



Protecting K-12 from Cyberattacks

Prevent Data Breaches with Active Breach Protection

Summary

Only Comodo can claim 100% effectiveness in preventing ransomware and zero-day exploits from causing harm. The Comodo Dragon platform provides a security environment that verdicts 100 percent of unknown files. The platform renders an almost immediate verdict on the status of any unknown files, so it can be handled accordingly by software or human analysts.

This shift from reactive to proactive is what makes Comodo's Unified Endpoint Security solution unique and gives you the capacity to protect your educational institution—from network to the web to cloud—with confidence and efficacy.

Tel: +1 (888) 551-1531
Tel: +1 (973) 859-4000


Learn more online
www.comodo.com

200 Broadacres Dr,
Bloomfield, NJ 07003

Since 2019, the cybersecurity landscape of the K-12 sector has undergone a dramatic transformation.

The pandemic forced an overnight move to remote, and then hybrid, classrooms that put a spotlight on the importance of every school and school district implementing a sound cybersecurity strategy. But, because of the lack of available resources that could be devoted to the issue, compounded by a lack of the cybersecurity technologies and staff trained to use them if they happened to be in place, schools suddenly became significantly vulnerable to cyber- and ransomware attacks.

This data-driven eBook is designed to enable school district leaders, superintendents, IT professionals, and security and operations administrators with the necessary information and resources to examine risks. We will provide an overview of the cybersecurity threats to K-12, how the challenges facing under-resourced school districts have increased dramatically since the pandemic, and how you can cost-effectively protect your school and community at large from malware and ransomware attacks.



No one can stop
zero-day malware
from entering your
network, but Comodo
can prevent it from
causing any damage.

Zero infection.
Zero damage.

K-12 organizations are a prime target for malicious actors.

Between 2019-2020 ransomware attacks against educational institutions increased 100%. The average ransom paid by US institutions in 2020 was \$112,435 — and of those who paid only recovered 68% of their data.

The stats are sobering, but unfortunately the trend has only gotten worse. From August 14 to September 12, 2021, educational organizations were the target of nearly 6 million malware attacks — comprising 63% of all malware attacks during that time frame.¹

Devices, such as laptops, loaned to students and staff during the pandemic are returning to schools, and their networks, full of threats due to a lack of security updates. In 2020 alone, 1,268 Microsoft vulnerabilities were discovered — a 48% increase from 2019. These unsecured devices reconnecting to school networks is a recipe for malware attacks.

The message is clear: current cybersecurity strategies aren't working. K-12 organizations are spending more than ever before on solutions that aren't offering true protection. Additionally, security operations centers are becoming more complex to manage with higher overhead expenses.

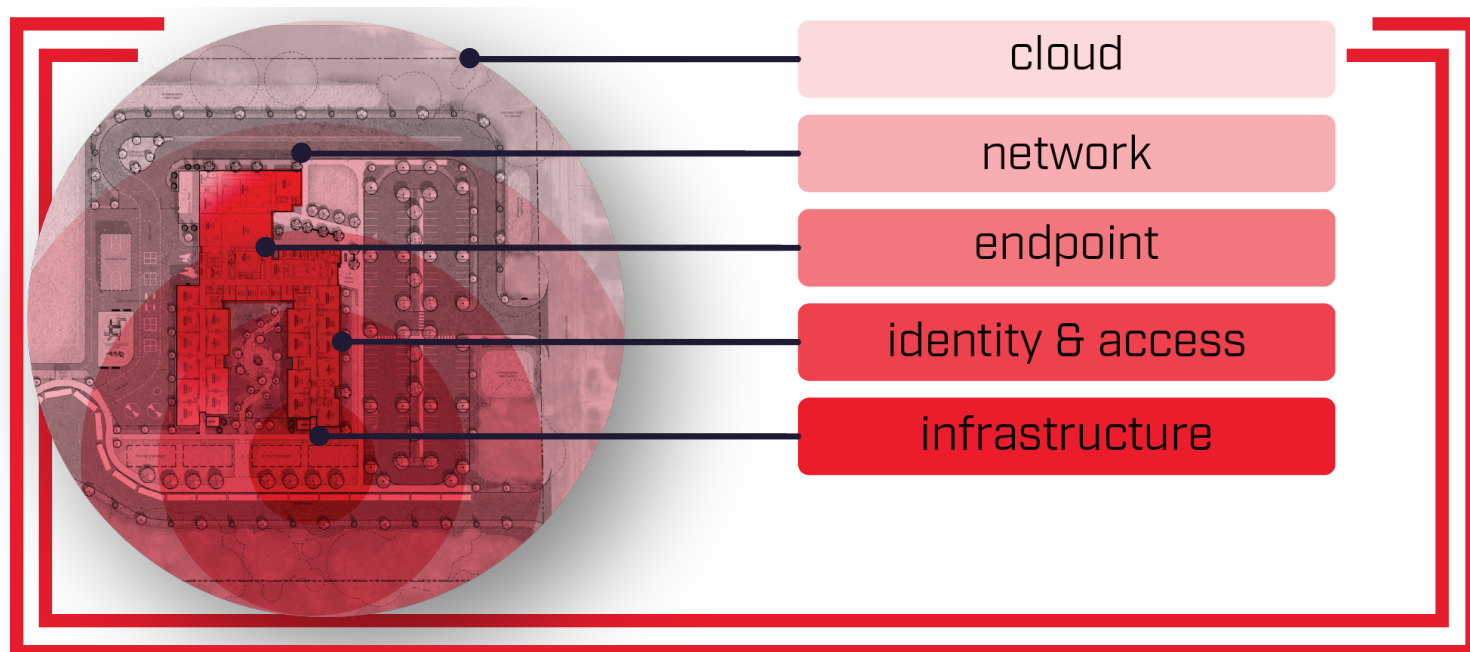
A few common-sense factors can be attributed to this rise:

- ◆ Schools are being forced to rapidly move online, which means deploying new technology devices to support teachers, staff and students.
- ◆ Adopting new platforms of all types without time to plan, prepare and implement necessary safeguards.
- ◆ Permitting staff to use third-party vendors without going through the normal vetting process.
- ◆ IT staff granting users elevated access to devices and/or remote access to tools that were not serviced by IT personnel due to COVID-19 physical restraints.
- ◆ Finally, thousands of devices eventually reconnecting to school networks, without the resources necessary to properly examine and continually monitor for potential risks.²



The New Reality of K-12 Demands a New Approach to Cybersecurity

- ◆ Each school district is unique, but generally K-12 IT directors must overcome a few general issues when strategizing around cybersecurity.
- ◆ Schools of every size lack expertise and resources to defend against malware attacks.
- ◆ Ransomware attacks prevent schools from functioning as intended. When systems are shut down, everything is compromised. Even the seemingly small things become mountains to climb, such as:
 - How will cafeterias function without card readers?
 - How will teachers gain access to lesson plans?
 - How will students attend virtual classrooms?
- ◆ Lack of resources to manage endpoints effectively, allowing the attack surface to remain available for attackers to exploit.
- ◆ Schools store personal information for students and teachers, and connect with a large number of external bodies and providers and, of course, parents, who primarily communicate with the school via email. This necessitates the need to manage personally identifiable information (PII) and the necessary precautions to avoid a data vulnerability incident.
- ◆ Private and public schools alike often store the financial and personal data of donors, board members, and other high-profile individuals, making the school a prime target for ransomware attacks.

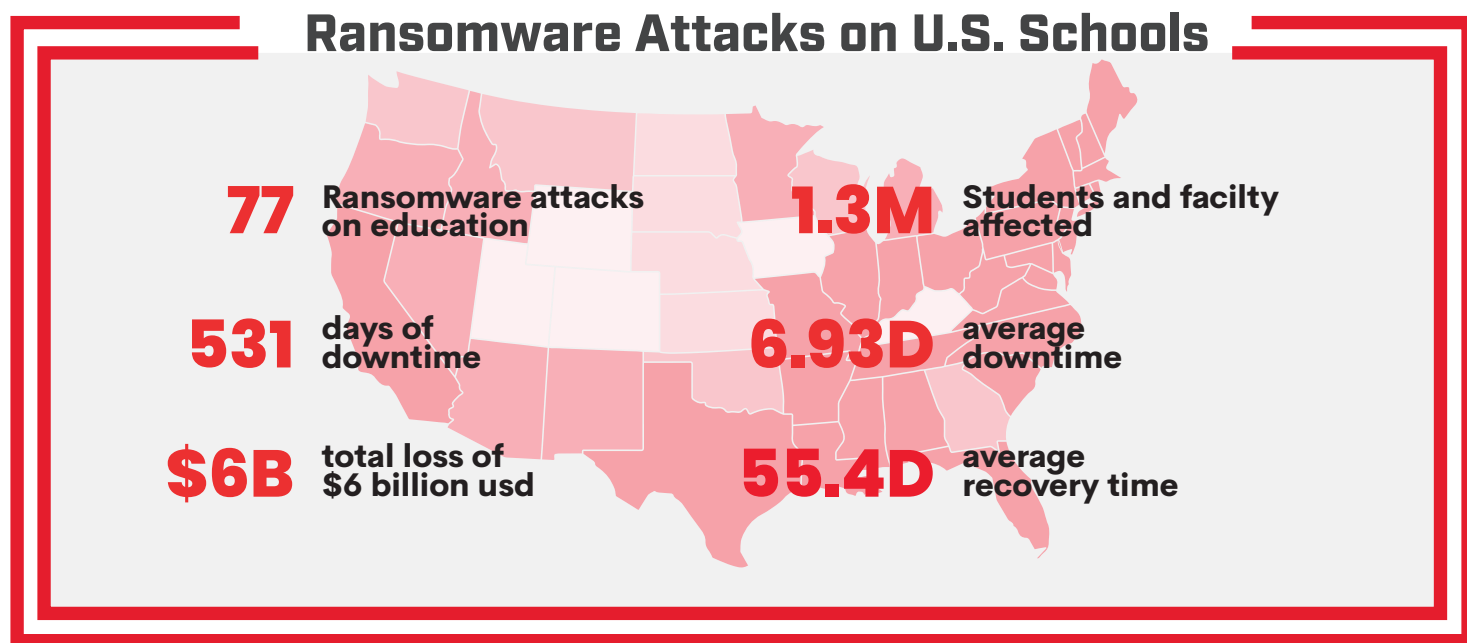


K-12 Attack Surface Introduces Exponential Risks

Schools have a very large attack surface with many different parts of the community-at-large unknowingly at risk, including city and state departments.

In our connected world, a single compromised school can lead to a school district then 25 school districts in one city. All leading to a potential gateway to the larger city and state targets.

The threats are real. There were 77 ransomware attacks on schools and colleges in the U.S. during 2020. These attacks resulted in 531 days of downtime, resulting in over \$6 billion of loss³. Yet, the expectations for under-resourced schools are enormous.



Like the enterprise, K-12 schools must adapt to new, more flexible models of delivering instruction safely — even when schools are able to return to “normal” operation.

Comodo's Advanced Endpoint Protection (AEP) platform delivers a cost-effective, robust unified cybersecurity approach that reduces the attack surface and stops 100% of known and unknown malware and ransomware attacks.

Reducing the Attack Surface with a Unified Cybersecurity Approach

Risk Mitigation & Risk Management

Now that schools are operating in a hybrid world, the potential attack surface just got exponentially larger. Many think-pieces out there will recommend that schools and organizations take a "Zero Trust" approach to your cybersecurity strategy. That is sound advice, but it doesn't solve the entirety of the problems facing K-12 orgs.

Essentially, the root problem that Zero Trust solves is to restrict access and segment your network to avoid the spread of an attack and, crucially, to make it extremely difficult for attackers to move laterally and propagate once inside your system. The more difficult it is, the less time and attention will be expended within the environment, driving most attackers to seek out another victim. Zero Trust has become a popular term to throw around in reference to all things cybersecurity, but it's toothless.

Rather than deal with the malware or ransomware once it's inside your environment, Comodo is there to prevent the breach from ever happening. Our proprietary technology stops the execution of malicious software — keeping it at the front door, where it can't do any damage, instead of letting it in the house.

To learn more about Zero Trust, we recommend reading our blog post [What is Zero Trust Security?](https://enterprise.comodo.com/blog/what-is-zero-trust/)

[Learn more](#)<https://enterprise.comodo.com/blog/what-is-zero-trust/>

Never trust, always verify.

The central guiding principle in the Unified Cybersecurity model of information security is "never trust, always verify." It seeks to mitigate and manage risk by eliminating internal "trusted" zones within networks and instead make security omnipresent throughout the entire ecosystem. All network traffic is untrusted, and all data must be continuously inspected.

The Unified Cybersecurity method is a holistic approach that emphasizes the importance of protecting critical K-12 institutional data, as well as student and teacher privacy, from data breaches, while defending against malware and ransomware attacks, meeting invasion and denial of service attacks.

Zero Trust puts a premium on visibility and ongoing monitoring over perimeter-based defenses and strategic goals over particular tools and technologies.

The Unified Cybersecurity approach is rooted in three core concepts.



CONCEPT NO.1

NEVER TRUST, ALWAYS VERIFY

Eliminate the concept of trust from your network's design. You must assume all traffic and executables, known or unknown, are a potential threat until proven otherwise. All data should be inspected, verified and secured, no matter where it resides. Data that sits in an on-premise data center is to be treated the same way as data hosted in the public cloud. No traffic is to be allowed by default.

We have solved the malware problem with our patented isolation technology. Only Comodo's AEP technology can prevent malware from doing harm at runtime while our unified endpoint security delivers the greatest solution at the most affordable price.



CONCEPT NO.2

PROTECT STUDENT, TEACHER AND SCHOOL DATA

A unified security strategy begins with a focus on the data. Schools need to understand where data is stored, how it is used, why it is sensitive and what might put it at risk. Schools must implement granular access control policies to protect it and prevent unwanted access to and sharing of sensitive data and resources. The consequences of a data breach involving student and teacher data can be dire and long-lasting. For example, in 2021 there was a massive breach in the Broward County School District that exposed sensitive data of over 50,000 students and staff — including phone numbers, social security numbers, addresses, private health records, and dates of birth.⁴ The results of a data breach of this sort can result in online harassment of both students and teachers, as well as identity fraud, financial fraud, and can affect college admission opportunities in the future for students.⁵



CONCEPT NO.3

CONTINUOUSLY MONITOR YOUR INFRASTRUCTURE AND NETWORK TRAFFIC

Ongoing monitoring of all network traffic enables your security team to spot anomalous user behavior or suspicious activities quickly. This is the key to keeping incursions from becoming breaches. Maintaining logs of all internal and external traffic will also improve visibility into your environment. Of course, because of the sudden move to online and hybrid schools, the traffic and amount of endpoints that must be monitored has grown exponentially. A large school district, for instance, had more than 91,000 devices assigned to staff and students post-March 2020. 91,000 devices that will, eventually, reconnect to the schools' network.⁶

Reducing the Attack Surface with a Unified Cybersecurity Approach

Cyber Hygiene

These three principles call for organizations to adopt a data-centric approach to securing their environments and endpoints. Rather than assuming that some users—or certain types of traffic—can be deemed “trustworthy,” reducing the attack surface through a unified security strategy demands that every file be treated as potential malware, and every user as a possible threat agent.

Additionally, having an efficient endpoint monitoring tool can bring a lot of benefits to your school. These benefits include improving your cyber hygiene by identifying and remediating patch levels and vulnerabilities. This will give your security team complete control to mitigate risks to the attack surface.

Only after users have proven themselves trustworthy should they—or the data packets they generate— be given access to the network.

5 STEP PLAN

Start Integrating a Unified Cybersecurity Approach

To make it easier, we’ve outlined a NEVER TRUST, ALWAYS VERIFY five-step plan to help you incorporate a unified cybersecurity approach to your organization's security infrastructure plan and reduce the attack surface.



STEP 1: Incident Response Plan



STEP 2: Map the data and transaction flows within your school’s network



STEP 3: Isolation and Analysis



STEP 4: Endpoint Detection and Response



STEP 5: Continuously monitor your ecosystem



STEP 1

Incident Response Plan

Every organization should know what they are going to do in case of a ransomware or malware attack. At a high-level, schools need to have a list of the individuals, their responsibilities, and the key actions they need to execute in the event of a cyberattack. The various components of an incident response plan should include detection and initial analysis of an attack, identifying the impact, and determining if the attack has concluded or if it is still ongoing.

Schools will need to contain the situation and identify the root cause, eliminate the malware, and remediate any vulnerabilities across their network. Once the data breach has been resolved, schools will want to develop a post-incident plan to review processes, technologies, and tools to mitigate the risk of another incident.

STEP 2

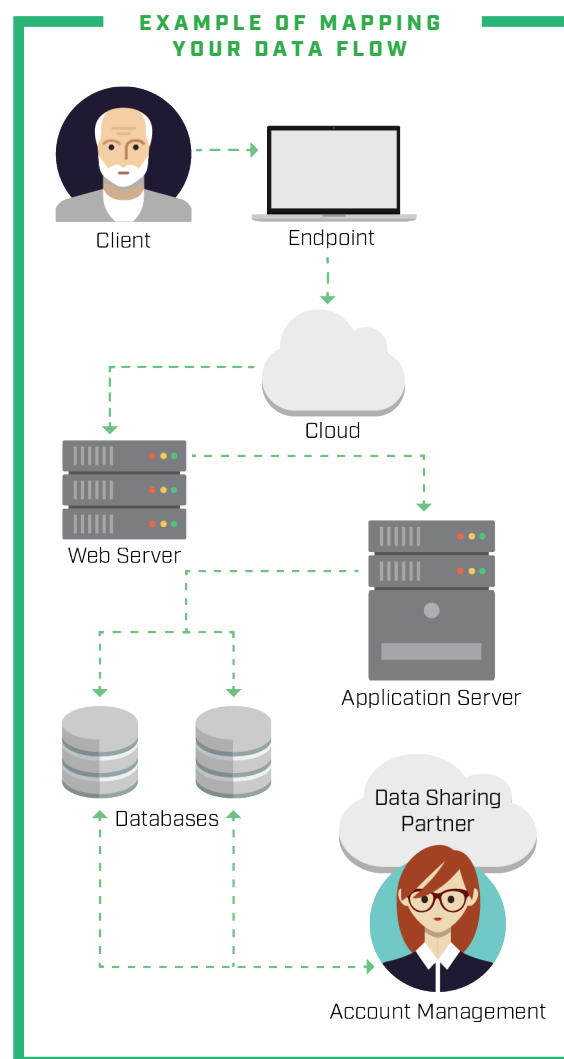
Map the data and transaction flows within your school's network

Because your data's security and integrity are central to the unified cybersecurity paradigm, a thorough understanding of where your data resides and how it flows between users, devices, systems and other resources in your IT environment is essential. You'll need to engage stakeholders across the organization in this process since it usually involves network architecture, third-party services and questions about user needs and value to the organization.

In fact, in each of the last two years (2019 & 2020) 75% of all data breaches that affected public K-12 schools in the U.S. resulted from security incidents involving vendors and other partners.⁷

It is wise to create a comprehensive inventory of your data assets that identifies where data is stored, how it is collected or created, who uses it, and how it travels. You can create visual representations of these processes or flows, called data flow diagrams, at varying levels of abstraction.

If your organization must adhere to compliance requirements such as the Payment Card Industry Data Security Standard (PCI-DSS) or the EU's General Data Protection Regulation (GDPR), you probably already have existing data flow diagrams you created to meet these requirements.



STEP 3

Isolation and Analysis

In order to safely detect questionable software, the executable software needs to be isolated in a safe space for execution, otherwise the point of detection might occur well beyond when it can be blocked. Our proprietary Advanced Endpoint Protection (AEP) technology uses kernel level API virtualization where executables can be launched without fear of infecting the host machine.

This virtualized environment allows executables to go through a test run of a full installation and execution. When the application is launched, it has full access to all of the registry and systems files that would be expected. These files are then monitored to see what steps the application is taking without any interference. This allows the endpoint protection to observe what is occurring and with AI & ML make determinations as to whether the actions are safe or not. Crucially, business as usual can continue for all users on the network while our isolation technology goes to work on the software in question.

STEP 4

Endpoint Detection and Response

Implement continuous monitoring mechanisms that allow you to know what happened and what is happening. Comodo's Endpoint Detection and Response (EDR) gives our customers the tools of continuous vigilance and provides IT teams with the story of how the malware arrived, what was its intent, and what is currently happening. Preventing malware from causing damage is one thing, but IT teams must also improve cyber hygiene while accounting for scenarios where the compromise isn't associated with malware. For instance, a malicious user who utilizes legitimate applications to gain access to another system and steal data. If someone were to utilize a script engine to invoke a connection over a non-standard port/protocol, or even something that may seem benign, like installing a bitcoin miner on a server.

It is important to note that most endpoint protection solutions rely on detection as a precursor to prevention. Malware that goes undetected will be allowed to execute and write to the hard drive. This presents a problem with the approach of all modern day endpoint solutions. False positives and false negatives remain an issue because of limitations in detection efficacy. Modern solutions reliant upon detection will continue allowing unknown files to execute, which creates avenues for a Kaseya style attack to take place as it utilized a trusted application. For example, during investigation of a data breach resulting from a malicious insider (no malware), EDR can be used to detect the point of initial compromise at an early stage; to trace the attacker across many touched endpoints in an IT environment; and to identify what data is being stolen and through what means (USB write, email attachment, etc.).

The benefits of an effective EDR strategy are clear.

- ◆ Continuous real-time visibility of your endpoints with detection & response.
- ◆ IT teams can identify attacks with the accurate root-cause analysis for effective remediation intelligence.
- ◆ Detect threats faster and better.
- ◆ Achieve deeper endpoint activity visibility.
- ◆ Alleviate response fatigue of your under-staffed IT teams.

STEP 5

Continuously monitor your ecosystem

The attack surface for K-12 organizations has grown exponentially in this post-pandemic reality. And with it, the need for robust and vigilant monitoring. The threats are increasing and the expectations for cyber safety are far greater than they've ever been.

You may now be asking yourself, "How does an underfunded, under-resourced, under-staffed IT department protect their schools data and network, while also being asked to continuously monitor the health of our systems?" We don't think you should have to, which is why we offer Managed Detection and Response (MDR) — advanced 24x7 cybersecurity service that extends threat monitoring and threat hunting from endpoints to the network and cloud. Our MDR security experts service your organization remotely from the Comodo SOC across the globe, allowing you to focus on the critical day-to-day tasks of running a school.

Comodo's MDR service delivers a cost-effective solution to expand your IT security staff, because we don't believe improving your cybersecurity posture should break the school's budget. As part of our MDR service, our security experts proactively search for vulnerabilities, continuously monitor your IT systems for indications of compromise, and provide in depth reports. We work closely with your IT team to prioritize and fix security flaws and remediate issues.

A few benefits of Comodo's MDR service:

- ◆ Protection against zero-day web threats, without hindering students' learning experience or impacting employee productivity.
- ◆ Detection of 100% of unknown fileless threats with Comodo's intelligent file analysis engine.
- ◆ All components work in tandem to deliver you the reports and remediation needed to handle every incident quickly.



Protecting school IT environments from ever-evolving cyber threats has never posed more of a challenge than it does today.

As cybersecurity costs continue to increase, malicious activity shows no signs of slowing down. Cybercriminal operations are more carefully targeted and better funded than ever. Nationwide state-level adversaries remain active, and even relatively unsophisticated hackers have successfully compromised enterprise networks.

In this environment, a Unified Cybersecurity Architecture offers the opportunity to tilt the odds in favor of the defenders. Not every organization has the resources to conduct ongoing monitoring or threat-hunting in house.

The Comodo Dragon Platform is a scalable solution that can support school districts of all sizes thanks to our cutting-edge patented isolation technology, unparalleled network security, and 24/7 Managed Detection and Response service.



Comodo's unique isolation technology prevents breaches by containing and analyzing 100 percent of unknown files that come in contact with a network in a virtualized environment. As an unknown file executes on an endpoint, the file is instantly contained and analyzed, while users experience no interruption in the system's performance.

While the unknown file is in isolation, it is analyzed statically and dynamically in the cloud. 95% of the time, a "trusted" verdict is returned in under 45 seconds. 5% of the time, human experts further analyze unknown files to provide "trusted safe" or "malicious" verdicts.

Comodo's isolation technology never trusts unknown files and always verifies they are safe before releasing them from the container.

Ransomware Protection for K-12

Only Comodo can claim 100%

effectiveness in preventing ransomware and zero-day exploits from causing harm. The Comodo Dragon platform provides a security environment that verdicts 100 percent of unknown files. The platform renders an almost immediate verdict on the status of any unknown files, so it can be handled accordingly by software or human analysts.

This shift from reactive to proactive is what makes Comodo's Unified Endpoint Security solution unique and gives you the capacity to protect your educational institution—from network to the web to cloud—with confidence and efficacy.

About Us

Comodo has experts and analysts in 185 countries, - Based in Bloomfield N.J., Comodo has a 20-year history of protecting the most sensitive data for businesses and consumers worldwide.



Comodo is the world's leader of next-generation open-source cybersecurity, with the industry's most disruptive innovations. We help customers stop breaches with groundbreaking isolation technology that neutralizes ransomware, malware and cyber-attacks. Our complete cloud-native framework delivers a zero-trust architecture with active breach protection for the most comprehensive defense against zero-day threats. Comodo's cybersecurity products maximize intelligent sharing between every component of the platform, therefore providing superior security. We are the only company that analyzes and gives a trusted verdict for 100% of files on a network.

Comodo leverages innovation to celebrate and support the cybersecurity community by offering the very first open-source endpoint detection and response (EDR). We believe an open-source model using community-powered collaboration will ensure every organization has access to the industry's most sophisticated EDR.

Let's Discuss the Next Steps

Contact

Tel: +1 (888) 551-1531

Tel: +1 (973) 859-4000

Online

Preview the product

www.comodo.com/demo

Email

sales@comodo.com

support@comodo.com

ENDNOTES

- ¹ <https://www.google.com/url?q=https://gcn.com/articles/2021/09/15/k12-college-cyberattacks.aspx>
- ² <https://www.google.com/url?q=https://k12cybersec-cure.com/wp-content/uploads/2021/03/StateofK12Cybersecurity-2020.pdf&sa=D&source=docs&ust=1637954228083000&usg=AOvVaw1aGji9tIMkt-jeFfITvrKW> The K-12 Cybersecurity Resource Center, March 10, 2021), 7. eBook.
- ³ https://www.comparitech.com/blog/information-security/-school-ransomware-attacks/#How_does_2020_compare_to_previous_years
- ⁴ <https://www.google.com/url?q=https://www.govtech.com/education/k-12/broward-schools-warn-50k-employees-students-of-d&sa=D&source=docs&ust=1638896487390000&usg=AOvVaw0XAiZk4HHzMpCZPxhMz0de>
- ⁵ https://www.google.com/url?q=https://www.securityin-fowatch.com/education/article/21243610/cybersecurity-threats-challenge-k12-schools-resilience-and-preparedness&sa=D&source=docs&ust=1637954228072000&usg=AOvVaw0ZkaUiU68jr-2BBnldwsO_
- ⁶ https://www.google.com/url?q=https://www.securityin-fowatch.com/education/article/21243610/cybersecurity-threats-challenge-k12-schools-resilience-and-preparedness&sa=D&source=docs&ust=1637954228072000&usg=AOvVaw0ZkaUiU68jr-2BBnldwsO_
- ⁷ <https://www.google.com/url?q=https://k12cybersec-cure.com/wp-content/uploads/2021/03/StateofK12Cybersecurity-2020.pdf&sa=D&source=docs&ust=1637954228>