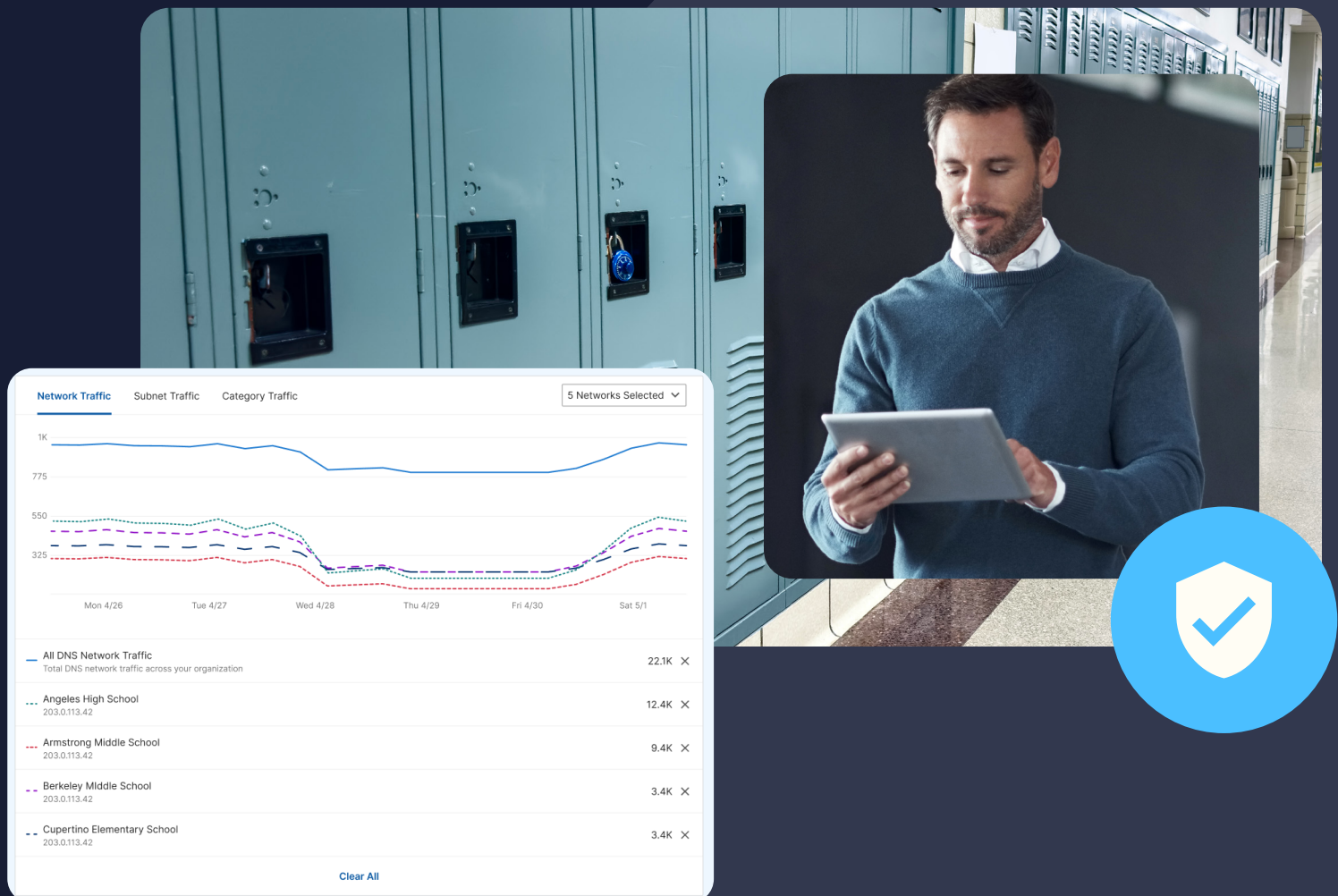




Navigating Web Filtering *Deployment Strategies* for K-12



Navigating Web Filtering Deployment Strategies for K-12

Introduction

How Web Filter Deployment is Changing

- The Rise of Cloud Filtering
 - Benefits of Cloud Filtering
- The Enduring Value of On-Prem Filtering
 - Benefits of On-Prem Filtering
- The Power of Hybrid Solutions
 - Benefits of Hybrid Deployment

Meeting Statutory Requirements & Guidelines

- CIPA Compliance
 - Key CIPA Requirements
- Coppa and Student Data Privacy
 - Key Coppa Considerations for Schools
- Key Compliance Features Checklist

Choosing the Right Deployment Strategy for Your School

- Assessing Your Current Needs and Infrastructure
- Common Web Filtering Deployment Options
 - On-Prem
 - Hybrid
 - Cloud

How to Choose a Web Filtering Vendor

- Essential Vendor Capabilities Checklist

Conclusion

Frequently Asked Questions

About Goguardian Admin

- Why Choose Goguardian: Our Comprehensive Solution
- Understanding Goguardian DNS Precision Filtering: Key Features
- Network Filtering with Cloud Policies
- Internal IP Address Reporting
- Agent Awareness for Optimized Filtering
- DNS Fallback for Uninterrupted Protection
- Unparalleled DNS Traffic Reporting

The current state of web filtering

Creating a safe and secure online environment for schools is more important — and challenging — than ever before. IT administrators know better than anyone how incredible yet dangerous the internet can be for young learners. They have the vital job of ensuring students can access everything they need to excel with technology in the classroom while also defending them against inappropriate content and cyber threats. Add meeting state and federal safety mandates to that, and the responsibility just keeps growing.

We speak with dedicated IT professionals daily; it's the only way to truly understand the needs of those looking for a comprehensive guide to equip IT leaders, network administrators, and district decision-makers with the knowledge they require to navigate numerous web filtering deployment strategies, from cloud to on-prem and hybrid. This guide offers a comprehensive understanding of each model and its benefits, enabling you to make an informed decision that optimizes your resources, enhances student safety, and ensures seamless network performance within your specific environment.



Deployment is *changing*

Web filtering in education has seen significant shifts in just the last few years, driven by technological advancements, changing learning modalities, and the sheer number of devices on campus. On-prem solutions made sense when they were one of the only options. Now, web filter deployment has evolved into an entire ecosystem that includes cloud-based and hybrid approaches. Understanding what has changed is key to choosing the most effective strategy for your district.

The *rise* of cloud filtering

Cloud-based web filtering solutions are flexible, scalable, and easier to manage. In a cloud model, filtering logic and policy enforcement reside in the vendor's data centers, with traffic usually routed through cloud proxies or managed via lightweight agents on devices.

Benefits of cloud filtering include:

Scalability: Easily accommodates fluctuating student and device counts without requiring hardware upgrades.

Off-site protection: Extends filtering policies to devices used outside the school network (e.g., 1:1 programs, remote learning).

Reduced capital expenditure (CapEx): Shifts costs from large upfront hardware purchases to more predictable operational expenses (OpEx).

Lower IT maintenance: Reduces the burden on IT staff by offloading hardware maintenance, software updates, and infrastructure management to the vendor.

Faster deployment: Eliminates the need for complex on-site hardware installation, allowing for quicker setup and policy enforcement.

Always up-to-date: Cloud solutions are continuously updated by the vendor, ensuring access to the latest filtering intelligence and features without manual intervention.

Distributed traffic processing: Avoids network bottlenecks at the gateway by distributing filtering across devices or cloud infrastructure.

Enhanced security & data backup: Cloud providers typically offer robust physical and digital security measures, including data encryption and redundant backups.

Why on-prem filtering *still* matters

Despite the popularity of cloud solutions, on-premises (on-prem) web filtering still holds significant value for many school districts. In this model, filtering appliances and software are installed directly within the school's physical network infrastructure.

Benefits of cloud filtering include:

Granular control & customization: Provides IT teams with maximum control over filtering rules, network traffic, and integration with existing on-site systems.

Data security & sovereignty: For districts with strict data residency or security policies, keeping data within their physical control can offer peace of mind.

Leveraging existing infrastructure: Ideal for districts that have made significant investments in on-prem hardware and have the internal expertise to manage it.

Optimized for BYOD & unmanaged devices: Can offer highly effective filtering for devices connecting directly to the school network, including personal devices (BYOD) and those without agents.

Consolidation of services: On-prem appliances can sometimes serve multiple functions, such as firewall capabilities, potentially reducing hardware footprint.

Assured filtering: In some configurations, an inline on-prem filter can make it more challenging for devices to bypass filtering, providing a strong layer of defense.

Budgetary flexibility: For districts with dedicated capital budgets, a one-time hardware purchase might align better with financial planning.



Schools are *switching* to hybrid solutions

Recognizing no single solution fits all, many districts are adopting a hybrid approach, combining elements of both on-prem and cloud filtering. This strategy aims to leverage the strengths of each model, creating a flexible and resilient filtering infrastructure.

Benefits of hybrid deployment include:

- + Optimized load distribution:**
Balances traffic processing between on-prem hardware and cloud services, preventing bottlenecks and enhancing performance, especially as internet usage grows.
- + Seamless on/off-site protection:**
Extends comprehensive filtering to all devices, whether they are on the school network (managed by on-prem) or off-site (managed by cloud agents).
- + Flexible authentication:**
Can simplify user authentication for modern devices like Chromebooks via cloud integration, while maintaining robust authentication for on-prem devices.
- + Gradual migration path:**
Allows districts to transition to cloud-based solutions at their own pace, protecting existing investments while incrementally adopting new capabilities.
- + Tailored to diverse device environments:**
Ideal for environments with a mix of managed devices (laptops, Chromebooks) and unmanaged BYOD, ensuring appropriate filtering for all.
- + Redundancy and resilience:**
Combining deployment methods can create a more robust system, with one acting as a fallback for the other in certain scenarios.

Meeting statutory requirements & guidelines

Web filtering in schools isn't just optional, it's legally required. Districts must navigate a complex web of federal and state regulations designed to protect children online and ensure responsible technology use.

CIPA compliance

The Children's Internet Protection Act (CIPA) mandates that schools and libraries receiving E-rate discounts must have an Internet safety policy and use technology to block or filter Internet access to obscene or harmful material.



Key CIPA requirements include:

Blocking/filtering harmful content: Technology must be in place to prevent access to inappropriate or harmful content.

Online safety policies: Districts must have policies addressing online safety, including overseeing students' online activities.

Digital citizenship education: Programs must be in place to educate learners about appropriate online behavior, cyberbullying awareness, and social media interaction.

COPPA and student data privacy

The Children's Online Privacy Protection Act (COPPA) governs the online collection of personal information from children under 13. While primarily aimed at commercial websites, it impacts schools when they use third-party online services.



Key COPPA considerations for schools include:

Caregiver consent: Schools often act as agents for guardians in providing consent for educational technology services.

Privacy policies: Clear and comprehensive privacy policies must be in place.

Data security: Information collected from students must be kept confidential and secure.

Key compliance features checklist

When evaluating any web filtering solution, administrators should ensure it addresses the following critical aspects for compliance and effective student safety:

-  **Real-time content analysis:** Goes beyond simple URL blacklists to analyze page content dynamically, preventing access to harmful material even on legitimate sites.
-  **Granular categorization:** Provides detailed categories and subcategories to allow for precise policy enforcement, minimizing over-blocking while ensuring safety.
-  **On/off-site protection:** Ensures consistent filtering policies apply to all school-issued devices, regardless of location, and differentiated filtering for when students are at home.
-  **Comprehensive incident reporting:** Captures 100% of relevant browsing data to build a complete contextual picture for investigations and compliance audits.
-  **Robust user authentication & identification:** Accurately identifies users across various devices and networks to apply personalized policies and provide detailed reporting.
-  **Social media controls:** Offers flexible options for managing social media access, including read-only modes or age-appropriate restrictions.
-  **VPN blocking:** Detects and blocks attempts to bypass filtering using proxies or VPNs.
-  **Cross-platform compatibility:** Provide consistent filtering and policy enforcement across a wide range of operating systems and devices, including Windows, Mac, ChromeOS, and mobile devices.
-  **Audit trails & reporting:** Provides detailed logs and reports for compliance verification and accountability.
-  **Data security & privacy certifications:** Adheres to industry best practices and relevant certifications for protecting sensitive student data.

What is the *right* deployment strategy for your school?

Choosing the best web filtering deployment strategy is a strategic decision that should align with your district's unique needs, existing infrastructure, budget, and long-term technology roadmap.

Assess your current needs and infrastructure

Here are some of the questions you should be asking when evaluating your deployment strategy:

- + Device landscape:** What types of devices are used (e.g., Chromebooks, Windows laptops, Macs, personal devices)? Are they primarily school-issued or personal? Are they managed by client-based agents?
- + Network architecture:** What is your current network setup? Do you have existing DNS servers or other network appliances? What is your current bandwidth capacity and future projections?
- + Off-site filtering requirements:** How critical is it to filter devices when they are outside the school network (e.g., for 1:1 programs, remote learning)?
- + IT staff resources:** Do you have dedicated IT staff with the expertise and time to manage on-prem hardware and software, or are you looking for solutions that minimize this burden?
- + Budget constraints:** Are you prioritizing capital expenditure (large upfront costs for hardware) or operational expenditure (more predictable subscription-based costs)?
- + Customization needs:** How much control and customization do you require over your filtering policies and infrastructure?
- + Compliance mandates:** What specific federal and state regulations (e.g., CIPA, COPPA) must you adhere to, and how do different deployment models impact compliance?
- + Scalability projections:** How rapidly do you anticipate your student and device population growing, and how easily can your chosen solution scale to meet future demands?

Explore your options for web filtering deployment

Based on your assessment, your district might find one of the following deployment strategies to be the most suitable.

	<u><i>On-prem</i></u>	<u><i>Hybrid</i></u>	<u><i>Cloud</i></u>
What this model means:	Involves installing filtering appliances or software directly within your school's physical network infrastructure. All web traffic is routed through these local systems for filtering and policy enforcement.	This approach blends elements of both on-prem and cloud filtering. Typically involves retaining a less powerful hardware appliance on-site. Combines the on-site appliance with the deployment of client-based agents or cloud-managed DNS for a proportion of devices, especially those that go off-site.	The entire web filtering logic, policy enforcement, and reporting reside in the vendor's cloud infrastructure. Devices are typically managed via lightweight client-based agents or by directing DNS queries to the cloud service.
Ideal for:	Districts that have heavily invested in existing on-prem infrastructure. Organizations with the internal IT staff to maintain and manage this equipment. Those who desire full responsibility over their system and data. Those who are comfortable with completing updates on their devices and do not wish to overhaul a generally reliable system.	Forward-thinking districts with a mixed device environment (e.g., on-site desktops, off-site Chromebooks, BYOD). Those who seek to optimize their filtering strategy for maximum control and comprehensive coverage. The ideal choice for those who value the deep insights of on-premise filtering alongside the scalability and ease of use of a modern cloud platform.	Districts looking to reduce on-site complexity and minimize capital expenditure. Those who seek a solution that makes costs more manageable and subscription-based. Well-suited for environments with overwhelmingly managed devices and a need for flexibility and scalability.
Benefits:	Offers maximum control and customization. Keeps data within the district's physical control. Can leverage existing hardware investments.	Allows you to protect existing investments while gaining the flexibility and extended coverage of cloud solutions. Can improve cost efficiencies and simplify management by distributing the load.	Offers rapid deployment and minimal on-site maintenance. Provides automatic updates and seamless protection for devices both on and off campus. Provides high scalability and can reduce the burden on local network processors.

How to choose the *right* filtering partner

When it comes to selecting the right web filtering vendor, there's so much more to consider than just cost. Districts should approach this decision the same way they would when forming any strong partnership. Ideally, the vendor should be deeply committed to your district's success, seeing the relationship as a long-term partnership rather than just a revenue stream. You need a comprehensive solution that not only understands the unique challenges of K-12 education but is also backed by a strong implementation and support team and committed to continuous innovation in an ever-changing digital environment.

Vendor capabilities checklist: Cover the essentials

When evaluating potential web filtering partners, you should be looking to ensure they meet these critical criteria:

Content analysis:

The solution should go beyond simple URL blocklists to analyze page content completely, preventing access to harmful material even on otherwise legitimate sites. This minimizes over-blocking and ensures subdomains are covered.

Powerful reporting:

The vendor should provide immediate, actionable insights into network traffic. There should be no delay in understanding incidents, ensuring you get the data you need, when you need it, to respond effectively.

Comprehensive on/off-site protection:

The solution should offer a truly unified approach, ensuring consistent filtering policies apply to all school-issued devices, whether they are on your school network or off-site, for seamless protection in 1:1 programs and remote learning.

Full incident reporting & context:

The solution should capture 100% of relevant browsing data, including user names, internal IP addresses, and canonical names (CNAMES), to help you build a complete contextual picture around any incident, simplifying investigations and compliance audits.

Simplified & robust authentication:

The solution should integrate seamlessly with common directory services (e.g., Google Directory, Microsoft AD) for smooth user authentication, ensuring accurate policy application and user-level reporting.

Flexible social media controls:

The vendor should provide granular controls over social media access, allowing you to tailor policies to your district's needs, including read-only modes or age-related restrictions, without blanket blocking.

Proactive VPN blocking:

The filtering intelligence should actively identify and block attempts to circumvent policies using proxy servers or VPNs in real-time, maintaining the integrity of your filtering.

Simplified configuration & management:

While powerful, the solution should be designed for ease of use. Cloud-managed policies should simplify configuration, and features like agent awareness should reduce the complexity often associated with hybrid deployments.

Multiple deployment options (cloud, on-prem, hybrid):

The vendor should recognize that every district is unique and offer a flexible suite of solutions that can be deployed entirely in the cloud, on-prem, or a hybrid model, ensuring you get a tailored solution that fits your specific infrastructure and needs.

Cross-platform compatibility:

Provide consistent filtering and policy enforcement across a wide range of operating systems and devices, including Windows, Mac, ChromeOS, and mobile devices.

Scalability for future growth:

The solution's architecture should be built to scale. Whether your student population grows or device strategy evolves, the solution should adapt effortlessly, protecting your investment for the long term.

Proven K-12 expertise & support:

The vendor should have a long-standing history and deep understanding of K-12 education, demonstrating itself as a trusted partner. Dedicated support should be available to assist you, ensuring your filtering solution operates exactly how you need it to.



Conclusion

IT administrators hold a role that is just as vital to maintaining a safe educational ecosystem as that of a teacher. As edtech continues to flood the market, IT admins carry the challenging responsibility of suggesting and selecting the web filtering strategy that will impact how students learn and how educators keep them engaged. Now, you have the right information to make informed decisions that align with your district's unique needs and compliance requirements to create safe and productive learning environments for every student, every day.

Frequently asked questions

Q: What is DNS filtering?

A: Domain Name System (DNS) filtering is a method of web filtering that blocks access to websites at the domain level. When a user attempts to access a website, their device sends a DNS query to a DNS server. If the DNS server is configured with filtering policies, it can block the request for prohibited domains, preventing the user from reaching the site. This method is effective for broad content control and protecting against malicious domains.

Q: Why is DNS filtering important for schools?

A: DNS filtering is crucial for schools to maintain a safe and productive online learning environment. It helps block access to inappropriate content, protect against malware and phishing sites, and enforce internet usage policies across all devices connected to the school network, including personal devices (BYOD) and unmanaged devices. It's also a foundational component for meeting regulatory compliance requirements like CIPA.

Q: How does DNS filtering help with troubleshooting network issues?

A: Advanced DNS filtering solutions can provide valuable insights into network traffic patterns. By logging DNS queries and responses, administrators can identify unusual activity, pinpoint devices or users generating excessive traffic, and understand which domains are being accessed. This data can be instrumental in diagnosing network performance issues, identifying potential security threats, and verifying policy enforcement.

Q: Can DNS filtering cause over-blocking?

A: While DNS filtering is effective, basic implementations can sometimes lead to over-blocking if policies are too broad or if a legitimate domain hosts both appropriate and inappropriate content. More advanced DNS filtering solutions employ granular categorization and intelligent awareness features (e.g., recognizing when a device has a client-based agent) to minimize over-blocking and provide a more nuanced filtering experience.

Q: Is data secure with DNS filtering solutions?

A: The security of data with DNS filtering solutions depends on the vendor and deployment model. Cloud-based solutions typically rely on the vendor's robust data center security and encryption protocols. For on-prem components, the district retains control over local data, while communication with cloud services should adhere to secure standards. Reputable vendors prioritize data privacy and comply with relevant regulations like COPPA.

Q: How quickly can a DNS filtering solution be deployed?

A: Deployment time for DNS filtering solutions can vary. Cloud-only DNS filtering can often be deployed very quickly, sometimes in a matter of minutes or hours, as it primarily involves reconfiguring DNS settings. On-prem or hybrid solutions, which may require installing local software or appliances, can take longer, ranging from days to weeks, depending on the complexity of the network and the chosen setup.

Q: Can DNS filtering filter BYOD and unmanaged devices?

A: Yes. A primary benefit of network-level DNS filtering is its ability to apply policies to any device connected to your network, regardless of whether it has a client-based agent installed. This makes it an excellent solution for ensuring all devices accessing your network are filtered, including guest networks, personal devices, and IoT devices.

Q: How does a DNS filtering solution handle canonical names (CNAMEs)?

A: Advanced DNS filtering solutions often include canonical names for domains that point to other domains. This means when a user accesses an alias (e.g., mail.company.com pointing to ghs.googlehosted.com), the reports can display the true underlying domain. This is crucial for understanding why certain policies might be triggered and for more accurate troubleshooting, providing a full contextual picture.

Q: What is the difference between an on-prem DNS filtering solution and a cloud-only DNS filtering solution?

A: An on-prem DNS filtering solution involves installing a local DNS server within your district network that relays DNS queries, allowing for filtering based on internal IP addresses and subnets, providing granular control and detailed reporting over local traffic. A cloud-only DNS filtering solution typically routes all DNS queries directly to the vendor's cloud service, often relying on external IP addresses for policy application. While cloud-only offers simplicity and off-site coverage, an on-prem component can provide deeper network-level insights and control over local traffic.

Q: How do I implement an on-prem DNS filtering solution?

A: Implementation typically involves installing a service or appliance on a server within your network. This service acts as a DNS relay, listening on port 53 and forwarding requests to the filtering vendor's cloud DNS for policy enforcement. After installation, you'll usually configure network settings (like DHCP) to point devices to this new DNS server and then set up subnets and assign policies within the vendor's management console. For complex environments, seeking guidance from the vendor's solutions engineers is highly recommended.

About GoGuardian Admin

GoGuardian Admin is the comprehensive web filtering and student safety solution keeping nearly 13M students engaged and focused in classrooms. It provides IT administrators with the tools needed to manage online access, protect students from harmful content, and gain visibility into network activity. GoGuardian DNS precision filtering and its advanced reporting capabilities are integral components of the GoGuardian Admin ecosystem, working with our existing deployments to deliver an all-encompassing approach to digital safety.

With GoGuardian Admin, you gain:

- + Intelligent web filtering:** Powered by AI and machine learning to categorize and filter content in real-time.
- + Student safety monitoring:** Proactive alerts for self-harm, violence, and other threats.
- + Device management:** Tools to manage and track school-issued devices.
- + Comprehensive reporting:** Dashboards and reports that provide actionable insights into browsing activity, network traffic, and student engagement.
- + Flexible deployment:** Choose the right mix of cloud, on-prem, and hybrid solutions to fit your unique environment.

Why GoGuardian: A comprehensive solution

At GoGuardian, we are committed to empowering schools with the most advanced, flexible, and insightful web filtering solutions available. Our GoGuardian DNS precision filtering, coupled with comprehensive reporting and the intelligent agent awareness feature, offers a powerful answer to the complexities of modern network management. By providing visibility, streamlined troubleshooting, and adaptable deployment options, we enable you to create a safe, productive, and compliant online learning environment for every student.



GoGuardian DNS precision filtering: Key features

GoGuardian DNS precision filtering integrates with your existing network infrastructure while leveraging the power of GoGuardian Admin's cloud-based policy management and reporting. It's designed to provide the robust, granular control of an on-prem solution with the intelligent insights and flexibility you expect from GoGuardian.

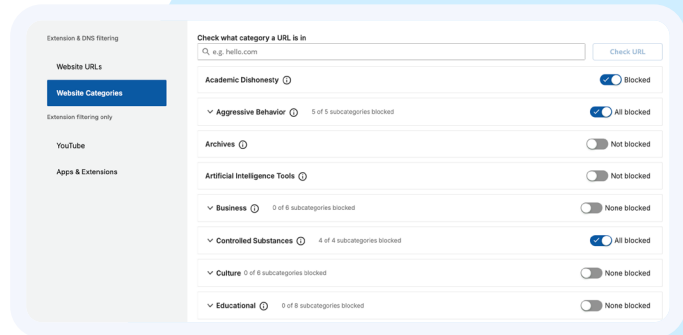
Network filtering with cloud policies

GoGuardian DNS precision filtering allows you to filter a defined range of IP addresses within your network using policies centrally configured and managed in GoGuardian Admin. This hybrid approach offers:

Unified policy management: Create and manage all your filtering policies (for agents and DNS) from a single, intuitive cloud interface.

Customizable policies: Tailor policies precisely to the unique needs of different devices, user groups, and network segments within your environment.

Consistent enforcement: Ensure policies are consistently applied across all devices connected to your on-prem network, regardless of their operating system or agent status.



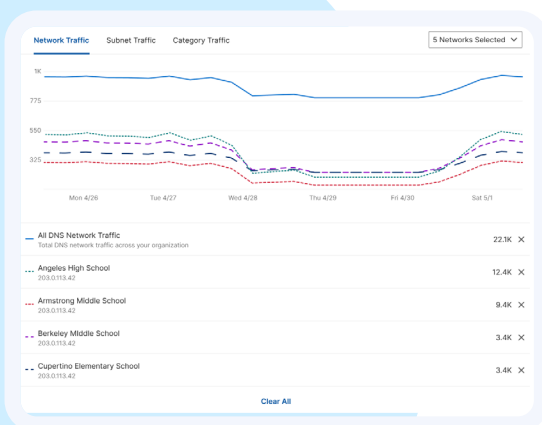
Internal IP address reporting

Visibility is crucial for effective troubleshooting and network management. GoGuardian DNS precision filtering enhances this by reporting web traffic with both public and private IP addresses.

Deep insight into device activity: Gain a clear understanding of which specific devices and internal IP ranges are generating traffic, allowing for precise identification of issues.

Streamlined troubleshooting: Quickly pinpoint the source of unusual activity or filtering conflicts by linking browsing events to internal IP addresses in the Browsing Activity screen in GoGuardian Admin.

Comprehensive traffic analysis: Review web traffic by device or IP range, providing a complete picture of network usage and potential anomalies.



Agent awareness for optimized filtering

A common challenge in hybrid environments is “double filtering,” where both an on-device agent and a network-level DNS filter attempt to apply policies, leading to over-blocking and user frustration. GoGuardian DNS precision filtering's intelligent Agent Awareness feature solves this by:

Preventing duplicate filtering:

Our smart DNS filter recognizes when the GoGuardian App or GoGuardian extensions are installed on a device, preventing redundant filtering.

Reducing over-blocking:

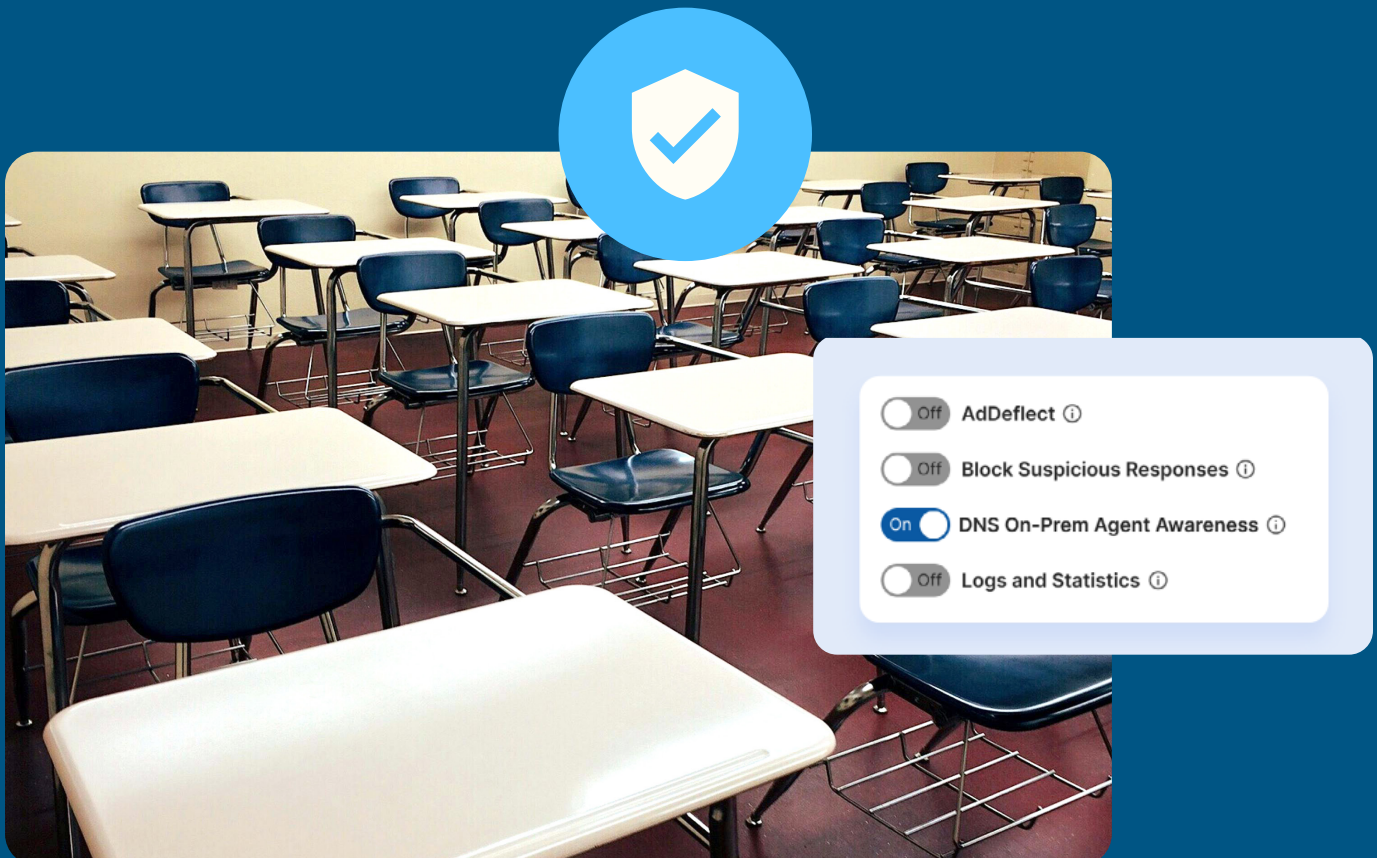
By allowing agent-filtered users to bypass DNS filtering, you can significantly reduce instances of over-blocking, improving the user experience and reducing IT support tickets.

Simplifying troubleshooting:

When agent awareness is enabled, IT Admins can more easily isolate whether a filtering issue originates from the agent or the DNS layer.

Enabling configurable controls:

This feature can be toggled on or off at the Organizational Unit (OU) level within GoGuardian Admin's advanced configuration, giving you granular control over its application.



DNS fallback for uninterrupted protection

Beyond basic filtering, GoGuardian Admin’s enhanced DNS reporting provides deep, actionable insights into your network traffic, transforming raw data into intelligence.

Comprehensive dashboard views: Access intuitive, interactive dashboards that visualize DNS traffic trends by:

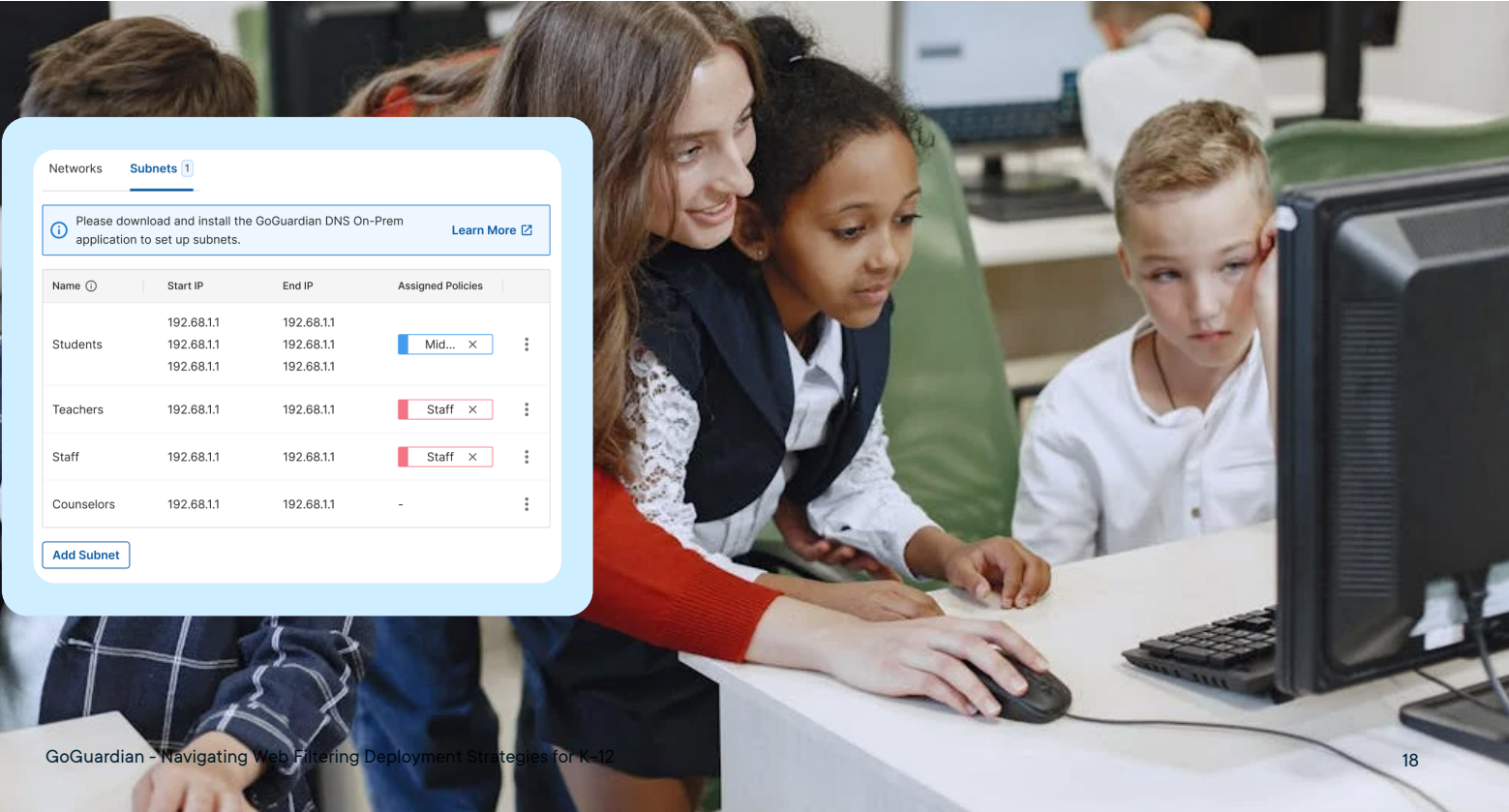
- Network traffic:** See requests across all, or specific, DNS networks over time.
- Website category:** Understand traffic patterns across educational, appropriate, gaming, and other categories.
- Internal/external IP addresses:** Monitor traffic originating from or destined for specific IP ranges, with the ability to toggle between internal and external views.

Real-time insights: Identify spikes, trends, and anomalies in bandwidth consumption, category usage, and views/blocks.

Troubleshooting power: Quickly identify potential conflicts, unusual activity, or policy gaps with detailed data.

Exportable data: Export chart views as PNG images or underlying data as CSV files for further analysis and reporting to stakeholders.

Canonical name (CNAME) reporting: For domains that point to other domains (aliases), our reports now display the true canonical name, providing critical context for troubleshooting and understanding why certain policies are triggered.



GoGuardian Admin is the #1 choice for K-12 web filtering and designed to create safer, more productive digital learning environments. Powered by advanced AI and machine learning, GoGuardian Admin provides K-12 schools with industry-leading web filtering, unified policy management across all devices and operating systems, and instant alerts for harmful content.

Learn more: <https://www.goguardian.com/admin>

