The passing of the Counter-Terrorism and Security Act 2015 means educational establishments now have a statutory duty to prevent students from being drawn into terrorism. With the Internet and social media playing a huge role in the radicalisation of young people, a comprehensive security approach is essential for complying with the government’s Prevent duty.

Contact Infosec Partners +44 (0)845 257 5903 | www.InfosecPartners.com
“We all have a duty of care to challenge, at every turn, the twisted narrative that has corrupted some of our vulnerable young people. Schools must play a vital role in protecting pupils from the risks of radicalisation.”

John Hayes, Security Minister
THE PREVENT DUTY & ONLINE SAFETY

What is Prevent?

In the summer of 2015, the UK government made Prevent (its full name is the Preventing Violent Extremism strand) a statutory duty for schools, childcare providers and further education establishments. Along with prisons, local authorities and NHS trusts, they are now under a legal obligation to “have due regard to the need to prevent people from being drawn into terrorism”. According to the government’s guidance, the day-to-day responsibilities of teachers and staff now include being able to spot children who might be vulnerable to radicalisation.

Monitoring, blocking and reporting on inappropriate activity

Schools and other education establishments have been focused on filtering website content and blocking website categories in an attempt to satisfy duty of care requirements around online safety and cyberbullying. However with the introduction of enhanced requirements and auditing guidelines, along with the updated guidance on the Prevent Duty, schools now have a requirement to look much deeper into internet and social media traffic to identify potential children at risk. This includes identifying sites that may appear innocuous but attempt to display harmful content to children and to keep accurate records of exactly who does what, whether the internet requests are allowed or blocked. This helps to identify the signs of radicalisation, whether explicit or significant as part of a pattern of behaviour.

How Fortinet solutions meet obligations of the Prevent Duty

1. Category based web filtering
   - All internet requests can be filtered for attempts to access sites and resources known to be involved in discussions around terrorism, requests can be automatically blocked and recorded from any device.

![Fortinet content filtering categories relevant to the Prevent Duty](image-url)
2. Deep control of social media and web based applications

- Ability to look inside of applications like Facebook, twitter, Pinterest, Instagram and chat sites to search and identify harmful posts and material, not just the list of sites visited.

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Category</th>
<th>Technology</th>
<th>Popularity</th>
<th>Risk</th>
<th>Deep App Control</th>
<th>Last Released</th>
</tr>
</thead>
<tbody>
<tr>
<td>Twitter_Login</td>
<td>Social Media</td>
<td>Browser Based</td>
<td>⬤ ⬤ ⬤</td>
<td>⬤ ⬤ ⬤</td>
<td>Yes</td>
<td>2016-01-12</td>
</tr>
<tr>
<td>Flickr_Login</td>
<td>Social Media</td>
<td>Browser Based</td>
<td>⬤ ⬤ ⬤</td>
<td>⬤ ⬤ ⬤</td>
<td>Yes</td>
<td>2015-10-19</td>
</tr>
<tr>
<td>Pinterest_Post</td>
<td>Social Media</td>
<td>Browser Based</td>
<td>⬤ ⬤ ⬤</td>
<td>⬤ ⬤ ⬤</td>
<td>Yes</td>
<td>2016-01-15</td>
</tr>
<tr>
<td>Google-Plus_File.Upload</td>
<td>Social Media</td>
<td>Browser Based</td>
<td>⬤ ⬤ ⬤</td>
<td>⬤ ⬤ ⬤</td>
<td>Yes</td>
<td>2016-01-15</td>
</tr>
<tr>
<td>Facebook_File.Download</td>
<td>Social Media</td>
<td>Browser Based</td>
<td>⬤ ⬤ ⬤</td>
<td>⬤ ⬤ ⬤</td>
<td>Yes</td>
<td>2016-01-05</td>
</tr>
<tr>
<td>Tencent_Wave_Logout</td>
<td>Social Media</td>
<td>Browser Based</td>
<td>⬤ ⬤ ⬤</td>
<td>⬤ ⬤ ⬤</td>
<td>Yes</td>
<td>2015-10-19</td>
</tr>
<tr>
<td>Google-Plus_Post</td>
<td>Social Media</td>
<td>Browser Based</td>
<td>⬤ ⬤ ⬤</td>
<td>⬤ ⬤ ⬤</td>
<td>Yes</td>
<td>2016-01-19</td>
</tr>
<tr>
<td>Facebook_Login</td>
<td>Social Media</td>
<td>Browser Based</td>
<td>⬤ ⬤ ⬤</td>
<td>⬤ ⬤ ⬤</td>
<td>Yes</td>
<td>2016-01-11</td>
</tr>
<tr>
<td>Yammer(Login)</td>
<td>Social Media</td>
<td>Browser Based</td>
<td>⬤ ⬤ ⬤</td>
<td>⬤ ⬤ ⬤</td>
<td>Yes</td>
<td>2015-10-21</td>
</tr>
<tr>
<td>Yammer_File.Upload</td>
<td>Social Media</td>
<td>Browser Based</td>
<td>⬤ ⬤ ⬤</td>
<td>⬤ ⬤ ⬤</td>
<td>Yes</td>
<td>2015-10-20</td>
</tr>
<tr>
<td>Yammer_File.Download</td>
<td>Social Media</td>
<td>Browser Based</td>
<td>⬤ ⬤ ⬤</td>
<td>⬤ ⬤ ⬤</td>
<td>Yes</td>
<td>2015-11-16</td>
</tr>
<tr>
<td>LinkedIn_File.Upload</td>
<td>Social Media</td>
<td>Browser Based</td>
<td>⬤ ⬤ ⬤</td>
<td>⬤ ⬤ ⬤</td>
<td>Yes</td>
<td>2016-01-26</td>
</tr>
<tr>
<td>LinkedIn_File.Download</td>
<td>Social Media</td>
<td>Browser Based</td>
<td>⬤ ⬤ ⬤</td>
<td>⬤ ⬤ ⬤</td>
<td>Yes</td>
<td>2016-01-26</td>
</tr>
<tr>
<td>Yammer_Post</td>
<td>Social Media</td>
<td>Browser Based</td>
<td>⬤ ⬤ ⬤</td>
<td>⬤ ⬤ ⬤</td>
<td>Yes</td>
<td>2015-11-17</td>
</tr>
<tr>
<td>Tumblr_Post</td>
<td>Social Media</td>
<td>Browser Based</td>
<td>⬤ ⬤ ⬤</td>
<td>⬤ ⬤ ⬤</td>
<td>Yes</td>
<td>2015-12-31</td>
</tr>
<tr>
<td>Facebook_Post</td>
<td>Social Media</td>
<td>Browser Based</td>
<td>⬤ ⬤ ⬤</td>
<td>⬤ ⬤ ⬤</td>
<td>Yes</td>
<td>2016-01-19</td>
</tr>
<tr>
<td>LinkedIn_Post</td>
<td>Social Media</td>
<td>Browser Based</td>
<td>⬤ ⬤ ⬤</td>
<td>⬤ ⬤ ⬤</td>
<td>Yes</td>
<td>2016-01-26</td>
</tr>
</tbody>
</table>

Figure 2. Fortinet’s Deep App Control allows more thorough control and monitoring of application usage

3. Strong authentication

- Strong authentication of all users as they join the school networks (wired & wireless), to provide 100% assurance of student identity, authentication of individual user sessions.

4. Integration with active directory groups

- Through ease of integration with active directory groups, filtering and reporting can be easily customized for different age groups based on group membership and device type used.

5. Device registration and control

- Bring Your Own Device (BYOD), where students and staff are allowed to work or use their personal computers such as laptops, tablets, is increasingly popular but a challenge that many organisations initially face when implementing a BYOD approach is how to secure the network and information accessed by these devices.
- Personal devices of users, as they are not fully trusted, owned and managed by the school, can be restricted so that they are only allowed to view a subset of the Internet. Alternatively these devices can be registered as trusted BYOD devices and certificates pushed to each device. Full SSL inspection can then be performed as per school owned devices in order to monitor all internet browsing activity, including https sites where traffic is encrypted with SSL certificates.
6. HTTPS Deep inspection, SSL decryption and advanced filtering

- Filtering of HTTPS traffic is essential to be able to inspect encrypted websites. HTTPS deep scanning inspects all encrypted traffic to identify instances indicative of radicalisation or terrorism, whilst respecting a user’s privacy by optionally not scanning banking, health care and personal privacy sessions.

7. Safe Search

- Safe Search and Search Engine Keyword Enforcement Popular search engines include the ability to perform image searches, and display thumbnail image results. Providing a safe search option that enforces the safe mode of popular search engines to limit the displayed results to content considered safe according to the safe search policies of each search engine. In addition search engine keyword filtering can be used to block searches of specific keywords or phrases related to extremism.

8. Recording of all webs searches

- Reporting and filtering of keywords used in popular web searches, used to identify trends of groups of users searching for words and phrases relating to extremism.

Top Search Phrases

<table>
<thead>
<tr>
<th>#</th>
<th>Phrase</th>
<th>Requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>How to join ISIS</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Jihadi Bride</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Travel to Syria</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>Message to America</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>War on Islam</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>YODO - you only die once</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>Jihobbyist</td>
<td>1</td>
</tr>
</tbody>
</table>

Figure 3. Analysing search phrases can detect patterns of behaviour of specific individuals, and identify vulnerable groups of individuals.
9. Compliant reporting

- From the log report shown in Figure 4 below, not only can it be seen that the user ‘jsmith’ tried to visit a number of inappropriate sites, it can also be seen from which device, through which server and what action was taken. Clearly this is an exaggerated example but it shows the power of Fortinet solutions to help administrators identify unacceptable activity and take the appropriate actions both for the establishment and to comply with the Prevent duty.

![User log report example](image.png)

**Figure 4. Example of detailed web browsing activity**
Appropriate restrictions

The prevent duty puts a responsibility on the educational establishment to perform in depth filtering and reporting of a user’s internet usage, the prevent guidance also make it very clear that no monitoring is deemed to be ‘covert’.

There are many technologies and security products that are more intrusive in nature, capturing all activity on a user’s device. These intrusive, covert technologies are not appropriate for the sensitive task of protecting children from extremism, additionally there are areas of law which may introduce additional risk and exposure for the school and for the learner by the deployment of these covert technologies, the recording and storage of young person’s most sensitive information and from the inherent risks to all of possessing that type of personal material.

Fortinet solutions strike the right balance between detailed monitoring, whilst still respecting the privacy and personal life of the children in the care of the school.

FortiGuard Quick Facts:

FortiGuard Labs operate in North America, Asia Pacific, and Europe.

- In a typical week, FortiGuard Labs process over 220 TB worth of threat samples, and add or update approximately:
  - § 2 million antivirus signatures
  - § 18,000 intrusion prevention (IPS) rules
  - § 250 million URL ratings in 78 categories
  - § 47,000,000 antispam signatures
- In addition, FortiGuard Labs track more than:
  - § 5,800 application control signatures
  - § 700 database security policies
  - § 3,000 web application firewall attack signatures and has uncovered over 200 zero-day threats
SECURING SCHOOLS: The Protect Duty

- Ofsted compliant enforced separation of curriculum and admin resources
- Strong web content filtering to Safeguarding standards
- Data leak prevention protects sensitive data leaving the school
- Internal and external firewall segregation
- Reduce the risk of cyberbullying activity through application control
- Intrusion detection & bandwidth management included
- FortiClient extends the coverage to protect students and staff at home
- Secure Tokens provide strong authentication for staff connecting remotely
- Satisfy all Protect Duty & counter-terrorism requirements for monitoring
- Record and alert all web search terms relating to terrorism
- Identify the risk of students being drawn into terrorism
- Identify those at risk through real-time alerts, keeping students safe from the dangers of radicalisation and extremism
- Ensure students are safe from terrorist and extremist material through appropriate filtering

“Promote the values of democracy, the rule of law, individual liberty and mutual respect and tolerance for those with different faiths and beliefs whilst using the Internet.”

DUTY OF CARE

Schools are charged with the duty to protect children in their care but given the increasing dependence on connectivity, as well as the use of the Internet as part of the standard learning approach, how can they suitably provide this?


Contact Infosec Partners today for solutions to overcome the challenges.
ABOUT INFOSEC PARTNERS

A trusted advisor to significant organisations, Infosec Partners provides full-spectrum information security expertise and managed services to some of the world’s largest and most sensitive businesses, high-profile individuals and families.

Infosec Partners’ flexible security service portfolio allows clients to outsource whole or component parts of their information security requirements, or access specialist security support as needed, when impartiality is critical. Founded in 2004 and head quartered in the UK with a trusted global network, Infosec Partners combines a business-led risk management approach and highly trained advisors, with proven technical capability to deliver optimal security solutions for all types of organisation.

www.infosecpartners.com