smoothwall

The Web You Want

Safeguarding

Product Release: Glamis

The Radicalisation Risk

International terrorist organisations have become a significant focus of both the media and government, with legislation continually evolving to try and halt their impact. A primary area of concern relating to their domestic proliferation is their strategy of drawing young people into radicalisation via trusted institutions, both in person and via the internet.

Over the last 12 years in the UK various legislative acts have arisen relating to the safety and protection of children. The Children Act of 2004 focuses on protecting children from a wide variety of issues such as abuse, substance misuse, bullying and radicalisation. Following on from that the Counter-terrorism and Security Act in 2015 placed an increased emphasis on protecting children from radicalisation.

This introduced the 'The Prevent Duty' strategy which details specific steps educational establishments and bodies of trust should implement in order to ensure the protection of young and vulnerable people.

Most recently, 'Keeping Children Safe in Education' is new statutory guidance released in September 2016 which identifies that all schools and colleges should have appropriate filtering and monitoring in place to keep children safe online.

The Technology Challenge

Within the context of this increased legislation the internet is rapidly evolving, not only in terms of the number of websites and the collaborative web, but also in the way the web is becoming totally secure. There are also an increasing number of ever smarter proxies for people to circumvent traditional filtering.

To Block or Not to Block?

As an industry we need to change our approach by not just blocking content, but keeping children safe by actually looking at the intent of what they are trying to achieve. This presents a difficult problem for school administrators and safeguarding officers.

In contrast with the need for increased awareness of pupil's activities, there are references made by the Government via Ofsted guidance to provide 'appropriate levels of filtering', with the emphasis on staff having appropriate training to ensure they have the knowledge to identify children at risk of being drawn

into terrorism. The approach is to encourage and support schools to move from locked-down systems that block content, to systems that manage content.

'Keeping Children Safe in Education' refers to various aspects of filtering and monitoring, specifically describing the needs of the technology. Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that 'over blocking' does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

A good example of the complexities of internet Safeguarding in action can be illustrated by taking a selection of terms used by the FBI and GCHQ as words which would typically be used by people being radicalised:

Tamil Tigers

Suicide bomber **Eco-terrorism**

Recruitment Iraq **Target** Nigeria

Pirates Terrorism **Radical** Daesh

Enriched Islamist IRA

Afghanistan Nuclear Chemical weapon

Fundamentalism

You can see here that most of these words on their own are harmless, and the context of the search could be completely innocent.

This means it's not possible to strictly block on these terms, it would be far too restrictive. Interestingly, the government recently launched its own website - Educate Against Hate. If the same terminology blocking methods were applied to Educate Against Hate, the website would be blocked. For this reason simply blocking problem terms is not a suitable solution to meet the legislative need.

UK Ofsted further endorse the non-blocking approach when they refer to the role of schools and the need for the leaders and the governors of the schools to prepare pupils for life in modern Britain. They aim to emphasise values of democracy, law, mutual respect, equality, and greater understanding of people of all faiths, races, genders, and abilities. This is designed to get children quite rightly prepared for life in modern Britain.

In turn however, a liberal and modern Britain also has some potential threats for children. Key to tackling this, and also referred to in Ofsted guidance, is the effectiveness of Safeguarding, and the "effectiveness of leaders and governors work" to keep children safe. Ofsted specifically refer to keeping children safe from sexual exploitation and the dangers of radicalisation, and so this is the area we are most interested in. Safeguarding Officers have expressed interest in how we can put tools in place which don't block, but actually look at trends and look at where children are, from a technology perspective, being led into areas they shouldn't be.

Key Safeguarding roles

If we examine key safeguarding roles, we can infer an extended 'chain of trust' which runs from the filtering supplier, through to the technology leads in the school (typically the System Administrators) and ultimately the individuals who hold the legal responsibility.

The filtering supplier and the System Administrator are key to providing the tools and the experience to provide the information that is needed, but ultimately it's neither of these two who hold the legal responsibility. The responsibility is held by the head teacher, the Safeguarding Officer, or the Governors of the school.

What is needed are the tools and the systems between the filtering supplier and the Systems Administrator to enable creating reports that are actually meaningful and can be read 'out of the box' by those individuals holding the legal responsibility, allowing them to identify the individuals or groups that might be at threat.

This is the content of the creation of the Smoothwall Safeguarding reporting feature.

Identifying the need

Web filtering has changed dramatically over the past few years, and so the first step was to define what level of performance is needed in order to achieve these legal thresholds for delivering protection. We already have a complete circle of filtering that enables us to block activity. Over the last few years our solution has grown from standard URL filtering through search terms, real-time content inspection/modification, to SSL and egress filtering. There are a lot of tools all our customers have to enable them to identify and block activity that really shouldn't be seen by students in schools. In this context a block is an 'event'; something that happens that you can prevent.

In the Ofsted guidelines, not everything you could block needs to be blocked, remembering the need to enable the effectiveness of the work of the leaders and those holding responsibility to raise awareness and keep pupils safe. This is the monitoring side and is intent-based, as opposed to event-based.

Smoothwall Safeguarding functions on the belief that the best way to protect pupils is to combine the two. Safeguarding for us is a combination of blocking or event-based activities, with monitoring, which are the intent-based ones. A simple block is no longer good enough and particularly if you want to give students access to the reality of a modern, liberal society.

What do we mean by intent?

In the first instance these are the things that the student might be exposed to that enable us to identify if they are being 'drawn into' something. A good example of this might be search terms which are easy to block. However in many cases the search terms involved are actually also legitimate ones.

To understand this more deeply we can consider the example of a pupil using the search term 'Isis'. Isis is not a search term anyone would want to block, as there are reasons why a school class might want to explore Isis from the perspective of current affairs, research the Egyptian god, or the flower of the same name.

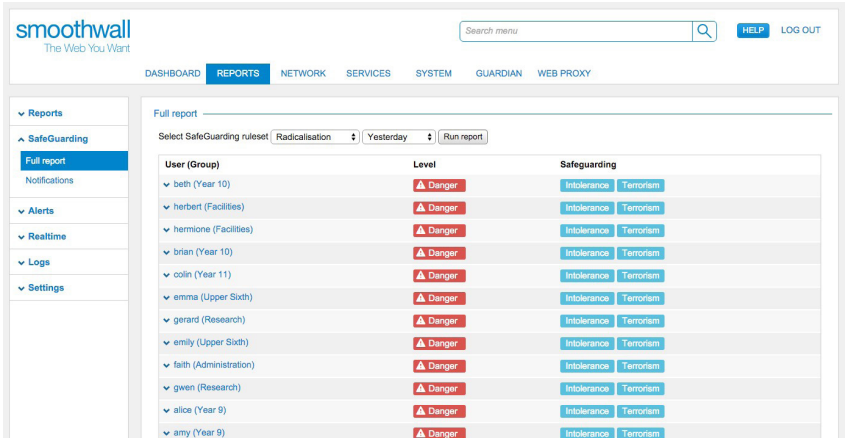
More important than search terms alone are search terms followed by domain requests —this starts to build a story: someone searched for something, then went to a suggested site. In addition to where they went, what did they contribute on the site? We are able to look at post requests within a site, including a social media site, potentially including permitted domains. We are able to see that in the future there could be a need to capture full content from a post request to provide extra information where there is a particular student the Safeguarding Officer might be concerned about. Email content could also be examined, although many pupils see this as something obsolete this may in fact make email a perfect place to hide content.

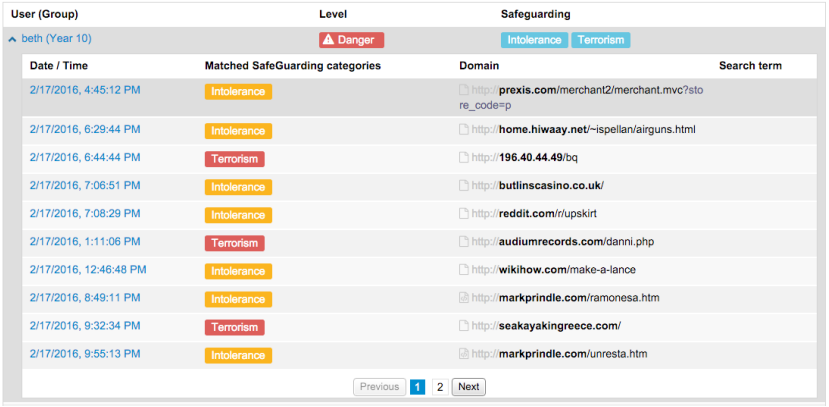
Instant messaging content needs to be considered — not just stand alone instant messaging applications, but also the chat functionality included in applications such as Snapchat and Instagram which combine web browsing, instant messaging and many other communications means within a single application. The end goal becomes to try and find a way to build a story of the activity and therefore address a threat to a particular student or group of students.

Safeguarding Reporting as a Feature

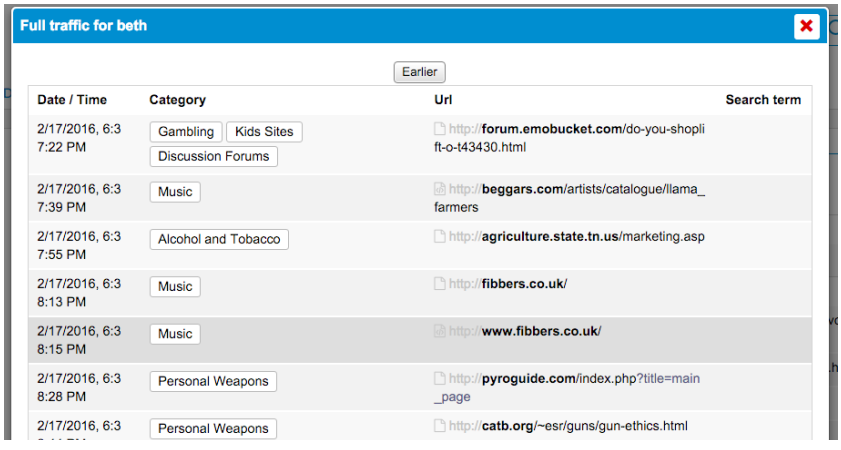
Safeguarding allows the System Administrator to run reports against Safeguarding rulesets to view those users who have breached them during specified time periods. A colour-coded indicator shows the severity of the breaches. 'Out of the box' seven safeguarding category rulesets are defined: for example, Radicalisation includes the Guardian categories of Terrorism and Intolerance. These look at the student activities, in the first instance search terms and web access, classify them into certain categories and assign a severity rating.

Each category within a ruleset has a severity level assigned to it. The severity level of the ruleset breach reflects the highest level of category breach. For example, if the user breaches against Intolerance (which is a Caution) and Terrorism (which is Danger), the ruleset breach will show as Danger.





Safeguarding also provides a mechanism for a detailed view, such that if there is a particular student where a report raises a severity of a breach which is high enough to cause concern, you will at that point be able to drill down into the chain of events going on that caused that particular breach. Clicking on an individual user gives a detailed user activity report, showing any breaches within the report period selected.



Within the user activity report, clicking on a breach expands the view to include all browsing history either side of the breach. This detailed report provides the Safeguarding officer with a context to a user's activities, helping them to determine if intent is present.

Safeguarding notifications allow reports on a student or group of students to be emailed to the responsible individuals in the school. The System Administrator is able to set up a daily, weekly or monthly email notifications against a chosen ruleset, and enter the email group they wish to receive it.

For further information

Please contact our Product team via email or by submitting feedback to our customer forum.

Email: product@smoothwall.com
Visit: smoothwall.uservoice.com

For help or support, please call
08701 999 500

smoothwall
The Web You Want

www.smoothwall.com