Smoothwall for Education

Whitepaper

Digital Safeguarding

Reducing violence in schools with digital threat detection

A practical guide for Superintendents

smoothwall®

us.smoothwall.com

Whitepaper

1.0 About this document

This document is a practical guide to help schools and school districts understand how digital threat detection can help identify and eliminate threats to student safety.

Written by Smoothwall's online safety experts, it explains what digital threat detection is, how it can detect children at risk of harming or being harmed and how your schools can integrate it into their existing school safety plans.

It answers the key questions many school and district leaders are asking and shares real cases of threat detection in action.

If you have any questions about digital threat detection, its implementation or digital safety in general please do not hesitate to contact the Smoothwall team.

We'd be happy to help.

About Smoothwall

Smoothwall is a leading web filtering and digital threat detection developer. Since 2001, Smoothwall solutions have protected millions of students worldwide.
We pioneered the development of real-time content aware web filtering and have since launched further threat detection and safeguarding solutions to protect users in the digital world.

Proactively developing and improving our products based on the needs and requirements of schools is what we do best and is what makes us a leading safeguarding provider in education.

smoothwall®

2.0 Introduction

For most children in the U.S. the Internet, computers and mobile devices are all part of everyday life.

Today's students are true digital natives — the first generation to know social media and mobile devices since birth.

The widespread accessibility to technology and the Internet has also expanded learning opportunities beyond the classroom.

Now 90% of students use digital learning materials at home. Although that's a great advantage for schools, it brings with it inherent dangers.[1]

The constant exchange of communication and information mean many students live in a perpetual state of being "online", with their combined social and education lives all within the palm of their hands.

This constant hyper connectivity has resulted in a surge in the number of children and young people suffering from mental health issues - with many more, it is believed, suffering in silence.

Studies are now warning about the link between time spent on social media and mental health problems, amongst teens in particular.[2]

Many students suffering from mental illness who went on to commit violent attacks in recent years had expressed concerning behavior on social media beforehand.

Prevention is now more critical than ever. 2017-2018 was the deadliest year for students. It had the highest death toll in a single academic year from school shootings in recent decades.[3]

As part of its response, the Federal Government has now strengthened its commitment to technology as a means of addressing these threats.

In July 2018, the Federal Commission on School Safety, in partnership with the U.S. Secret Service, published a comprehensive guide on preventing school violence. The guide advises schools to examine online behavior scanning as one of three recommended assessment procedures.

Despite this, many schools and their school districts are still unclear about how to safeguard children. Many are unaware of the role threat detection can play in identifying students at risk of being harmed or causing harm.

[1] Merchant, Richard Greg, and Preeta Banerjee. (2016). Digital Education Survey. Deloitte Development.

[2] The Impact of Social Media on Children, Adolescents, and Families. , Apr 2011, 127 (4) 800-804; DOI: 10.1542/peds.2011-0054

[3] Decker, Stacey, and Evie Blad. "School Shootings This Year: How Many and Where." Edited by Holly Peele and Hyon-Young Kim, Education Week, Editorial Project in Education, 15 Nov. 2018 www.edweek.org/ew/section/multimedia/school-shootings-this-year-how-many-and-where.html.

Social media was the most common source of threats in the 2017-2018 school year, accounting for 39.2% of all threats.

Violent Threats and Incidents in Schools: An Analysis of the 2017-2018 School Year The Educator's School Safety Network (ESSN)

3.0 The growing dangers

Why the need for digital threat detection.

Why schools are in the dark

With social media now an ever-present consciousness in young people's lives, a constant obsession to obtain the most Snapchat streaks or Instagram likes can mean they are prepared to expose themselves to unknown contacts and immense risk.

From violent and threatening messages to sharing inappropriate images, schools can struggle to keep up and are often in the dark about what's really going on.

All students with an online presence are at risk.

The fact is serious risks are often shared online before anything happens.

Whether it's a student with a gun in their backpack, a student who is hours from suicide, or a student about to engage in illegal drug use – sometimes a clue that something may be about to happen can only be seen through their use of technology.

Without appropriate digital threat detection schools are left to rely on what they see and on what other students tell them. Neither factors are reliable.

Identifying risks that may otherwise go unnoticed

Digital threat detection enables school leaders to identify risks that may otherwise go unnoticed.

It gives a deeper picture of issues and concerns, alerts you to issues at an earlier stage and provides you with clear-cut evidence that's vital when working with external agencies and partners.

Digital threat detection is becoming one of the most effective means of preventing harm in schools today.

Where physical security measures can prevent a threat at the school gate, digital threat detection provides crucial insight into student behavior much earlier, facilitating intervention before a low-level risk becomes a live and present threat.

The impact of unidentified risk

The Centers for Disease Control and Prevention (CDC) reports that among U.S. high school students, health risk behaviors – specifically those related to substance use, sexual risk, violence and mental health and suicide – are linked to lower academic grades.[4]

When young people are not able to process their emotions or understand their mental illness, they can resort to extreme measures such as self-harm, suicide and violence to others.

The school district's challenge

School districts are now under more pressure than ever to ensure student safety.

In large and commonly overstretched school districts and with class sizes often more than 30, identifying every risk may feel like an impossible task.

And it's not getting any easier.

The online threats to a child's safety and well-being are increasing all the time.

Assault

Every day, approximately **100,000** children are assaulted at school.

Source: CDC, National Center for Injury Prevention

Suicide

1 in **6** high school students has seriously considered suicide.

Source: CDC

Bullying

1 in **7** students in Grades K-12 is either a bully or a victim of bullying.

Source: CDC, National Center for Injury Prevention and Control

Self-harm

70% of students who self-harm are female.

Source: National Association of School Psychologists

Mental health

20% of youth ages **13-18** live with a mental health condition.

Source: National Institute of Mental Health

Abuse & grooming

1 in **25** youth received an Online sexual solicitation where the solicitor tried to make offline contact.

Source: Wolak et al

[4] "Adolescent and School Health." Centers for Disease Control and Prevention, Centers for Disease Control and Prevention, 17 Aug 2018.

4.0 What is digital threat detection and how it works

As online dangers continue to increase so does the technology capable of addressing them.

What is threat detection?

It's not all bad news however. As online dangers continue to increase so does the technology capable of addressing them.

Digital threat detection is a technology based solution specifically designed to scan for signs of danger.

A child at risk of harming or being harmed will often consciously or unconsciously share their thoughts or feelings online. By scanning their keystrokes on any school device high risk words or phrases can be identified in real time enabling schools to intervene early and avert the risk.

Serious issues such as a suicide risk, violence against other students, drug use, and other factors can all be detected in real-time if a child has used their keyboard in any way to view content, message someone, look for information, type out their feelings – even if they delete it immediately or never press 'send' or 'enter'.

Digital threat detection creates a deeper layer of visibility for Superintendents, Principals and Teachers - all of whom are responsible for student safety but who, in normal circumstances, often cannot see what is happening.

How it works

There are generally two types of active threat detection solution available:

1. **Non-third party moderated**
2. **Third-party human moderated**

Unmoderated

When a student or staff member types or views high-risk words into a digital device, a screen capture is made by the digital threat detection system. This capture could be of a browser, an email, a Microsoft Office document, a social media platform, a chat room or an encrypted app such as WhatsApp.

Digital threat detection is not like CCTV, it doesn't record everything. It only captures moments of online activity that are identified to have implied risk.

The system will immediately create a risk-grade based on the captured activity. Schools can see risk alerts in real-time, easily enabling them to act on severe alerts immediately. By accurately grading risks, schools can decide which alerts need their immediate attention and which can be dealt with later.

Lower level alerts are not discarded. In a robust intelligent solution, they will be analyzed to uncover any concerning patterns and trends.

For example; a student searching online for 'magazine' and then later chatting on Facebook Messenger about 'clip', could indicate they are describing a loaded firearm.

This search is seemingly harmless, and without the system's trend analysis, that student may go undetected.

Moderated

The other type of threat detection is one that is human moderated. In this solution, a capture is made in the same way as before. Artificial Intelligence (AI) then analyzes the capture and creates a profile of the alert context. AI analysis can remove false positives and escalate the alert if it is flagged as concerning activity. The capture is then sent to a human moderator for further analysis.

The analyst grades the capture and decides on the severity of the alert. They will also remove any further false positives if there are any present. Severe alerts are immediately sent to administrators and alerts that do not require immediate review may be sent in scheduled reports.

Most providers have a safeguarding portal for educators to log in and see the full context of the alert and gather any additional evidence that may be required.

Educators are encouraged to understand how social media can help prevent and respond to crisis risks.

Social Media and School Crises National Association of School Psychologists

Illustrative case scenarios

The following cases show how threat detection can help you identify risks. These scenarios are based on real stories although the names and details have been changed to protect confidentiality.

Threat detection type: **None in place**

Marie 7th grade

Risk type:
Cyberbullying & self-harm

1. Marie moved in the middle of the school year and was having trouble fitting in.

2. She became depressed and began a Word document on her computer as a diary.

3. As her depression worsened she read a forum online about depression and began to cut herself.

4. She covered her arms and legs for weeks to hide her self-harm. It wasn't until she started gym class that her teacher noticed the scars.

5. If digital threat detection had been used, this risk could have been spotted and she could have received treatment.

Brian 9th grade

Risk type:
Violence against others

1. Brian brought a knife into school.

2. He messaged one of his peers that he was going "to get" Peter from his science class for making fun of his shoes the other day.

3. Later that afternoon, Brian attacked Peter.

4. The log was found the next day by administrators, after painstaking forensic analysis of the computer Brian was using.

5. If digital threat detection had been used, this risk could have been spotted and the stabbing avoided.

Freddie 9th grade

Risk type:
Drugs

1. Freddie was working on a shared Google Doc with a friend.

2. Freddie quickly typed in "want to light up after class?". The friend agreed and then deleted the words.

3. At break-time, Freddie and his friend met up and smoked marijuana.

4. The use of drugs was discovered several weeks later by another student that overheard their conversation but was unsure about reporting it.

5. If digital threat detection had been used, this incident would have been spotted and the drug-use avoided.

Threat detection type: **Digital**

Emma 6th Grade

Risk type:
Child exploitation

1. Emma was working on a project on her computer in the library.

2. She was sent a threatening email saying that if she didn't meet someone called Richard after school, he would post the photos she sent to him so that everyone could see what she had done (using serious sexual language). She was told "not to tell anyone" about the meeting.

3. The serious sexual language triggered a severe risk alert to administrators.

4. A school counselor received the alert. She was able to intervene by asking Emma to come and talk to her.

5. The counselor invited Emma's foster parents into the school and used the support of her social worker and other administrators to help.

Richard was reported to the police and the school was able to provide law enforcement with clear evidence of the incident. The threat detection system de-escalated the problem and ensured Emma received the help she needed.

Matthew 7th grade

Risk type:
Gun violence

1. Matthew was in a math class where the teacher had set a 20-minute assignment.

2. While his teacher helped another student on the other side of the classroom, Matthew wrote a note on screen, "I think James brought in a gun".

3. An alert was triggered at this point and sent to school administrators. Matthew nudged his best friend to take a look. His best friend saw it but then Matthew's math teacher called the class to attention. Matthew quickly deleted the note on his screen.

4. The responding administrators had seen the alert and its severity. Having a full safeguarding picture of the school, the administrators knew which James the note was referencing.

5. They de-escalated the situation by immediately sending a law enforcement officer to disarm the student in the classroom without causing excess panic.

Sara 9th grade

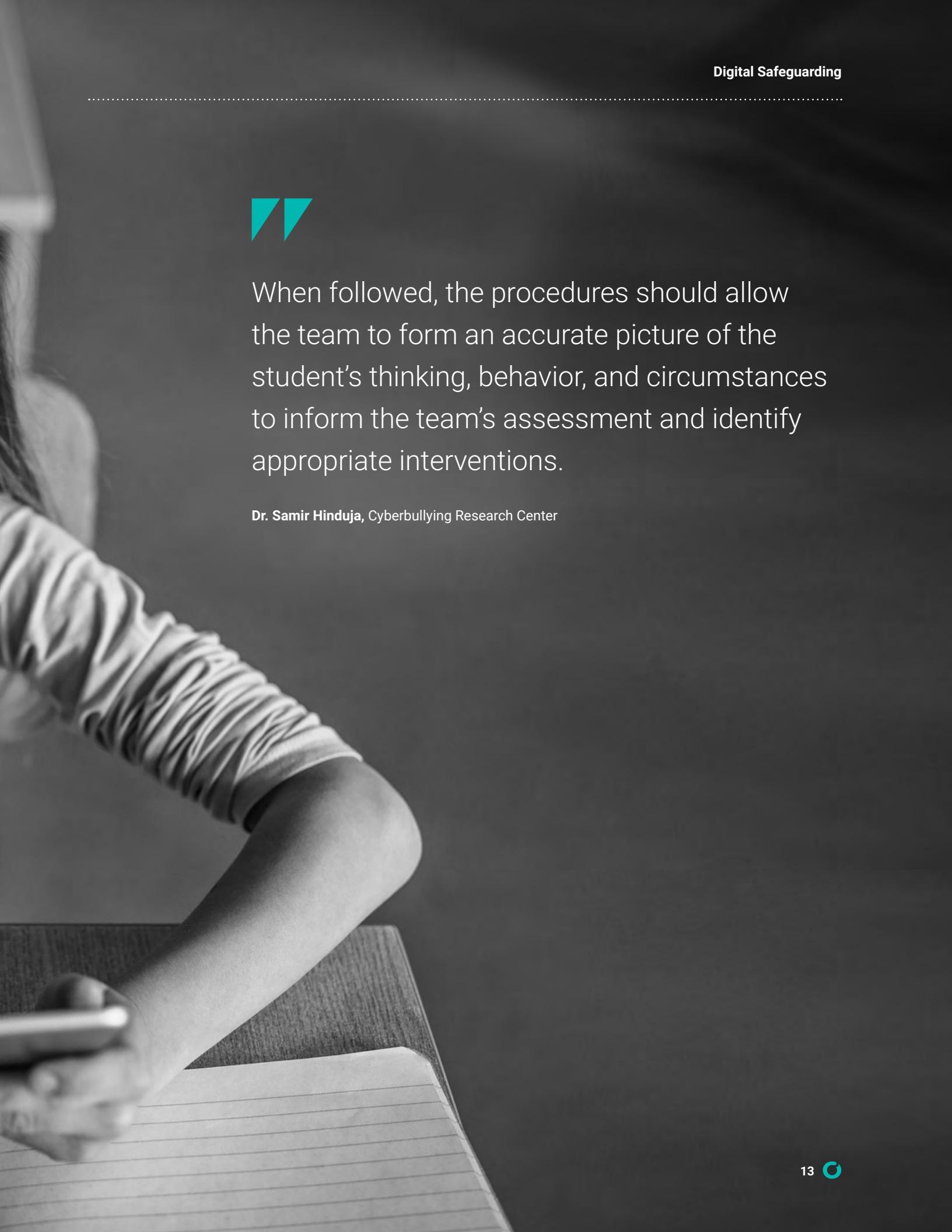
Risk type:
Bullying

1. A relationship rift had caused a group of girls to set-up a "we hate Sara Jones" Facebook group.

2. The girls posted harmful messages anonymously in the group with cruel comments.

3. Sara told a teacher but didn't know who was involved.

4. The school added customization around Sara Smith's name on the website. The administrator received alerts of 5 girls adding to the group within 24 hours and could follow up on the situation.



When followed, the procedures should allow the team to form an accurate picture of the student's thinking, behavior, and circumstances to inform the team's assessment and identify appropriate interventions.

Dr. Samir Hinduja, Cyberbullying Research Center

5.0 Evaluating a threat detection solution for your district

What makes a good threat detection solution

The first steps to selecting and implementing a threat detection solution is for the Superintendent to assess the gaps in current threat detection procedures.

We call this stage ASK, ASSESS, DEFINE.

1. ASK your schools to review their current threat detection practices

Ask your schools to review whether they are using the most effective solutions to identify students in need. The matrix provides general guidelines together with a traffic light system to highlight where, if any, their threat detection gaps may be.

	Effective threat detection	Basic threat detection	Weak threat detection
Policy/set-up			
Age	The system is entirely customizable and can be set to respond to different age groups.	The system has some customization features between grade levels.	Students have restricted access to device features and only use approved features. Teacher supervises students, looking for at-risk students.
Threat detection policy	An acceptable use policy is used, and digital citizenship is embedded into the culture of the school.	An acceptable use policy is applied to all students.	Students are limited to specific websites when using the internet.
Devices	The system can scan all school-owned devices.	The system can support all managed devices in school.	Only works on desktop computers or only physical scanning used.
Processes			
Prioritization alert management	Alerts work in real-time and enables administrators to address concerns when needed immediately. They are activated by various sources, both online and offline.	Alerts are risk-graded but administrators are not notified in real-time. Alerts may not appear outside of the browser. The system may be limited to the amount of information included in captures.	Only compatible with desktop computers. Physical scanning by teachers used, only during school hours.
Flexibility	Intelligent analysis and profiling is used to gain a full picture of a student. Added human moderation will ensure only the right risks get through and with the right severity level.	Schools can customize their risk-grading and words to fit the cohort. They can customize by class groups to avoid curriculum captures.	Administrators look through logbook for evidence of issues. Limited or no prioritization of activity. Limited categorization capabilities. School depends on teacher top see an incident.

Procedures			
Reporting and evidence	The full context of an alert can be viewed in a report. Grade-level trends or student profiles can be analyzed.	Context is given with screen shots as evidence.	Logbooks take time to ensure nothing is missed. Limited evidence given. Relies on busy teachers to report activity.
Threat detection policy	An acceptable use policy is used and embedded into the culture of the school. It is also used for the purposes of teaching online safety.	An acceptable use policy is used with all students.	Students are told what they should do when accessing the internet.
Data storage	Data is held in a guarded offsite setting with robust levels of online protection.	Data is held in a secure setting with good online protection.	Data is held physically on site and has no additional security restrictions.
Impact			
What is the outcome and impact of your	Alerts are risk assessed in real-time through AI, resulting in a precise capture of activity. Only designated administrators have access to review alerts and notify stakeholders.	Alerts are listed by severity level. The system relies on the administrators to review alerts. Gives text evidence, no screen capture.	Alerts not acted upon quickly enough. Evidence is limited. If incidents are reported, privacy protocols are weak and student anonymity may be at risk. Potential for rumors to spread around the school.
Compatibility			
Size of school district	Larger settings dealing with many students and where staff time is limited. System uses profiling, AI and human moderation to make sure a school doesn't miss anything important.	Settings where administrators have the time to go through alerts and false positive. Contextual evidence is not factored if they are forming a plan of action.	Small settings in which students work in very small groups with simple networks or have additional dedicated staff.

2. ASSESS areas of non or weak compliance to determine level of threat detection support needed

The result of the review will determine your next step. If your schools predominantly report green-level practices, the need for further action will be low.

If your assessment reveals varying levels of provision, you may consider recommending a technology-based threat detection solution to individual schools who need it most.

If your assessment reports predominantly amber or red-level practices, you may wish to implement school-wide threat detection as a means of raising standards quickly and to an appropriate level.

Remember: A good threat detection provision will allow you and other school leaders to form an accurate picture of a student's thinking, behavior, and circumstances to inform appropriate interventions. This is the guidance from the U.S. Secret Service, Enhancing School Safety Using a Threat Assessment Model: Creating a Comprehensive Targeted Violence Prevention Plan.

3. DEFINE an approach to implementation

Smoothwall's threat detection solutions can be deployed within a single school or set up to scan multiple groups of schools from a central point.

Threat detection systems rely on a dedicated person within the school or district office to scan alerts raised by the system. If your preference is to scan multiple schools, then settings can be customized to give individual schools access to the customer portal to see own captures, while an overall scan within your governing body keeps an eye on all schools.

6.0 How to integrate threat detection into your school safety plan

It's important to ensure that digital threat detection is integrated effectively and efficiently into your current school safety plan.

Failure to do so can cause conflict and missed threats, ultimately compromising school and student safety.

The following are key points to consider when choosing the right solution for your district.

Risk assessment

- Will the threat detection solution fit into your current prevention processes to identify students at risk?
- Will the features effectively assess activity and categorize flagged risks?
- Will it be easily accessible to administrators in order to determine levels of risk without missing major concerns?
- Does the solution allow you to take proactive measures or promptly react to concerning activity?
- Does the system function in real-time?
- How long does it take for an administrator to receive alert?
- Can it be customized to scan activity based on grade-level?
- Can it be customized for a specific school?

Data privacy

- Does it include online and offline captures?
- Can it scan browsers, e-mail, Microsoft Office files, offline apps, chat rooms, and encrypted messaging?*
- Would you like to scan devices outside of school hours and/or off-site?
- Is the information gathered limited to designated administrators?
- Who will be notified of alerts? What types of alerts will they receive?
- Does the system provide detailed evidence of the alert to share with relevant administrators or parents?
- Does the alert produce a physical capture that provides further context to the associated activity?
- Will it give you a better understanding of risks that may not involve time in school or at home without invading student privacy?
- How will the solution store data?
- Is it kept in a secure setting?

Action plan

> Consider who will receive notifications and who will respond to severe alerts requiring immediate action. Think about the role of each, including district leadership, school principals, school mental health professionals, counselors, and school law enforcement.

> Who will receive notifications and who will respond to alerts of high severity that require immediate action?

> What information can administrators see when they receive an alert?

> Can you set an activity threshold before the risk is escalated to a high-risk alert?

> If high-risk activity scanned out of school hours and/or off-site, will administrators receive real-time alerts? If so, how will they respond?

***Note:** Alerts are just as likely to come from an offline Word document as they are from a more obvious source such as a chat room or email. Not having this level of reach will impact the breadth of risks captured.

7.0 Frequently asked questions

How much should we expect to pay for threat detection?

Digital threat detection solutions range in price depending on the number of users scanned, the quality and range of scanning, whether it is real-time risk grading, moderated by humans or AI, and other factors. Most quality providers, like Smoothwall, will offer solutions to match your unique requirements and budget.

How are other schools budgeting for this?

Sources of budget vary from state to state. Since most budgeting decisions are made at a district level, some district leaders may choose to fund it from their school safety budget if they have one.

The Federal STOP School Violence Act of 2018 reauthorizes a Justice Department program focused on stopping school threats. It provides $50 million per year for states to strengthen their school safety measures and was amended to include funding for technology such as reporting systems for threats of school violence.

Digital threat detection is eligible for funding as a reporting system for threats of school violence. Not only does it report on threats of school violence without relying on tip lines, it also reports student safety concerns such as suicide, self-harm or drug abuse. Funds are dispersed as state-based grants.

To find more information on your state's school safety budget, contact your state education agency.

How does digital threat detection protect student privacy?

A trustworthy provider will strive to not only protect students, but also their privacy. At Smoothwall, our digital threat detection solution is only activated to capture instances that our intelligent technology identifies to carry risk; information that is not identified to carry risk does not activate threat detection therefore it is not captured.

Only designated school administrators will receive alerts and have access to this information. It is then up to school policy as to how and when administrators respond on alerts. Smoothwall will only access information if administrators request technical support.

How do we know that a threat detection system will store our data securely?

You will need to ensure the safety of your sensitive data. Providers should be able to show evidence of where your data is stored. At Smoothwall, data privacy is a top priority and all data is stored in a secure Microsoft Azure protected cloud data site in the U.S.

How can we check the impact a threat detection solution might have on our School's IT systems?

You should check with your vendor that their software is discreet and that your technical environment has the required capacity to support it on your school network. Smoothwall's threat detection solutions have no impact on performance and work silently in the background as well as complement any web filter. A student will not be aware that threat detection is taking place or that a capture has been taken when they are using a device.

What's involved in implementing a threat detection solution?

Installation can vary by provider. Ask if there is a requirement for staff to have specific technical knowledge and if the system is cloud-based. At Smoothwall, installation is simple and straight forward with no technical knowledge required. It can be as easy as flipping a switch, or a simple download, depending on your current filtering provider.

We already have web filtering, why do we need threat detection as well?

Web filtering blocks content to prevent students from accessing it. It is critical for your schools as it ensures that they are blocking adult content to remain compliant with the Children's Internet Protection Act (CIPA). However, web filtering cannot scan what a student types into their computer. Most web filtering systems do not send alerts in real-time, giving schools the ability to promptly act on high-risk activity. Threat detection and web filtering work hand in hand to provide your schools with a robust digital safety capability that helps you keep students safe.

Our schools are overstretched as it is. Won't threat detection add more safety concerns to address?

Most providers understand this and will offer a choice of solutions to match the level of capacity your schools have available. At Smoothwall, solutions are customizable and can range from custom alerts, to manual severity risk grading.

Will threat detection make unnecessary captures of content used for educational purposes

In some solutions, customization is available to manage your risk settings so that you can remove key topics for specific classes. However, in doing this you should be careful not to remove content that might be needed. Every school has different requirements which is why a good threat detection system will vary and have flexible settings to suit your environment.

Is threat detection scalable for larger institutions?

If you are a larger district, it is important that you check to see how a provider can create a scalable solution to meet your needs. Ask them to explain the time-frame and process of installation. All Smoothwall threat detection solutions are easily scalable due to their simple installation, minimum impact on networks, cloud-based portal, and automatic updates.

Have a question?
Contact our online safety experts.
We'll be happy to help.

Tel: 1 800 959 760
Email: inquiries@smoothwall.com

Whitepaper

> Schools have every right to scan what's done on their property, with their equipment, on school-issued accounts.

Benjamin Harold, Education Week

What next?

Ask yourself

Are you confident that your schools are picking up, in real-time, each of the risk concerns on your school digital devices – online and offline?

Do your threat detection and safeguarding strategies match legislative requirements?

If you don't know, it's time to check. If you're unsure or have a question, contact Smoothwall's Online Safety Experts who will be happy to help.

Arrange a free demonstration

To see a free, no-obligation demonstration of Smoothwall's threat detection or to ask any questions please contact us.

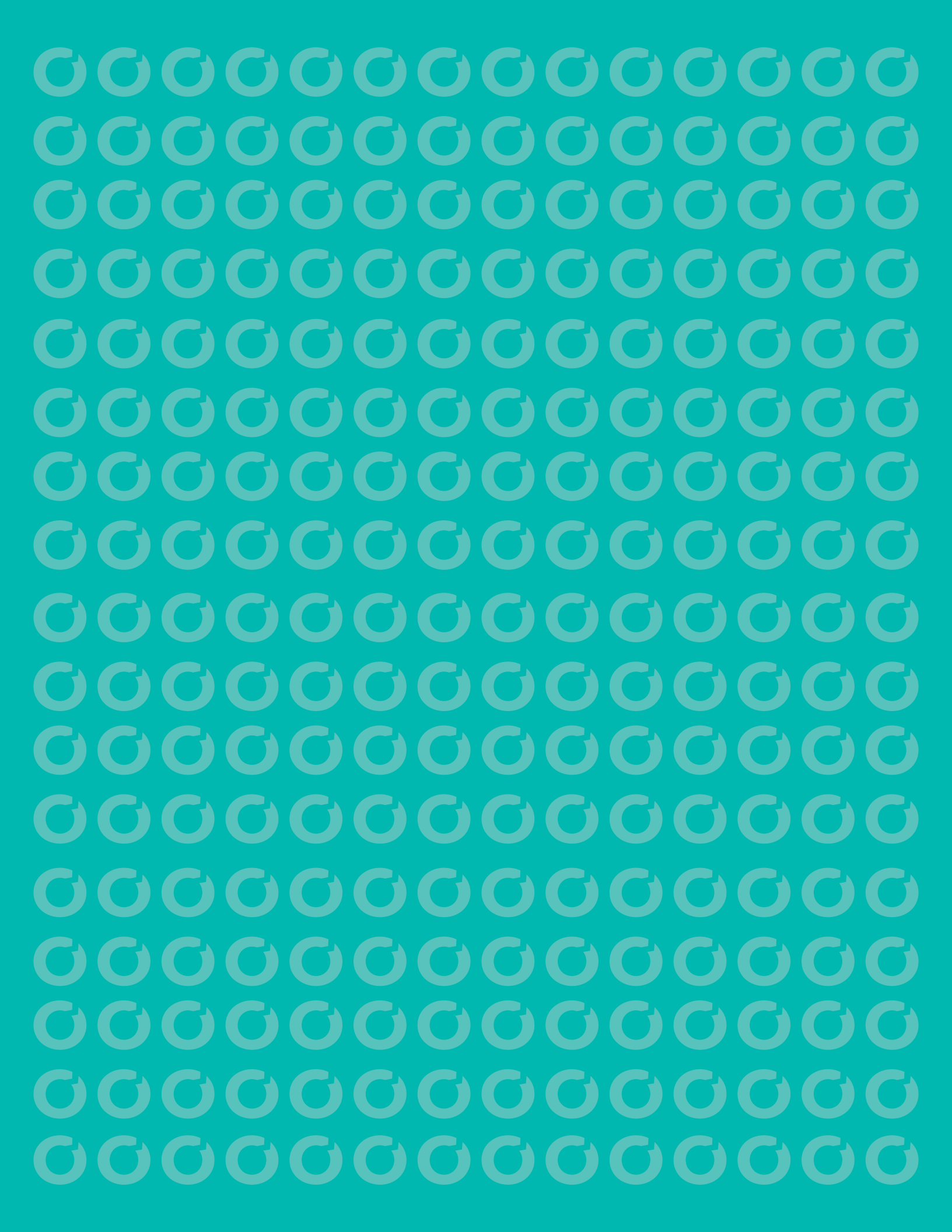
Smoothwall

1435 West Morehead Street
Suite 125
Charlotte, NC 28208

Tel: +1 800 959 3760
Email: inquiries@smoothwall.com

us.smoothwall.com

smoothwall®



Smoothwall

1435 West Morehead Street
Suite 125
Charlotte, NC 28208

Tel: +1 800 959 3760
Email: inquiries@smoothwall.com

us.smoothwall.com

SmoothwallUS
Smoothwall US
Smoothwall-Inc
SmoothwallTV

smoothwall®