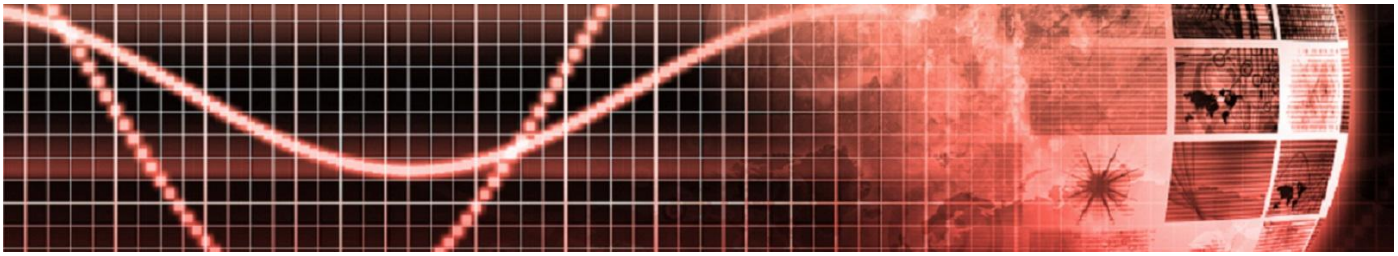
DEEP SECURE



XML Guard

XML is a widely used format for structured data and is excellent for rapid application development and interoperability. It is central to the provision of web services. But the complexity of the XML formats and protocols means targeted attacks can use these services to gain entry and leak information. It also means conventional XML gateways that offer some protection against attack are themselves liable to be attacked and disabled.

- ✓ Block the spread of malware
- ✓ Data loss prevention
- ✓ Hold users accountable
- ✓ Defend against unknown attacks
- ✓ Advanced content verification
- ✓ Safe passage for business information
- ✓ Maximum protection against advanced attacks

The Deep-Secure XML Guard controls XML data entering and leaving the organisation, defending against advanced attacks and misuse. Its self-defending architecture means it can exert the required control without itself becoming vulnerable to attack.

It is used by organisations that need to tightly control web services traffic used for document management, collaboration, billing, e-commerce, inventory, etc. Such organisations could be in government, law enforcement, defence, pharmaceuticals, finance and utilities.

The Guard terminates network connections and extracts the XML requests and responses from them. It verifies the content is acceptable before using a new connection to deliver the data. By acting in this way, as an application level proxy, no vulnerabilities in the internal network are exposed to an attacker. This defends the system against new and unknown attacks and methods of leaking information.

Advanced Content Verification

The Guard does not simply check the XML requests and responses to ensure they are free of attacks and hidden sensitive information. Advanced attacks go to considerable lengths to evade detection, so content checking functionality is liable to miss something.

To counteract this, the XML Guard distils the essence of the XML data, and data in other formats that might be embedded in it, into an intermediate format that is easy to verify. Once the information content has been verified as fit to pass, it is converted back to XML ready for delivery. This process is called transshipment. It means attacks and leaks hidden in the way information is represented are not preserved, so attackers are denied the ability to target applications with malware and to covertly leak information.

In particular, transshipment of XML gives control over the way the delivered XML is encoded. For example, namespace prefixes can be determined, character entities replaced and whitespace normalised. This greatly reduces the variety of data that an application will need to handle, making thorough testing more tractable.

With transshipment, unnecessary or potentially dangerous data is simply discarded. There is no reliance on signatures or anomaly detection, so the Guard will always defend against unknown attacks. For more details on transshipment, see the Transshipment briefing paper.

Controlling XML

Requests and responses can be checked to ensure they are approved forms of XML data. In this way the Guard can prevent applications receiving data they do not expect, which

might cause them to malfunction, or from sending out inappropriate data as a result of some other fault.

It is also possible to ensure responses are properly matched to requests. This protects applications from mishandling data received out of order, and also denies advanced attackers from using otherwise legitimate responses to carry covert messages.

The Guard can be configured to transform XML data as it passes through it. This can be used to change the way data is represented to allow applications to interoperate. Also elements of data that must not be passed can be removed or replaced with dummy data, without needing to modify the original application.

Safe Passage for Business Information

The XML Guard has two network interfaces, one connecting to each network. It terminates connections on one interface and starts new connections on the other. By acting in this way, as a full application layer proxy, and using transshipment to verify the information content of data passing through it, the Guard ensures nothing passes from one system to the other except required business information.

The XML Guard is internally divided into zones so that the relatively complex XML handling code is separated from the security critical content verification code. The zones ensure the effective attack surface of the Guard is very small, and the use of Deep-Secure's patent pending *Ring Architecture* means the Guard can be managed from a single point without degrading zone separation. The result is a self-defending Guard capable of withstanding direct sophisticated attack.

Easy Management

Administrators use a web interface to manage the Guard. A separate network interface can be used for management traffic and administrators can be identified using digital certificates, providing maximum protection against advanced attacks.

The XML Guard integrates into the organisation's security and network management regime, by providing logs using standard protocols. The logs report on the XML traffic passing through the Guard, which allows the monitoring system to correlate activity across the system. Logs also report on administrator activity, allowing administrators to be held to account for their actions.

Protocols

HTTP and HTTPS can be used to send XML requests and receive XML responses. The POST method is used to carry the request in a single MIME part.

Simple XML RPC can be used to send an XML request and receive an XML response. A single TCP connection can carry a sequence of requests and responses, either as a sequence of XML documents or as XML stanzas.

Monitoring information can be sent to the organisation's SEIM using SNMP or syslog.

Platforms

The XML Guard is supplied as an appliance running Deep-Secure's DSOS, which is a stripped down operating system having only those functions necessary for the Guard to function, thereby minimising the attack surface. A number of hardware platforms are supported.

The Deep-Secure LRB is a 19" rack mounted 1U half depth server. This utilises kernel mechanisms to provide internal zoning. Three network interfaces allow for a separate connection to a management network.

The XML Guard is also available under the Iguana Blue brand as a small form factor DIN rail mounted appliance (see www.iguanasecurity.com for details).

The Iguana Blue appliance utilises five physically separate processors to enforce the internal zoning. Three network interfaces allow for a separate connection to a management network.

The XML Guard can also be supplied as a VMWare ESXi virtual machine image. It can also be provided as a set of three virtual machines so virtualisation reinforces the internal zoning.

A one-way XML Guard is provided as a pair of LRB appliances connected by an optical network diode.

Any HTML5 compliant browser can be used to manage the XML Guard.