vector.

Can Isla protect my existing browsers?

Yes. Isla works seamlessly with all major browsers – Firefox, Chrome, Safari, and IE.

Who are your current customers including names and sizes?

Our customers span all major vertical markets, including financial services, healthcare, legal, media & entertainment, government, and more. These customers range in scale from a few dozen users to several thousand users. Our customers are very concerned about their security and privacy. As such, we don't publicly identify them or provide specific information about their deployments. Spikes Security does have references. Please contact our sales organization for more details.

How does Isla detect malware?

Isla is designed to isolate all web malware delivered through the browser. As such, Isolation technology does not need to detect malware. It treats all web content as a potential threat and stops it from gaining access to endpoint devices or entering your network.

How does Isla work remotely, for example, from a Home Office?

Does Isla work in the cloud?

Isla can be set up to be accessible from both inside and outside the network. Remote users can be secured globally via normal VPN connections, enabling them to be directed through the appliance and out to the Internet. Future versions of Isla will be optimized for cloud deployments.

How is the browser on the Isla appliance isolated?
What prevents it from being attacked?

Isla is physically isolated outside the secure network in the DMZ. Isla is deployed on a specialized appliance that uses a security-hardened version of Linux and incorporates hardware-assisted VM isolation for each user session, plus active monitoring with sensitive tripwires that instantly identifies and terminates any suspicious activity, which could be malware.

Isla's built with patent-pending AirGap isolation technology that provides multiple layers of protection, separation, and isolation. These components work together to make it virtually impossible for any web malware to compromise Isla appliances, the network, or endpoint devices.

In addition, Isla uses a fast, efficient, and secure Type 1 hypervisor to automatically create and launch each user session within a VM using hardware-assisted isolation leveraging Intel-VT extensions. Each user VM is isolated from other Isla users and from snooping by IT administrators.

Memory, disk, and CPU resources are not shared between users, thus preventing any form of malicious activity or even cross-contamination between user sessions. Once a user terminates a session, that VM is destroyed along with any stored data, session cookies, or residual data.

Does Isla prevent malware intrusion everywhere on the network?

No. Isla is focused on preventing all web malware delivered through web browsers, which represents the #1 threat vector for cyber attacks on the enterprise.

Other forms of cyber attacks are outside the control of an Isla solution. These include:

- Industrial espionage
- Password theft
- Email phishing attacks (through non web-based email clients)
- USB drives and accessories
- User misconduct
- Unsafe BYOD practices

Why is Isla a better solution than a form of web proxy?

Spikes Security provides network-level, browser malware isolation through its patent-pending AirGap isolation technology. This breakthrough technology has been integrated into the Isla family of security appliances, which are deployed in the DMZ. Isolation provides a level of security greater than that of a web proxy.

One very important difference between Isla and proxies like secure web gateways is that a web proxy does not transform content to stop dangerous malware from reaching the endpoint where it increases the risk of a breach. In addition, a proxy (or secure web gateway) is based on detection technology, which is susceptible to allowing zero-day malware into the network undetected. It also allows direct connection of all endpoints to the Internet.

Isla literally transforms the content requested by a user into a benign format. The transformed content is delivered back to the end user in an optimized, encrypted, and proprietary channel that is unrecognizable and unusable by malware. As a result, all data streams carrying requested content are automatically cleansed making it impossible for potentially malicious payloads, to reach any end user device.

Our environment includes compliance requirements such as HIPAA, FIPS, and more.

Is Isla vetted to adhere to compliance requirements?

We are working to gain FIPS certification. HIPAA's requirements are to ensure encryption of patient's records, and we absolutely meet these requirements. Spikes Security is happy to work with customers to ensure that we fit into their auditing architecture making sure encryption is maintained and any data transiting the system is secure while connected to Isla.

What items on the SANS critical security controls list does Isla handle?

While nothing can address all aspects of individual controls, Isla can be a part of your solutions within several of the SANS critical security controls including items 5, 11, 13, 14, and 17. Much of this will depend on how fully you enable the use of Isla within your organization.

What is the maximum number of open tab sessions?

Isla is tested with up to 125 open tabs in one browser.

Does Isla scale for large enterprises? How many users can it support?

Isla appliances are available in multiple capacity configurations – from 90 concurrent web sessions to 1,800. In addition, these appliances can scale linearly to support any number of users, across multiple locations. The entire deployment can be controlled as one system through our Control Center.

Which platforms can run Isla client?

The Isla client is currently supported on Windows, Mac OSX, and several Linux platforms. Consult your Isla sales representative for specific versions and latest additions to client support.

How is your solution priced?

Isla is a combination hardware/software solution. Pricing is based on number and capacity of the hardware appliance, plus annual licenses for Control Center management and customer support. Please contact sales for a pricing proposal by using the Contact form on our web site.

How would Isla protect against phishing via email?

If the email contains a malicious web link, which the user clicks on, Isla would isolate the malware outside the network as usual. However, if the email contains a malicious file opened by the end user, the IT organization would apply their security controls as needed.

Can I configure Isla for a high availability infrastructure?

Yes. Isla is HA capable. The appliance can be deployed in a paired, high-availability configuration with automatic failover for non-stop reliability.

Compatibility

Does Isla work with any type of browser plug-in?

The browser on the Isla appliance supports most major plug-ins, including Flash, Java, QuickTime, and Adobe Reader

Does Isla work with secure web gateways (SWGs) – such as BlueCoat or Websense?

The Isla appliance can sit in-line behind SWGs to ensure all web malware remains isolated outside the network. The SWG complements Isla by handling DLP, URL filtering, and content control functions.

How does Isla support BYOD devices?

Isla supports a BYOD policy by offering full protection from Web malware for personal endpoint devices running Windows, MAC, and Linux when they are connected to the Isla appliance. When personal devices are used outside the office for business use, they can connect to the Internet through Isla via a VPN connection.

How does Isla work for documents requiring electronic signatures?

Electronic signature applications like DocuSign are completely compatible with Isla and work seamlessly.

How does Isla handle SSL?

Isla is fully compliant with SSL 2.0 specifications, and established secure SSL connections with all web sites that support SSL.

How does Isla manage user access? Can you use Active Directory or LDAP?

Yes, The Isla Control Center management application is used to initially identify users. That identity can be connected to your Active Directory environment via LDAP when using an internal (private) Control Center.

Can we still limit access to web sites?

Yes. The Isla appliance can sit in-line with typical URL filtering tools to limit access to specific sites.

Can Isla be used to access internal applications and websites?

Isla is designed to support a feature called "Bypass." This feature will automatically launch a traditional browser such as Chrome, Explorer, Firefox, and others when the user needs access to an internal web site not connected to the Isla appliance.

As added security in such cases, the designated bypass browser is configured so that it does not have access to external web sites, and thus prevents external hackers from gaining access to a browser target.

Does Isla Control Center have reporting and logging features?

Yes. Control Center provides logs, usage reports, and metrics.

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