# Veriato

# How Firewalls Can Leave Your Institution Vulnerable

Utilizing a firewall to protect your network from insider threats can lead to a false sense of protection

**By Stephen Voorhees**

Firewalls are typically used to prevent hackers, or malicious actors from accessing your internal network. In addition, they are also utilized to filter Internet access to unapproved websites from within the internal network; however, that is not always the case when the machine is taken off the network. While they are able to see network traffic traversing the perimeter via firewall logs, and are likely to block website access, a perimeter firewall is unable to see the context of activities or any activity that is occurring solely within the network, leaving your educational institution vulnerable.

For example, firewalls are not able to record documents being transferred to USB drives or cloud storage. Firewalls also cannot monitor keystrokes to detect potentially harmful keywords that could be associated with cyber bullying, drugs, violence, inappropriate conduct, and other questionable content.

Veriato 360 can record all of these activities, and more, while providing screen snapshots, much like a CCTV camera, allowing you to see everything that was displayed on the end user's monitor(s).

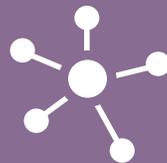## Possible examples of how firewalls can fall short on protection:

Firewalls cannot detect anomalies in email, or file transfer activities

Firewalls cannot protect against compromised credentials that could be used to log into a teacher's machine

Firewalls assume that only outsiders are a threat, and everyone inside is 100% secure and trusted

Firewalls cannot stop students from VPNing into other devices off the network, thus bypassing your blocking rules

Firewalls cannot stop
all proxy connections

Firewalls will not stop potential
internal attacks/mischief
to servers or computers

Firewalls cannot log possible
inappropriate content being
placed onto computers or taken
home on a removable drive

## Conclusion

Firewalls therefore do not provide sufficient protection for a multitude of vulnerabilities within your network. User Activity monitoring fills these gaps by continuously monitoring users for signs of risk.

To learn more, visit http://www.veriato.com/products/veriato-360

**Veriato**
www.veriato.com

**Veriato USA**
4440 PGA Boulevard, Suite 500
Palm Beach Gardens, FL 33410

**Veriato EMEA**
3rd Floor, Steward House
14 Commercial Way
Woking, Surrey
GU21 6ET, United Kingdom

https://plus.google.com/+Spectorsoft
https://www.linkedin.com/company/veriato
https://twitter.com/Veriato
https://www.youtube.com/SpectorSoft
https://www.facebook.com/VeriatoInc/