Once Wiretap is installed, you create “policies” that determine the content type, patterns and keywords that trigger certain actions. Using active directory integration, you can build policies that target or exclude specific countries, users, groups, business units, companies, names, etc.

Wiretap continually analyzes all content posted, regardless of the device used. If content in the message or file matches one of your policies, the selected action is taken within seconds and the content becomes an “incident,” subject to review.

If flagged for removal (or another action such as review) and tagged with a particular threat level, your internal staff reviews the content and may channel it for further investigation and follow-up with the sender, HR or others.

Key Wiretap Features

Enabling Safe Collaboration
Wiretap is the safeguard that allows you to apply the same level of caution and control to your ESN that you apply to operations throughout the rest of your organization. Wiretap monitors and secures all ESN activity continuously, 24/7 — including all public and private conversations, files and feeds.

It also protects your organization from accidental or purposeful infraction of company policies or compliance regulations. Wiretap runs undetected in the background, so you have security and peace of mind while your employees have unencumbered use of their ESN.

Easy to Install, Easy to Use
Wiretap deployment is quick and simple, connecting to your Yammer® network and running on your own infrastructure in your private cloud or on premise data center.

The interface is designed for simplicity, so ramp up is quick and you can get started setting policies right away. As you refine your monitoring needs over time, fine-tuning and adding new policies is a breeze.

Wiretap is installed within your network (whether it’s on-site or in an Azure®/Amazon AWS® environment), so all your existing network and security policies automatically apply — no need to worry about another cloud-based solution that needs secured and protected.

All the Features You Need, None You Don’t
Wiretap is the only enterprise solution that monitors and protects your ESN activity through:

- Ongoing scanning with immediate removal of suspicious messages and files
- Active directory integration for highly granular policy controls
- Automatic flagging and classification by threat level
- Customizable content controls
- Auto-tagging of content for automated social organization
- Installation on-site or in Azure®/Amazon AWS®
- Accessibility across all mobile devices
- Dashboard visibility into all Yammer® activity

How Wiretap Works

Set Policies

Once Wiretap is installed, you create “policies” that determine the content type, patterns and keywords that trigger certain actions.

Using active directory integration, you can build policies that target or exclude specific countries, users, groups, business units, companies, names, etc.

Determine Actions

You determine what actions should be taken for each (e.g. delete, flag, hashtag or notify a business or security team) and add these preferences into the system.

Analyze Content

Wiretap continually analyzes all content posted, regardless of the device used.

If content in the message or file matches one of your policies, the selected action is taken within seconds and the content becomes an “incident,” subject to review.

Follow Up

If flagged for removal (or another action such as review) and tagged with a particular threat level, your internal staff reviews the content and may channel it for further investigation and follow-up with the sender, HR or others.