Forcepoint Chat Guard

Chat is an important collaborative tool for businesses, used both internally and with partners, and increasingly a way of engaging directly with customers. However it provides another channel for cyber threats and misuse.

Key Benefits

- Block the spread of malware
- Prevent data loss
- Stop social engineering attacks
- Defend against unknown attacks
- Hold users accountable
- Verify content
- Self-defending

The Forcepoint Chat Guard controls the use of internet standard chat, to allow your organization to make use of chat without putting sensitive information and critical business processes at risk.

It is used by organizations that need to control external chat traffic, or chat between separate internal zones. Such organizations could be in government, law enforcement, defence, pharmaceuticals, finance and utilities.

The Guard terminates network connections and extracts the underlying 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.

The Guard also offers the firewalling and endpoint authentication functionality typically found in next-generation firewalls, so it can hide internal services and limit communication to trusted chat servers internally and externally.

Safe chat

The Guard controls internet-standard Extensible Messaging and Presence Protocol (XMPP) chat traffic between two servers on different networks. It transforms the representation of the chat messages passing through it in order to eliminate unwanted data and potentially dangerous constructs. By doing this, it protects against attacks that present carefully crafted malformed messages to exploit vulnerabilities and denies an attacker the ability to hide information in otherwise legitimate messages.

The transformation process is called transshipment. The XML stanzas that represent an individual chat message are transformed into Forcepoint's own intermediate data format, XDS, for verification. This is simpler than XML and avoids exposing the Guard itself to vulnerabilities in the XML processing code.

Transshipment does not try to identify an attack. Instead it leaves any malware or control data behind as it extracts the meaningful business information from the chat message. As a result there is no reliance on signatures or anomaly detection and the Guard will always defend against unknown attacks. For more details on transshipment, see the Transshipment briefing paper.

The Guard blocks user and chat room discovery, so internal activity is not disclosed to outsiders, and all forms of file sharing are blocked to prevent the ingress of malware and leaks of sensitive information.

Rich Chat

Even though communication through the Chat Guard is highly secure, users still have a rich experience. It handles rich text messages, so formatting is preserved. User status information is carried so it is possible to see when friends are online and multi-user chat is supported so provide chat rooms for collaborative discussions.

Self-Defense

The Chat 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 Forcepoint'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 Chat Guard integrates into the organization'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

The Chat Guard supports the XMPP Optimized Server to Server protocol. It is typically deployed in conjunction with Isode M-Link chat servers.

Monitoring information can be sent to the organization's SIEM using SNMP or syslog.

Platforms

The Chat Guard is supplied as an appliance running Forcepoint'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 Forcepoint LRB is a 19" rack-mounted 1U half-depth server. This utilizes kernel mechanisms to provide internal zoning. Three network interfaces allow for a separate connection to a management network.

The Chat 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 virtualization reinforces the internal zoning.

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

Request a demo →