Keeping Children Safe In Education (KCSIE 2016)

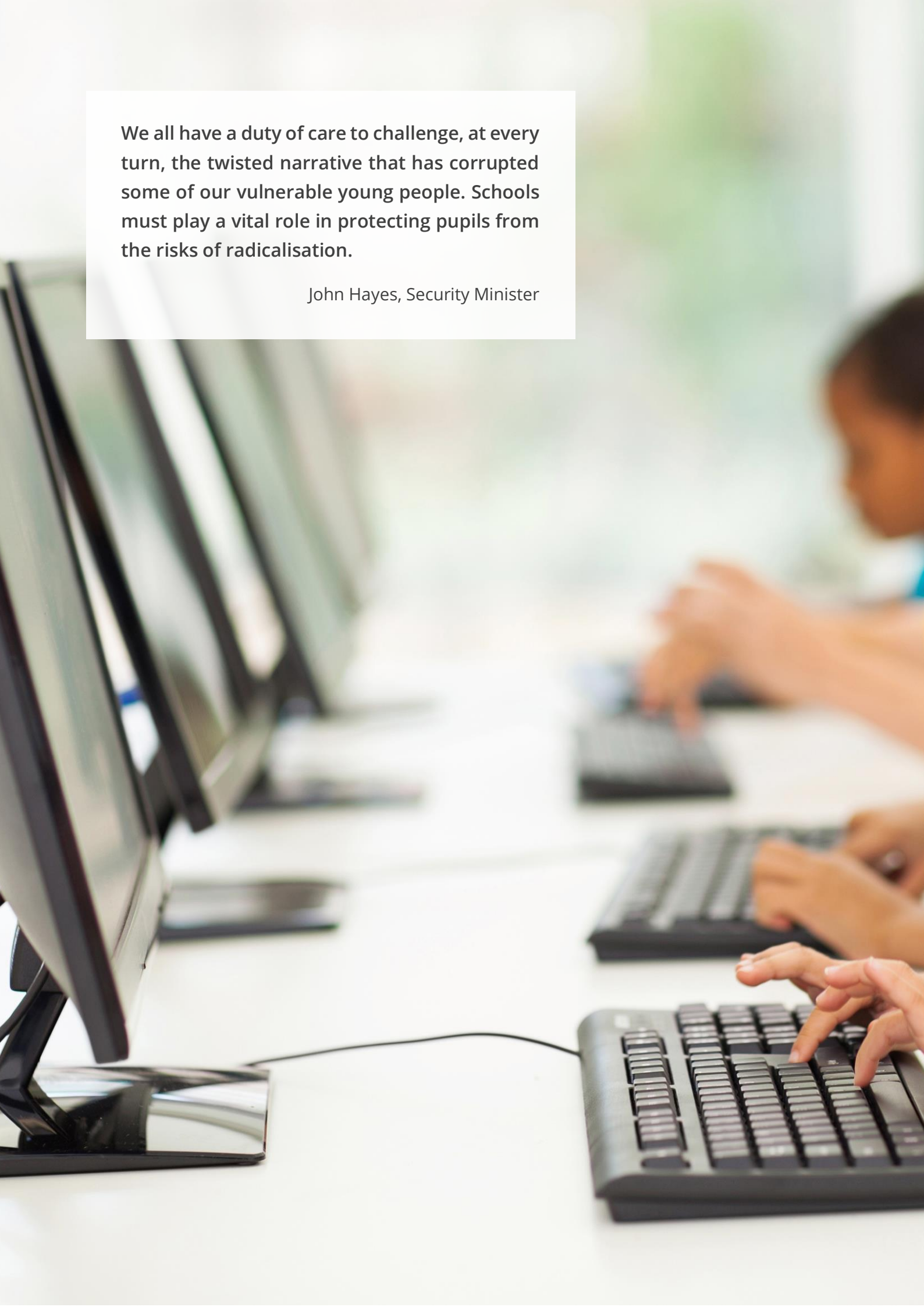
Safeguarding is everyone's responsibility

An amended version of the Keeping Children Safe in Education guideline (KCSIE) came into statutory force on 5th September 2016, with further emphasis on the need for all education professionals to understand that safeguarding is everyone's responsibility.

Safeguarding is not a new issue for schools but in the last decade, the demands of keeping children and young people safe have grown significantly.

The changes mean that every school will need to consider and review safeguarding policies and procedures, focusing particularly on how they protect and maintain duty-of-care amidst the growing online threats to each student's wellbeing.

InfosecPartners
CYBERSECURITY



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

Keeping Children Safe In Education

Trends in the use and accessibility of the internet and social media have led the Department of Education (DfE) to review the Keeping Children Safe in Education (KCSIE) guidance, which has been in place since 2014. The updated version which became statutory on 5th September 2016 means that every school will need to consider and review its safeguarding policies and procedures, focusing particularly on how they protect students online.

In this guide, Infosec Partners outlines KCSIE and demonstrates how fully integrated security solutions, such as those from Fortinet, can help schools meet the new requirements.

The Prevent Duty and Online Safety

Changes in the KCSIE guideline follows the UK government making Prevent (its full name is the Preventing Violent Extremism strand) a statutory duty for schools, childcare providers and further education establishments in the summer of 2015.

Along with prisons, local authorities and NHS trusts, they are under a legal obligation to "have due regard to the need to prevent people from being drawn into terrorism", with teachers and staff responsible for identifying signs that children might be vulnerable to radicalisation.

Monitoring, Blocking and Reporting

Schools and other education establishments have been predominantly focused on filtering website content and blocking website categories in an attempt to satisfy duty of care requirements around online safety and cyberbullying. However the KCSIE guidance actually *warns of the risk of over-blocking leading to "unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."*

With the enhanced auditing requirements needed to meet KCSIE and the Prevent Duty, schools now have 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.

Department for Education

Harmful content:

- DESCRIMINATION

  Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.

- PORNOGRAPHY

  Displays sexual acts or explicit images.

- SELF- HARM

  Promotes or displays deliberate self-harm including suicide and eating disorders.

- VIOLENCE

  Displays or promotes the use of physical force intended to hurt or kill.

Illegal content:

- DRUGS/SUBSTANCE ABUSE

  Promotes or displays the illegal use of drugs or substances.

- EXTREMISM & RADICALISATION

  Promotes terrorism and terrorist ideologies, violence or intolerance.

- CHILD ABUSE IMAGE CONTENT (CAIC)

  Displays images of child sexual abuse including pornography.

- PIRACY AND COPYRIGHT THEFT

  Includes illegal provision of copyrighted material.

Appropriate Filtering

KCSIE now requires a minimum requirement of specific databases to be integrated in the filtering solution. To comply, providers of content filtering tools/services need to be an IWF (Internet Watch Foundation) member which provides access to the child abuse image content (CAIC) list, as well integrating the home office police assessed list Counter Terrorism Internet Referral Unit (CTIRU) which keeps track of unlawful terrorist content.

Appropriate filtering should control access to inappropriate and harmful content as defined above. In addition, it should be flexible enough to meet the individual needs of each School for College setting and risk assessment.

Appropriate Restrictions

Educational establishment have a statutory duty to perform in-depth filtering and reporting of a user's internet usage, with guidance making it very clear that no monitoring is deemed to be 'covert'.

Security products exist that are more intrusive in nature, capturing all activity on a user's device, however these are not appropriate for the task of protecting children. There are areas of law which may introduce additional risk and exposure for both school and student through the deployment of intrusive technologies, from the recording and storage of young person's most sensitive information, and the inherent risks to all of possessing that type of personal material.

The right balance needs to be found between detailed monitoring, and respecting the privacy and personal life of the children.

Fortinet Solutions for Education

Security, simplicity and cost. Every IT Director faces these challenges for their environments. However, in Education maintaining an effective balance of these elements is critical all day, every day.

Today's digital classrooms require connectivity for almost any device. From primary to upper grade levels, students and staff often bring more than one device with them each day. The opening of networks to accommodate the growing number of devices fosters inevitable security risks which could lead to data breaches and data leaks of sensitive student and staff personal information.

Fortinet understands and appreciates the unique challenges educators face, in delivering engaging, relevant, and meaningful learning opportunities to students while maintaining a high level of network security to protect data and meet compliance standards.

Fortinet Security Fabric

Simply deploying security end to end is not enough. Security solutions must work together to form a cooperative fabric, spanning the entire network, linking different security sensors and tools together to collect, coordinate, and respond to any potential threat.

Having the right security woven throughout your network can make the difference between running a smooth, safe network or being the latest security breach headline.

Fortinet is the only company with security solutions for network, endpoint, application, data centre, cloud, and access designed to work together as an integrated and collaborative security fabric.

FortiGuard

FortiGuard Web Filtering is the only web filtering service in the industry that is VBWeb certified for security effectiveness, blocking 97.7% of direct malware downloads and stopping 83.5% of malware served through all tested methods in Virus Bulletin's 2015 security testing. According to Virus Bulletin, Fortinet is the only vendor in the 2016 VBWeb tests confident enough in their security solution to share results in a public test.

Every minute of every day FortiGuard Labs processes approximately 43 million URL categorization requests and blocks 160,000 malicious websites. And in a typical week, FortiGuard Labs process over 220 TB worth of threat samples, and add or update approximately:

- 250 million URL ratings in 78 categories
- 1.5 million new URL ratings
- 2 million antivirus signatures
- 18,000 intrusion prevention (IPS) rules
- 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

Category-based web filtering

All internet requests can be filtered for attempts to access sites and resources known to be involved in discussions around specific subjects, such as terrorism. Requests can be automatically blocked and recorded from any device.

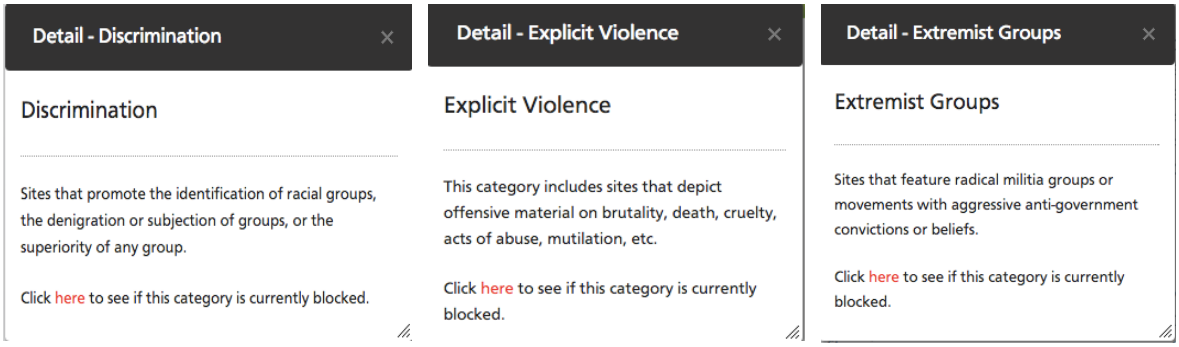
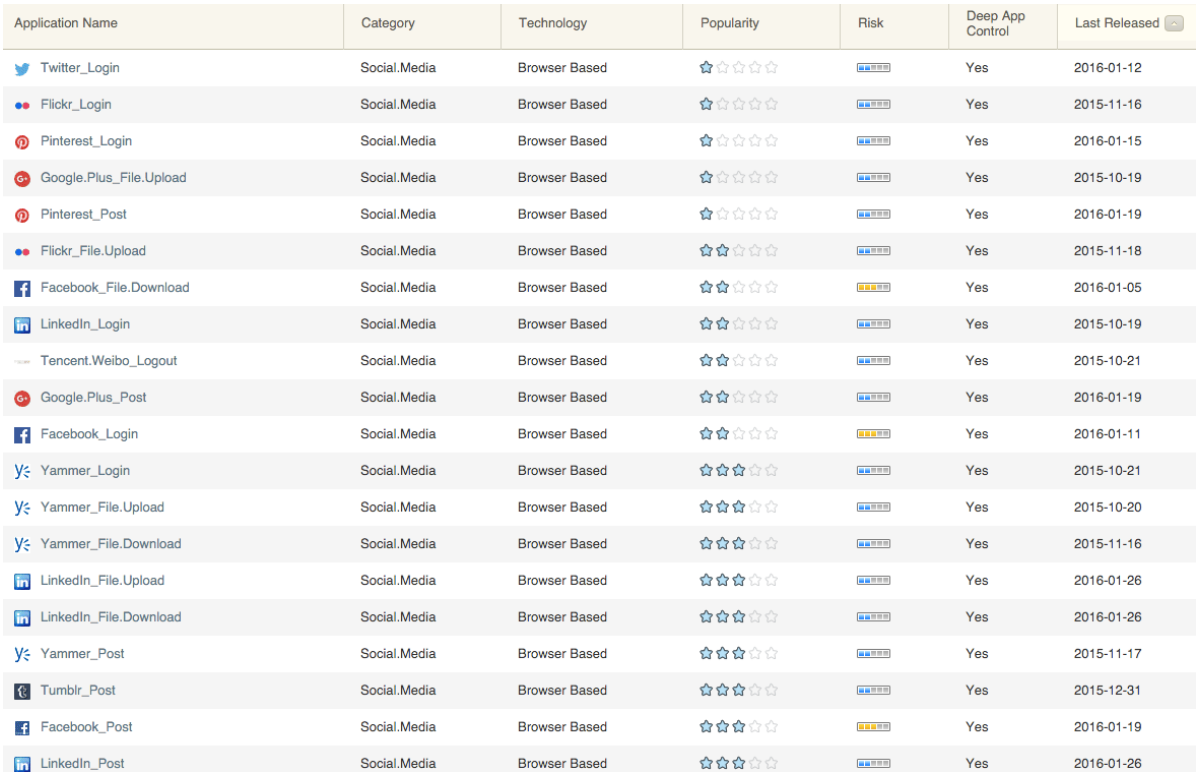


Figure 1. Fortinet content filtering categories relevant to the Prevent Duty

Deep control of social media and web based applications

Fortinet provides complete visibility and control over which applications are being used on the network, by whom, the bandwidth they are using and what priority they have over your network's valuable bandwidth. It allows you 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.



Application Name	Category	Technology	Popularity	Risk	Deep App Control	Last Released
Twitter_Login	Social.Media	Browser Based			Yes	2016-01-12
Flickr_Login	Social.Media	Browser Based			Yes	2015-11-16
Pinterest_Login	Social.Media	Browser Based			Yes	2016-01-15
Google.Plus_File.Upload	Social.Media	Browser Based			Yes	2015-10-19
Pinterest_Post	Social.Media	Browser Based			Yes	2016-01-19
Flickr_File.Upload	Social.Media	Browser Based			Yes	2015-11-18
Facebook_File.Download	Social.Media	Browser Based			Yes	2016-01-05
LinkedIn_Login	Social.Media	Browser Based			Yes	2015-10-19
Tencent.Weibo_Logout	Social.Media	Browser Based			Yes	2015-10-21
Google.Plus_Post	Social.Media	Browser Based			Yes	2016-01-19
Facebook_Login	Social.Media	Browser Based			Yes	2016-01-11
Yammer_Login	Social.Media	Browser Based			Yes	2015-10-21
Yammer_File.Upload	Social.Media	Browser Based			Yes	2015-10-20
Yammer_File.Download	Social.Media	Browser Based			Yes	2015-11-16
LinkedIn_File.Upload	Social.Media	Browser Based			Yes	2016-01-26
LinkedIn_File.Download	Social.Media	Browser Based			Yes	2016-01-26
Yammer_Post	Social.Media	Browser Based			Yes	2015-11-17
Tumblr_Post	Social.Media	Browser Based			Yes	2015-12-31
Facebook_Post	Social.Media	Browser Based			Yes	2016-01-19
LinkedIn_Post	Social.Media	Browser Based			Yes	2016-01-26

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

Strong Authentication

Fortinet provides multiple convenient options for 2-factor authentication It is important to have strong authentication of all users as they join the school networks (wired & wireless), to provide 100% assurance of student and staff identity, as well as authentication of individual user sessions, meaning that we can confidently trace activity with a specific authenticated user

Integration with Active Directory groups

Through ease of integration with active directory groups, filtering and reporting can be easily customised based on user and group (e.g. age groups) based on group membership and device type used, with individual users identified through their AD/LDAP credentials.

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.

As they are not fully trusted, owned and managed by the school, personal devices of 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.

Manage Encrypted Content

Many websites (including Google) are now utilising SSL encryption (HTTPS) as standard, to safeguard personal information when accessing them. Current research shows approximately 25-40% of all web traffic to be SSL encrypted and without the ability to inspect this traffic, your solution is effectively blind.

More concerning, is that without inspecting deep inside the content of encrypted streams, filtering policies will fail to correctly identify harmful and illegal content embedded within trusted social media sites and access may not be blocked.

Decryption of SSL traffic allows for HTTPS deep scanning to inspect all encrypted traffic to identify, for example, instances indicative of radicalisation or terrorism, whilst respecting a user's privacy by optionally not scanning banking, health care and personal privacy sessions. Once decrypted, all security services such as content filtering and anti-virus can be applied, just as it is for normal unencrypted connections

Flexible controls ensure "trusted" sites such hosted applications can remain uninspected to ensure maximum performance.

Safe Search

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 illegal and harmful content.

Recording of all Web Searches

Aside from blocking, the monitoring and reporting of keywords used in popular web searches can be used to identify trends or groups of users searching for words and phrases relating to illegal or harmful content such as suicide and extremism. Coupled with strong authentication, this can help education organisations to identify specific symptoms sooner.

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

Compliant Reporting

Having reporting intelligence easily accessible allows for any education organisation to quickly establish whether it is meeting all legal obligations, and its own risk-assessed policies are being applied appropriately. Configurable alerting allows for instant notification of policy infringement or notification for specific activities which may be undesirable.

As the log report in Figure 4 shows, 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 KCSIE and the Prevent Duty.

User: jsmith
Source IP: 192.168.223.53
Hostname (MAC): Win7_Ult_VM2
Source Interface: port2
Devices: FGVM010000045683

Detailed Web Browsing Log

#	Timestamp	Category	Website	Action	Bandwidth
1	2015-11-05 18:14:20		www.chechensinsyria.com	blocked	27.79 KB
2	2015-11-05 18:12:02	Peer-to-peer File Sharing	www.utorrent.com	blocked	889 B
3	2015-11-05 18:10:41		www.suicide.com	blocked	2.47 KB
4	2015-11-05 18:10:15	Pornography	penthouse.com	blocked	880 B
5	2015-11-05 18:10:02		www.jihadica.com	blocked	98.51 KB
6	2015-11-05 18:09:57		www.infoplease.com	blocked	16.12 KB
7	2015-11-05 18:07:53		www.jihadica.com	blocked	98.48 KB
8	2015-11-05 18:07:46	Advocacy Organizations	www.americansagainsthate.org	blocked	624 B
9	2015-11-05 18:07:45	Advocacy Organizations	www.americansagainsthate.org	blocked	345 B
10	2015-11-05 18:07:34		s7.addthis.com	blocked	26.16 KB
11	2015-11-05 18:07:34	Internet Radio and TV	www.springboardplatform.com	blocked	339 B
12	2015-11-05 18:05:32	Discrimination	www.kkk.com	blocked	13.25 KB
13	2015-11-05 18:05:27	Discrimination	www.kkk.com	blocked	5.34 KB
14	2015-11-05 18:05:05	Proxy Avoidance	lifehacker.com	blocked	364 B
15	2015-11-05 18:04:42	Proxy Avoidance	www.torproject.org	blocked	3.13 KB
16	2015-11-05 18:04:29	Proxy Avoidance	www.torproject.org	blocked	3.13 KB
17	2015-11-05 17:55:03	Hacking	anoninsiders.net	blocked	5.39 KB
18	2015-11-05 17:54:57	Hacking	anoninsiders.net	blocked	11.69 KB
19	2015-11-05 17:54:56	Hacking	anoninsiders.net	blocked	5.73 KB
20	2015-11-05 17:54:51	Hacking	anoninsiders.net	blocked	5.39 KB
21	2015-11-05 17:53:55	Weapons (sales)	www.gunbroker.com	blocked	602 B
22	2015-11-05 17:53:54	Weapons (sales)	www.gunbroker.com	blocked	356 B
23	2015-11-05 17:53:47	Weapons (sales)	www.impactguns.com	blocked	4.19 KB
24	2015-11-05 17:52:55		www.getselfhelp.co.uk	blocked	52.86 KB
25	2015-11-05 17:52:22	Advocacy Organizations	www.clarionproject.org	blocked	996 B
26	2015-11-05 17:52:13	Discrimination	www.barenakedislam.com	blocked	969 B
27	2015-11-05 17:51:58		jihadology.net	blocked	48.91 KB
28	2015-11-05 17:50:11	Gambling	www.bet365.com	blocked	596 B
29	2015-11-05 17:50:10	Gambling	www.bet365.com	blocked	322 B
30	2015-11-05 17:49:54	Tobacco	www.you-smoke.com	blocked	1.02 KB
31	2015-11-05 17:49:23	Pornography	www.playboy.com	blocked	288 B
32	2015-11-05 17:49:17	Pornography	www.playboy.com	blocked	886 B
33	2015-11-05 17:49:13	Streaming Media and Download	www.netflix.com	blocked	331 B
34	2015-11-05 17:48:48	Dating	authent.ilius.net	blocked	3.03 KB
35	2015-11-05 17:48:48	Dating	tk.ilius.net	blocked	3.03 KB
36	2015-11-05 17:41:35	Streaming Media and Download	www.netflix.com	blocked	598 B
37	2015-11-05 17:41:34	Streaming Media and Download	www.netflix.com	blocked	288 B
38	2015-11-05 17:37:49	Freeware and Software Downloads	ciscobinary.openh264.org	blocked	324 B

Figure 4. Example of detailed web browsing activity which allows education establishments to stay alert.

The first UK Fortinet Partner of Excellence

In 2014, Fortinet named Infosec Partners the title of their first ever Fortinet Partner of Excellence in the UK in recognition of our expertise in full-spectrum cybersecurity and proven capability to configure, manage and integrate their entire portfolio of security solutions (the first UK company to attain the Fortinet NSE 7 certification), along with that of any other vendor.

In 2016, it has never been more important to have a fully integrated security ecosystem, as evidenced by the response to the launch of Fortinet's Security Fabric and Fabric Ready vendor partner programme.

Securing Education

From the most prestigious independent schools to the country's top universities, Infosec Partners has helped education establishments to successfully develop robust security strategies and manage Safeguarding.

We listened to our clients and designed Infosec Partners services specifically for schools. Combined with the #SecuringSchools Crusade, including keynote speaker and security workshops at education events, #SecuringSchools Services helps schools understand the new threats facing them and teaches them how to take control of information and cyber security.

Working with Education organisations such as the Independent Schools Bursars Association (ISBA), Infosec Partners improves awareness of cyber threats and provides schools with tailored advice and expertise to meet their specific security needs.

Teacher's Control:

The Teacher's Portal by Infosec Partners, is a unique solution for schools and colleges, which combines the latest technologies in security and control systems, and allows teachers to take back control of their classrooms.

The modern classroom is a dynamic learning environment that's interactive and collaborative. The Teacher's Portal allows multiple participants to connect wirelessly and share content on a screen, or switch from one device to the next for seamless presentations and collaboration on the fly.

In addition to convenient controls for lighting, curtains and blinds, audio and visual equipment in the classroom, Teachers are also granted visibility over protection systems including internet access privileges and content filter settings by class, student and computer, simultaneously empowering Teachers and reducing the load on IT staff resources.

InfosecPartners
CYBERSECURITY

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

Secure your school, contact us today.

01256 893 662

secure@infosecpartners.co.uk

Infosec Partners Ltd.
The Long Barn, Tufton Warren
Hampshire RG28 7RH
United Kingdom