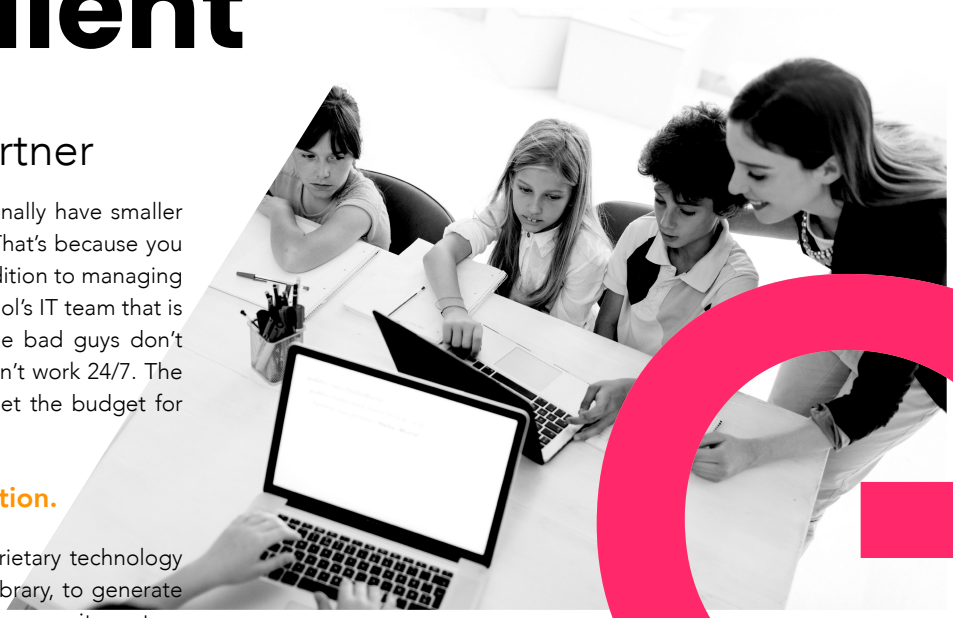
Gradient

your trusted —
— cybersecurity partner

When it comes to cybersecurity, schools traditionally have smaller IT teams that have the toughest job out there. That's because you have to take care of everything IT related - in addition to managing security. All too often there is no one on the school's IT team that is dedicated to security – and even if there is, the bad guys don't keep bankers' hours and your security person can't work 24/7. The choice seems to be - go it alone - or try and get the budget for more cybersecurity tools. Not anymore!



Gradient Cyber gives you a better option.

Gradient is a powerful combination of our proprietary technology and security experts that utilize our Cognitive Library, to generate AI driven cyber security assessments. As your cybersecurity partner Gradient's make the job of managing security much easier for school's smaller IT teams; without breaking the bank.

DOES YOUR CURRENT CYBERSECURITY PARTNER DO THIS FOR YOU?

GRADIENT'S TOTAL SOLUTION POWERED BY OUR PROPRIETARY TECHNOLOGY AND SENIOR CYBERSECURITY ANALYSTS.

Gradient's cybersecurity analysts extend and support your cybersecurity team by monitoring and analyzing traffic on networks, servers, endpoints, databases, applications, websites, and other systems, **looking for anomalous traffic that could be indicative of a cybersecurity incident or compromise.** Our Cybersecurity Analysts become trusted members of your cybersecurity team. Gradient's total solution of technology and dedicated cybersecurity analysts are able to reduce the false positives that cause alert fatigue. Allowing you to ***focus on real threats.***

Gradient's Security Intelligence Platform provide insights into your school's cybersecurity maturity and improvement with our native out-of-the box compliance features that are built on industry leading **cybersecurity frameworks - NIST, CMMC, CAT, & IMO.**

How Do We Do It?

01 NETWORK MONITORING

Gradient's AI driven Security Intelligence Platform allows us to fully monitor and protect your network.

- Bi-directional Netflow instead of uni-directional Netflow providing a full end-to-end session communication. This ingestion is done directly using PCAP data and Gradient's Quorum Collect appliance.
- Detailed Examination of IP addresses for potential threats.
- Localized port scanning against different port ranges to discover and pinpoint firewall misconfiguration.

02 LOG INGESTION

The amount of risks to networks continues to increase and Gradient's Security Intelligence Platform offers complex logging from on-site and/or cloud providers. These logs are mapped back to Netflow data to create a clearer view of the network's operation and detect suspicious circumstances.

- We ingest Active Directory Logs and Microsoft 365, along with Endpoint logs and other security-related data.
- We support firewall types that include Cisco ASA/Firepower, Watchguard, Sonicwall, Fortinet, Ubiquiti, Palo Alto, and Sophos.
- We also support AWS VPC/EC2 Flow log ingestion.

03 ENDPOINT INTEGRATION

The Gradient Platform integrates with several endpoint protection solutions to ingest logs and alerts for a holistic picture of the environment.

- LDAP logs are monitored for anomalous activity, authentication failures, and policy changes.
- Endpoint Protection events are monitored and mapped to network data to provide a clearer picture of endpoint communication.
- Endpoint inventory is enriched with network traffic data.

04 NETWORK DATA ANOMALY DETECTION

The Gradient platform provides actionable insights and algorithms that identify unexpected events, observations, or items that differ significantly from the norm.

- Artificial intelligence (AI) is used to detect anomalies and risks based on the network's history of behavior by utilizing machine learning techniques.

05 ASSET COMMUNICATION DISCOVERY

The Gradient platform provides detailed information on assets based on asset Netflow data. We see Industry standard signature-based detections and custom signature-based detections on recent activity in cyber trends as it relates to threats.

- Hashes used to compare files being transferred over the network against known bad file signatures.
- We monitor http, DHCP, SMTP and SSH traffic.

06 THREAT MANAGEMENT

The Gradient platform provides Threat Intelligence via our Cognitive Library - which is a combination of our own proprietary technology and industry-leading security and threat feeds.

- Tied into all of the major cyber analysts' threat feeds to ensure we identify malicious network traffic.
- Our platform provides detailed information on IP addresses and URLs, which allows a user to verify IPs that may be malicious.

07 INTRUSION DETECTION SYSTEM (IDS)

Gradient Security Intelligence platform has a built-in Cloud Based Intrusion Detection System to monitor the network traffic for malicious activity and policy violations.

- Gradient's IDS monitors network traffic for suspicious activity and creates an alert when such activity is discovered.
- We have a dedicated team to manage signature-based threats.
- We utilize a Cloud Based, Out-of-Band deployment ensuring that our IDS solution does not affect network performance at all.
- By utilizing cyber threat feeds from many top sources and because we are Cloud Based our "time-to-signature" for new malware variants is extremely fast.

Gradient Cyber