ICAP Multi-Protocol Monitoring

PARTNER APPLICATIONS

Overview

Our ICAP Multi-Protocol Monitoring service uses the Internet Content Adaptation Protocol to capture webmail sessions from approved web proxies in order to apply policies on the Sentrion. This eliminates the need to maintain policies on both the web proxy and the Sentrion. And unlike other solutions, our implementation reconstructs the raw webmail payload as actual email, making it much easier to read messages that have been flagged for review.

Audience

Regulated businesses and other companies that need to monitor webmail traffic flows along with email in order to comply with legal mandates and industry best practices regarding data leakage, message content, and acceptable usage.

Key Features and Functionality Overview

By far, the main vector for leakage of private and proprietary data is email. If someone wants to intentionally send restricted information outside the company, it's much easier to send an email than, say, smuggle paper documents past the security guard. But intentional leakage is just a small part of the problem. The most common leaks are unintentional. For example, a product designer intending to work over the weekend may send unencrypted specifications to a home email address. Or an HR officer sending personnel files to a department manager may not notice the email program's auto-complete feature has entered the wrong recipient in the "To" field.

The Sentrion Policy Engine can detect such incidents in the email stream and take action. But when employees use webmail to work from home or on the road, they can make exactly the same mistakes on messages that bypass the email system. How can you enforce policies for webmail without creating and maintaining an entirely separate policy system on a web proxy?

With Sendmail, as usual, the answer is simple. Our ICAP Multi-Protocol Monitoring service communicates with your choice of the Blue Coat web proxy platform or the open-source Squid proxy to capture webmail sessions in the Sentrion—and to execute the same policies used for standard email traffic. There's only one policy set to manage, and it works automatically across all email and webmail sessions—wherever your employees happen to be.

Incident remediation often requires human review of messages, so how do you deal with the XML (or other) code that webmail uses in transit from sender to webmail server? That's simple too. While other solutions force your compliance officers to dig through the XML code to find the actual message contents, our solution reconstructs webmail sessions as normal email—just as the sender intended for the recipient to see. With the email content in human-readable format, it's much easier to see where the violation occurred, and to gauge whether it was intentional or accidental. With the ICAP Multi-Protocol Monitoring service, you get:

- One policy set to manage for all your email and webmail
- Consolidated incident remediation and reporting for both email and webmail
- Human readable messages in the remediation system for both email and webmail

Best of all, you get peace of mind knowing that webmail your employees send from anywhere around the world is just as much under your control as the email sent through the Sentrion itself.