The Department of Defense (DoD) Directive-Type Memorandum (DTM) 09-026 allows DoD agencies to access Social Media sites assuming each agency provides adequate protection against malware and advanced threats, and is able to block access to prohibited sites and content. Websense is uniquely positioned to provide not only compliance with these requirements but also industry leading protection against advanced threats from Social Media.

What does DTM 09-026 say?

- The NIPRNET (Non-classified Internet Protocol Router Network) shall be configured to provide access to Internet-based capabilities across all DoD components.
- Commanders at all levels and Heads of DoD components shall continue to deny access to sites with prohibited content and to prohibit users from engaging in prohibited activity via social media sites. (e.g. pornography, gambling, hate-crime related activities).
- All use of Internet-based capabilities shall comply with paragraph 2-301 of Chapter 2 of the Joint Ethics Regulation (Reference (b)) and the guidelines set forth in Attachment 2.

Websense offers real-time inline advanced threat protection and granular social media control

Websense offers real-time, in-line protection against advanced malware threats that goes far beyond any signature-based defense, such as AntiVirus, firewalls, or even most Next Generation Firewalls. With Websense TRITON solutions you are protected against the latest zero day exploits.

Websense TRITON gateway solutions also provide granular control over what parts of social media sites employees can access and use. For example, employees may utilize Facebook posts, but be blocked from Facebook chat and picture uploads. Over 30 different Social Media controls give you great control over the social media content accessed by employees, reducing your exposure to threats, improving productivity, and limiting your legal liability.

Real time, in-line threat protection

- Websense Advance Classification Engine (ACE) provides real-time protection against advanced threats.
- More than 10,000 analytics analyze traffic and provide a composite risk score.
- Feeding ACE is Threatseeker Network, which is the World’s largest threat detection network spanning 900 million endpoints and handling 3-5 billion web requests per day.
- Inspect SSL traffic and ensure safety on social media sites with our proxy deployments.

Granular social media access control

- Extend Acceptable Use Policy (AUP) to social media. Websense offers more than 120 content categories, including 30 for Social Media applications, with 11 alone for Facebook.
- Give employees well defined access to social media sites and decrease exposure to malware threats and infection by providing access to only those areas of social media sites you deem safe.

Intuitive management and reporting

- Websense offers over 60 pre-defined reports and many customizable reports on web threat levels and user activity for technical and business users.
The Websense difference: Websense ACE (Advanced Classification Engine)

ACE provides real-time, inline, contextual defenses for web, email, data and mobile security by using composite risk scoring and predictive analytics to deliver the most effective security available. It provides containment by analyzing inbound and outbound traffic with data-aware defenses for data theft protection. Classifiers for real-time security, data and content analysis — the result of years of research and development — enable ACE to detect more threats than traditional anti-virus engines every day (the proof is updated daily at securitylabs.websense.com). ACE is the primary defense behind all Websense TRITON solutions, and is supported by the ThreatSeeker Network.

For Social Media sites, ACE provides:

- Inline threat, phishing, scam and lure detection
- Real-time social media web content ratings
- Key defenses for SSL web traffic inspection
- Granular controls within social media scripts
- Data theft and loss protection

ThreatSeeker Network – The World’s Largest Threat Monitoring System

Websense ThreatSeeker Network managed by Websense Security Labs provides the core collective security intelligence for Websense security solutions. Uniting over 900 million endpoints including Facebook and Defensio social networking inputs enables ThreatSeeker Network with ACE (Advanced Classification Engine) security defenses to analyze 3-5 billion requests per day. This greater awareness to security threats results in real-time security updates to block advanced threats, malware, phishing attacks, lures and scams, plus provide the latest in web ratings. ThreatSeeker Network is unmatched in size and the use of ACE real-time defenses to analyze collective inputs.

Websense Certifications and Compliance Achievements

<table>
<thead>
<tr>
<th></th>
<th>Hardware</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPS 140-2 Level 1</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>CC EAL 2+</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>DoD CoN</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>HSPD#12</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>DoD STIG</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>IPv6</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

For more detailed compliance information please contact Websense.

Mobile, social, and cloud technologies drive productivity. But they also open the door to data theft and advanced attacks that can slip right by anti-virus, URL filtering and firewall defenses. Websense® TRITON™ solutions keep you a step ahead with web, email, data and mobile security solutions (available together or separately) that share a common architecture. The real-time defenses of Websense ACE (Advanced Classification Engine), plus flexible deployment options and a unified management console, make TRITON solutions vital in today’s dynamic environments.