Providing a Safe Learning Environment
Safeguarding Students with Fortinet
Introduction

Whether a single local authority maintained school, or part of a multi academy trust (MAT), providing a safe and secure learning environment is a critical part of safeguarding duty. Schools are increasingly making use of online tools such as Office365, Google Classroom and educational applications hosted on AWS or Azure. There is also formal collaboration and sharing of systems between schools, and provisioning of Internet access to staff and students. Whilst these assist in providing a modern and stimulating curriculum, they can expose children, staff and school assets to cyber threats.

The government’s Prevent and Safeguarding agenda goes some way to help schools minimise their exposure to cyber threats through recommending the use of content filters and blocking of inappropriate content. However, the nature of modern threats means content filters and firewalls alone cannot always identify whether something is harmful or not. For example a new variety of malware which has just been released and does not yet have an antivirus signature.

Another example is where schools are collaborating with each other and malware is passed via a trusted connection to another school without passing through a firewall or content filter.

Did you know?

The term malware is often associated with ransomware which encrypts computer hard drives and then demands a ransom to decrypt them. However, there are lots of types of malware and it can be used to perform tasks such as capturing usernames and passwords, stealing personal data like names and addresses, or even spying on computer users through their camera or monitoring their typing.

Firewalls, antivirus tools and content filters still play a key role in blocking inappropriate content and yet ransomware attacks such as WannaCry, Petya, and others still succeed in getting in. So how does a school allow safe access to information, make use of cloud services, and see the benefits of collaboration, without overblocking and inhibiting learning?

A Secure School – More Than Just a Firewall

A common approach to protecting against cyber threats is to add more equipment to what is already installed. This usually leads to complexity; different management tools for each device, multiple vendors to deal with from a procurement and support perspective, and a network made up of devices which operate independently and so cannot react as a “system.” Considering the range and scale of threats – from computers being encrypted with ransomware, to students being exposed to extremist views – the more appropriate reaction should be to consider a solution that addresses all of the IT needs of the school, including security, in a simple and easy to manage way. Fortinet offers a modular architectural approach called the Fortinet Security Fabric, which can quickly identify new threats and automatically protect the whole network, whilst keeping management, monitoring and configuration as simple as possible. Fortinet’s modular approach allows the most suitable components to be chosen, so benefits can be seen for individual schools as well as Local Authorities or MATs who wish to provide centralised services to a number of schools or academies.

Fortinet’s philosophy of delivering best in class Enterprise security solutions at a competitive price point is well aligned to the real-world challenges of schools, and can deliver easy to manage, high quality secure connectivity within the constraints of an increasingly challenged budget.

---

1 as defined in the Department of Education’s “Keeping Children Safe in Education” statutory guidance (updated in July 2021).
The Fortinet Security Fabric – a Modular Approach for Schools

Many cyber security threats, such as Wannacry, are indiscriminate and while not targeting a school specifically, can still cause disruption or even loss of important files like exam papers or student records. However, some threats are more targeted and there are specific considerations for schools, particularly when thinking about students being targeted by extremist or ideological groups. All of this means that schools need to consider a solution to protect against a broad range of threats but be easy to use and manage.

The Fortinet Security Fabric consists of a number of technologies which are designed to work collectively or independently. This modular approach allows schools and MATs to choose the most appropriate solution which will grow with them. For example the primary goal of complying with Prevent and Safeguarding duties can be met, but over time additional functionality can be added to further enhance the security posture.

These technologies range from firewalls to wireless access points, secure switches, secure email gateways and client software and are available in a variety of models to cater for any deployment size.

While this may seem like an overwhelming choice of products aimed more at a large Enterprise, most are relevant in a school environment and can be specified in a size and form factor to suit. Not only that, but many of the components can be managed and monitored from a common interface, ensuring day to day management is as easy as possible.

The Fortinet Security Fabric allows a school, MAT or Local Authority to improve their security posture one step at a time by:

1. Helping meet the Safeguarding guidelines
2. Delivering protection beyond Safeguarding
3. Providing secure unified access

1. Meet the Safeguarding Guidelines

Blocking access to harmful, inappropriate and dangerous websites is essential in order for a school to fulfil their Safeguarding responsibilities. The Fortinet Security Fabric can prevent students from visiting malicious sites, shield them from inappropriate online material, and maintain a safe and productive learning environment.

The Fortinet Security Fabric allows schools to make informed and automated decisions about which websites and online resources students can access, and which content they can download, instead of “over-blocking” and stifling educational access.
<table>
<thead>
<tr>
<th>FEATURE</th>
<th>FABRIC COMPONENT</th>
<th>PREVENT AND SAFEGUARDING BENEFIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block access to inappropriate websites</td>
<td>FortiGate Firewall with URL filtering subscription</td>
<td>Schools and governing bodies need to ensure children are protected from harmful and extremist content, through the use of appropriate filters and monitoring systems. (Section 67, Page 62 and Page 57 of the KCSIE Government document).(^2)</td>
</tr>
<tr>
<td>Monitor Google, Bing and Yahoo searches</td>
<td>FortiAnalyzer</td>
<td>By providing easily readable reports, and by storing monitoring information for a period of time, Fortinet is supporting schools in their requirement to implement monitoring.</td>
</tr>
<tr>
<td>Detailed logs of user browsing history</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reporting, monitoring and log retention</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network, desktop and server antivirus</td>
<td>FortiGate Firewall with network level antivirus</td>
<td>Part of protecting children from inappropriate content and radicalisation is ensuring that malware is not installed on their machine, which could install keystroke loggers or open up remote webcam access to monitor them with, or install software which presents them with offensive or inappropriate content.</td>
</tr>
<tr>
<td></td>
<td>FortiClient endpoint protection</td>
<td></td>
</tr>
<tr>
<td>Remote access for students, including blocking inappropriate websites</td>
<td>FortiClient endpoint protection software</td>
<td>By providing filtering and monitoring of student activity whilst they are away from school, students can be protected from inappropriate and offensive content.</td>
</tr>
<tr>
<td>and content while the student is away from the school</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


## 2. Protection Beyond Safeguarding

The government’s KCSIE document notes that whilst filtering and monitoring are an important part of the online safety programme for schools to consider, it is only one part, and a “whole school approach” to online security should be taken. Looking beyond the Filtering and Monitoring stipulation within the Prevent and Safeguarding, recommendations should include consideration of threats which cannot be detected by web filters and firewalls. Examples of these types of threats can include malware spread by email, phishing email campaigns, USB keys, and advanced threats which are not detected by traditional signature based filters.

Email is the most common way to spread ransomware and other malware and inappropriate content – either by attaching an infected document or by tricking a user into clicking through to an infected website. Yet firewalls and web filters cannot always identify the malware in the email because the malware is too new to be detected by their antivirus signatures.

Not only should schools consider suspicious activity and content which can get into a school from the Internet, but also the spread of content within a school, or perhaps between schools collaborating with each other.

As well as helping schools meet their Prevent and Safeguarding duties by providing web filtering, antivirus and monitoring, the Fortinet Security Fabric can be used to detect new malware whether it arrives in an email, on a USB key, or through web downloads. In most cases you can automatically stop it from getting into the school in the first place. Schools, MATs and Local Authorities can pick the most relevant components as needed, or as part of a phased roll out.

While each component offers value by itself, the unique ability of the Fortinet Security Fabric to share information between all components, and automatically update and react means that the greatest benefit is seen by using as much of the Fabric as possible.

The UK Safer Internet Centre (https://www.saferinternet.org.uk) has defined a set of guidelines to help schools understand what is appropriate filtering and monitoring, in order to meet their obligations under HM Government’s Prevent Duty, and the Department of Education’s “Keeping Children Safe in Education” document.

We are fully compliant with the UK Safer Internet Centre’s guidelines including membership of the IWF (Internet Watch Foundation), blocking access to Child Abuse Images and Content (CAIC), integrating the police assessed list of unlawful terrorist content as assessed by the Home Office, and offering many advanced features such as providing age-appropriate differentiated filtering, and filtering traffic from mobile apps not just web browsing. More information can be found on the UK Safer Internet Centre’s website or by contacting your Fortinet account manager or supplier.
### 3. Secure Unified Access

In order to minimise the likelihood of a malware infection, and to contain the spread of any infection, it is important to have enforcement as close as possible to the end user. For example if a student’s computer is not running the latest antivirus or has not been patched, it is more likely to become infected by malware. If it does become infected it may be able to infect other computers in the school as it is already inside the trusted school network. By enforcing compliance of that computer, making sure it is up to date, and quarantining it locally if it is not compliant, the risk of exposure to malware is minimised.

A key way of achieving this objective is to incorporate security into the underlying network as much as possible. Traditionally, connecting to the network was separate and distinct from securing the network. A much more comprehensive approach is to have the access network, wired and wireless, function as an extension of the security infrastructure. This ensures a consistent security posture with equal protection regardless of the type of connection. This approach also simplifies procurement and day to day management of the network.

Fortinet’s Ethernet switches and wireless Access Points (APs) play an active role in providing a safe environment for staff and students, by integrating with the Fortinet firewalls and the other Fortinet security devices. This allows enforcement of security policy at the user access level while at the same time simplifying management, configuration and monitoring. Users can be quarantined, traffic filtered, and separation of different users from each other can be achieved easily.

### Table: Security Fabric Components

<table>
<thead>
<tr>
<th>Feature</th>
<th>Fabric Component</th>
<th>Prevent and Safeguarding Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint compliance checking and quarantining</td>
<td>FortiClient endpoint protection</td>
<td>Prevent computers being connected to the network which do not have sufficient antivirus, personal firewall, or patch levels. This should minimise the risk of computers becoming infected and introducing that infection to the school’s network.</td>
</tr>
<tr>
<td>Unknown malware detection</td>
<td>FortiSandbox</td>
<td>Identify malware which has not been seen before, and cannot be detected by antivirus signatures and web filters.</td>
</tr>
<tr>
<td>Secure email – email quarantining, anti-spam and anti-phishing</td>
<td>FortiMail Can either integrate with Office365 and other email solutions, or provide a self contained email platform.</td>
<td>Detect and quarantine suspicious emails and content so they are not sent to students and/or staff. This reduces the risk of infection via email and protects email users even in the case of new malware.</td>
</tr>
<tr>
<td>Advanced monitoring and reporting</td>
<td>FortiAnalyzer</td>
<td>Knowing what is happening in the school network is important, so that security incidents and threats can be quickly identified and dealt with.</td>
</tr>
<tr>
<td>Compliance reporting (e.g. PCI) and multi-vendor monitoring</td>
<td>FortiSIEM</td>
<td>Reporting is an essential part of many compliance requirements. Failure to report can result in fines, or removal from the PCN and other networks or services.</td>
</tr>
<tr>
<td>Cloud access monitoring</td>
<td>FortiCASB</td>
<td>Monitoring and scanning data stored in cloud applications such as Dropbox, extends the school’s ability to protect students.</td>
</tr>
</tbody>
</table>
In Conclusion

Schools – whether operating as a single school, or part of a MAT or Local Authority managed group, have a responsibility to protect students from exposure to harmful or inappropriate material. Compliance with the Prevent and Safeguarding guidelines is the initial part of providing protection, but there is also a need to protect staff, students and school assets from new evolving cyber threats such as ransomware, and provide a reliable and secure environment for learning. The Fortinet Security Fabric offers a modular way to achieve this in a way which is easy to configure and monitor and highly effective.

Please contact your Fortinet account manager or reseller for more information, or to arrange a demonstration of our capabilities.