Linewize
BY FAMILY ZONE

UNDERSTANDING VPNs

The acronym “VPN” stands for “Virtual Private Network”. You will very likely have heard this term before, or certainly its abbreviated form, in conversations in the staff room or classrooms.

But what is a VPN, how do they work, and why do people, especially children, use them? To answer this question, we need some background.

The **internet**

The Internet is, in its simplest form, a vast public network of inter-connected devices. Every computer, laptop, phone, and many other familiar devices are connected in some way to the Internet. Through this connection we can access the information resources of the World Wide Web, the convenience of email, and many other services that today we take for granted.

Being public does not mean that it is insecure, nor that our personal information is necessarily exposed. Many interactions that require the security of data, such as purchasing something online with a credit card, are generally safe to perform.

However, there are cases where extra layers of network security are needed.

VPN's are the second most **frequently blocked category** during school hours.

#1 Social Media
#2 VPN
#3 Gaming
#4 Streaming Media

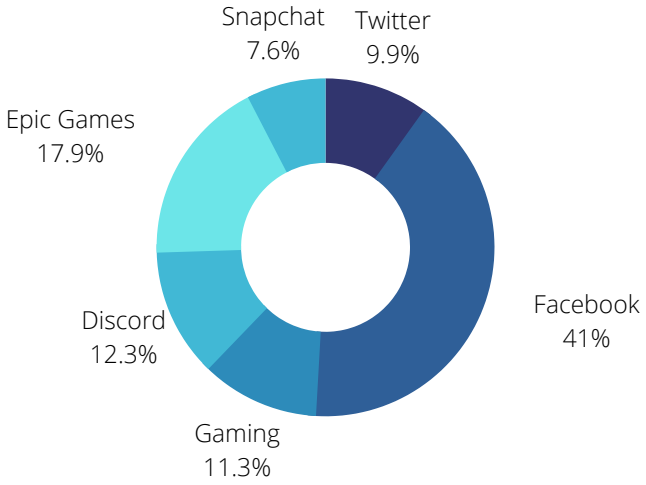
Private networks

The most common type of private network in peoples everyday lives is often a corporate network. Almost every business in the world has some kind of private network of devices, accessible only to the employees of that business. These private networks shield sensitive corporate data and prevent access to private network devices from the surrounding public network (the Internet).

Private networks of this nature will often host internal email, printer(s), and file storage services, amongst other things.

Distractions VPNs can allow

(Most blocked apps and sites)



Average data taken from March 2021 across 20 leading ANZ schools.

Virtual private networks

So what are “virtual” private networks? In short, they are private networks, hosted on the public Internet, that can be securely joined by any Internet-connected device. They are “virtual” in the sense that they overlay a public network and are comprised of otherwise unrelated devices.

So what are virtual private networks typically used for?

One of the main reasons that VPNs are used is that they allow a connected device, such as a computer, to masquerade in some way. For example, it is possible to connect to VPNs which will make a device appear as if they are within the United States, thus allowing access to US-only content (on Netflix, for example).

VPNs can also be used to circumvent firewalls and other traffic-blocking network elements. VPNs can do this by making access to explicit, illegal, or otherwise restricted content appear as normal network traffic. And this is why VPNs are an attractive tool to many, including students. However, if you know where to look, there are telltale signs of when a VPN is in use.

Top reasons students are using VPN's

Override schools networks

Steal online content

Anonymous use of the internet

Cyber Expert and Clinical Psychologist Jordan Foster from ySafe

Did you know?

VPNs are just one of many ways students can bypass school network filtering. Another common method is Hotspotting. Find out more in our School's Guide to Filter Avoidance.

Linewize and virtual private networks

Linewize benefits from partnering with in excess of 5,000 schools globally where our systems are constantly identifying new VPNs and adding these to our block lists.
As a company, we use three primary methods to detect and block the usage of VPNs.

They are:

1. URL lists;
2. Pattern detection with signatures;
3. Anomaly detection using artificial intelligence and machine learning.

Combined with the unique quarantining feature, the Linewize platform is the overall most capable platform for detecting, blocking, and discouraging the use of VPNs.

Significantly in excess of

50%

of middle/senior students are using or attempting to **use a VPN**.

Anonymous data collected from Linewize schools in 2020/2021

URL Lists

The first line of defence is Family Zone's massive database of website URLs. These are lists of known VPN provider websites.

This database is updated daily from various sources, including feedback from customers, to always stay one step ahead of the current and latest VPN apps as they come out.

Signatures

While operating, the traffic generated by VPNs may exhibit certain telltale patterns. The Linewize platform has a vast database of these patterns;

Signatures can include:

1. IP addresses and port numbers;
2. Connection behaviours;
3. Patterns within the data of the traffic itself.

When a pattern is detected the user attempting to use the VPN is immediately quarantined.

Anomaly **Detection**

New VPNs are being created all the time and therefore it is not possible to know, ahead of time, all of the currently active VPN traffic patterns. This is where the Linewize platform leverages artificial intelligence and machine learning.

Data from across the Linewize platform is crowd-sourced and ingested into these tools, which can then learn to differentiate between what looks like normal network traffic and what looks like VPN traffic. This process effectively creates new signatures that can then be used to block a VPN and quarantine users.

Discouraging VPN use (Quarantining)

The Linewize platform discourages VPN usage by quarantining users. In the context of the Linewize platform, “quarantining” means blocking all connections to the Internet (not just the ones associated with VPNs) for a set period of time. By default, this is 3 minutes but is configurable.

Quarantine on a user is triggered when tampering or circumvention activity is detected. This could be the act of trying to remove an agent from their laptop or accessing already-known VPN sources, which is a sign they are testing out VPN apps to see which one might be able to sneak past the filters.

The Linewize platform makes it easy for schools to see the heaviest users of VPNs. This subsequently allows the schools to take a targeted approach by only quarantining those students/groups that are of concern. Enabling Quarantine in such a targeted way is the best practice approach.

How has Linewize **positively impacted** VPN use in schools?

In a study of a large Australian independent school where Linewize was deployed in Month 1, the below table highlights the positive behavioural impact of a significant reduction in VPN activity by students over a 6-month period:

	Month 1	Month 6	% Reduction
VPN Attempts/Blocks - All	3,187,183 VPN hits	377,304 VPN hits	88%
Top 5 Offenders	510,777 VPN hits	21,698 VPN hits	96%

The following statement from Simon Ward, Director of Digital Learning at St Pauls Collegiate School Hamilton, New Zealand, highlights their experience with the Linewize VPN and Quarantine features:

> *"Just a quick note to say the Linewize Quarantine feature is excellent and has had an instant and dramatic effect on VPN use. Our use of VPNs is now zero which is so good to see".*

Book a Linewize **Demo**

Discover how Linewize solves your school's cyber challenges.

BOOK NOW →

About Linewize

The Linewize ecosystem is used by over 5,000 schools and 3 million students across the globe. It's a unique response to the challenge of today's connected learning environments, supporting the integration of technology, education and engagement to create cyber safe communities where students thrive.

For more information, visit **linewize.io** or email **sales@linewize.io**

Linewize
BY FAMILY ZONE

Linewize by Family Zone
Level 3, 45 St Georges Terrace Perth
WA 6000
help@linewize.io