FUNDS FOR LEARNING

K-12 Cybersecurity & E-rate Policy Report

Understanding Demand, Existing Funding, and the Path to Permanent Support

March 2026

FundsForLearning.com

97.7%	$3.7B	$246M
of E-rate applicants support cybersecurity eligibility (8-year average)	in Phase 1 cybersecurity pilot demand; 90x current annual firewall line-item costs	in total E-rate firewall demand over 6 years. Dwarfed by $3.7B in cybersecurity pilot demand

A Message from the CEO

To school administrators, IT directors, E-rate coordinators, and policymakers:

In November 2022, Funds For Learning submitted formal comments to the FCC urging the Commission to act on K-12 cybersecurity. We made a simple argument: the students and educators who depend on E-rate-funded networks deserve to have those networks protected. The program's mandate doesn’t end at connectivity.

Since then, a great deal has changed. The FCC launched the Schools and Libraries Cybersecurity Pilot Program, drawing 2,700 applicants requesting $3.7 billion in funding in its first phase. A smaller Phase 2 cohort revealed granular demand data: advanced firewalls, endpoint protection, identity management, and monitoring, presented not as abstract wish lists, but as funded line items from real schools, some of the most under-resourced in the country.

This report brings together four streams of evidence that, taken together, make a compelling case for a permanent, well-funded cybersecurity program within E-rate:

1. Eight years of survey data showing near-unanimous demand from E-rate applicants for cybersecurity eligibility.
2. Survey open-ended comments tracking the evolution of the cybersecurity conversation from general concern to specific, sophisticated requests.
3. Phase 2 cybersecurity pilot data providing the first public view of real-dollar demand by service type, state, and applicant profile.
4. Six years of E-rate firewall funding data, the program’s only current cyber-adjacent baseline, revealing both the value of existing support and the structural limitations that cap it.

The evidence is consistent and overwhelming. Schools are already requesting cybersecurity funding at a scale that dwarfs what the current program can support, and the most vulnerable districts are the most active participants.

This report is supported by 660 verbatim comments from school and library officials collected between 2019 and 2025. Their words document not an abstract policy debate, but a decade of real frustration, real attacks, and real gaps in protection. See the companion Appendix, “Applicant Voices on Cybersecurity.”

The question before policymakers is not whether the need exists. The data on that is settled. The question is whether the program will be designed to meet it. We offer this report as an analytical resource for that conversation.

John D. Harrington

Chief Executive Officer, Funds For Learning

Executive Summary

Funds For Learning's 2026 analysis draws on four primary data sources to assess the current state of K-12 cybersecurity funding through the E-rate program. This report synthesizes annual applicant survey data (2018–2025), the open-ended comments accompanying those surveys, line-item demand data from the FCC's Cybersecurity Pilot Program Phase 2, and six years of E-rate Category 2 firewall funding records (FY2020–FY2025). Collectively, these sources tell a consistent and urgent story.

Key Findings

#	Finding	Source
1	97.7% of E-rate applicants have supported cybersecurity eligibility every year for 8 consecutive years (2018–2025).	Annual Survey
2	Network security ranks 4th out of 10 eligible-service-list options in 2025, tied with already-eligible services and far above all others.	Annual Survey
3	660 cybersecurity-related comments across 2019–2025, rising from 13% of all comments in 2019 to 23% in 2023 and 22% in 2025. All 660 are published verbatim in the companion Appendix.	Survey Comments
4	Comments have evolved from general requests to sophisticated asks: EDR, SIEM, MFA, zero-trust frameworks, and insurance mandate coverage.	Survey Comments
5	Phase 1 of the cybersecurity pilot attracted $3.7 billion in demand from ~2,700 applicants, roughly 90x the annual E-rate firewall line-item costs.	Pilot Phase 1
6	Phase 2 pilot data shows $174M in pre-discount requests across 614 applicants, with monitoring/detection as the top service category.	Pilot Phase 2 Data
7	99.6% of Phase 2 pilot applicants qualify at the 90% discount rate, the highest-need schools in the country.	Pilot Phase 2 Data
8	Total firewall line-item costs across FY2020–2025 are $246.2M ($241.3M one-time + $4.9M recurring, all statuses), representing the firewall-specific portions of FRNs that in some cases also included other eligible services.	Firewall Data
9	The 'basic firewall' restriction rules 25% of one-time costs ineligible, suppressing both participation and approved amounts. The program is also structurally steering schools toward hardware rather than the ongoing managed services that dominate pilot demand.	Firewall Data
10	Per-applicant firewall costs spiked in FY2024 (+41% vs FY2022), reflecting aging hardware replacement cycles and rising security costs.	Firewall Data

FFL ANALYSIS

The convergence of all four data sources is striking. Survey demand has been overwhelming and stable for nearly a decade. Pilot demand was exponentially larger than existing firewall funding. And the firewall data, the only current cyber-adjacent baseline E-rate has, shows a program that is reaching the right schools but structured in a way that prevents it from meeting their actual needs. A permanent, expanded cybersecurity program is the logical conclusion of everything the data says.

Section 1: How E-rate Works and Where Cybersecurity Fits

The E-rate Program

The E-rate program (formally the Schools and Libraries Universal Service Support Mechanism) is administered by the Universal Service Administrative Company (USAC) under the oversight of the Federal Communications Commission (FCC). Since 1998, E-rate has provided discounts on telecommunications and technology services to eligible K-12 schools and public libraries, prioritizing the highest-need applicants through a sliding discount scale from 20% to 90%.

E-rate funding is divided into two categories. Category 1 covers broadband connectivity, the data transport services that bring internet access to a building. Category 2 covers internal network infrastructure, the equipment and services that distribute that connectivity within a building, including Wi-Fi access points, switches, firewalls, and cabling. Cybersecurity tools, to the extent they are currently eligible at all, appear in Category 2 under a narrow “basic firewall” interpretation.

The Cybersecurity Threat Landscape

K-12 schools have become high-value targets for ransomware, phishing, and data exfiltration attacks. The Cybersecurity and Infrastructure Security Agency (CISA) has consistently flagged the education sector as one of the most frequently attacked. Districts often operate with limited IT staff, aging infrastructure, and no dedicated security budget, a combination that makes them both attractive targets and poorly positioned to respond.

The consequences are real: student data breaches, instructional disruptions lasting weeks, ransom payments, and ongoing liability. No districts are facing new pressure: cyber insurance carriers requiring specific security controls (MFA, EDR, endpoint protection) as a condition of coverage. Schools that cannot afford these tools face a genuine bind: they need coverage but cannot qualify for it.

Policy Timeline

2022	2023	2024	2025 to Present
• 98% of E-rate survey respondents request cybersecurity included in E-rate program. • Funds For Learning submits formal comments urging action. • FCC seeks comment on advanced firewalls and network security.	• FCC comment period yields widespread support from hundreds of schools, libraries, manufacturers, service providers, and advocacy organizations. • FCC opens rule making (NPRM) for cybersecurity pilot.	• FCC formally adopts the $200M Schools and Libraries Cybersecurity Pilot Program (June) • 2,700 applications received requesting $3.7 billion in funding, demonstrating massive unmet demand. (Phase 1)	• FCC announces 700+ selected Phase 2 participants from the applicant pool (Jan) • First wave of cyber pilot funding released (Dec) • On-going waves of cyber pilot funding (Jan 2026 to current)

Section 2: What This Analysis Is Based On

Source 1: Annual Applicant Survey Cybersecurity Results (2018–2025)

Funds For Learning has conducted fifteen annual surveys of E-rate applicants. The survey captures applicant demographics, program satisfaction metrics, and opinions on proposed program changes, including the eligible services list (ESL). Cybersecurity eligibility has been a survey topic since 2018. In that period, 14,972 survey responses have been received, averaging 1,872 per year.

Source 2: Survey Open-Ended Comments

Each annual survey includes a free-text comment field. FFL analyzed 3,877 comments from 2019 through 2025 for cybersecurity-related content. 660 respondents specifically referenced cybersecurity, firewalls, content filtering, network threats, or related topics, representing 15% of all open-ended comments. FFL analyzed these comments for theme, specificity, and year-over-year evolution. The complete verbatim record of all 660 comments, along with thematic analysis and featured excerpts, is published as a companion document: “Applicant Voices on Cybersecurity” (see Appendix).

Source 3: Cybersecurity Pilot Program Data (Phase 2)

The Phase 2 dataset covers 614 unique applicants, 737 applications, and 3,422 funding request line items. Total pre-discount eligible amount: approximately $174 million. This dataset was analyzed by service category, state, participant type, urban/rural status, discount rate, and service provider. Note that Phase 1 demand ($3.7B) remains unavailable at the line-item level; Phase 2 is treated as an indicative but not representative sample of full program demand.

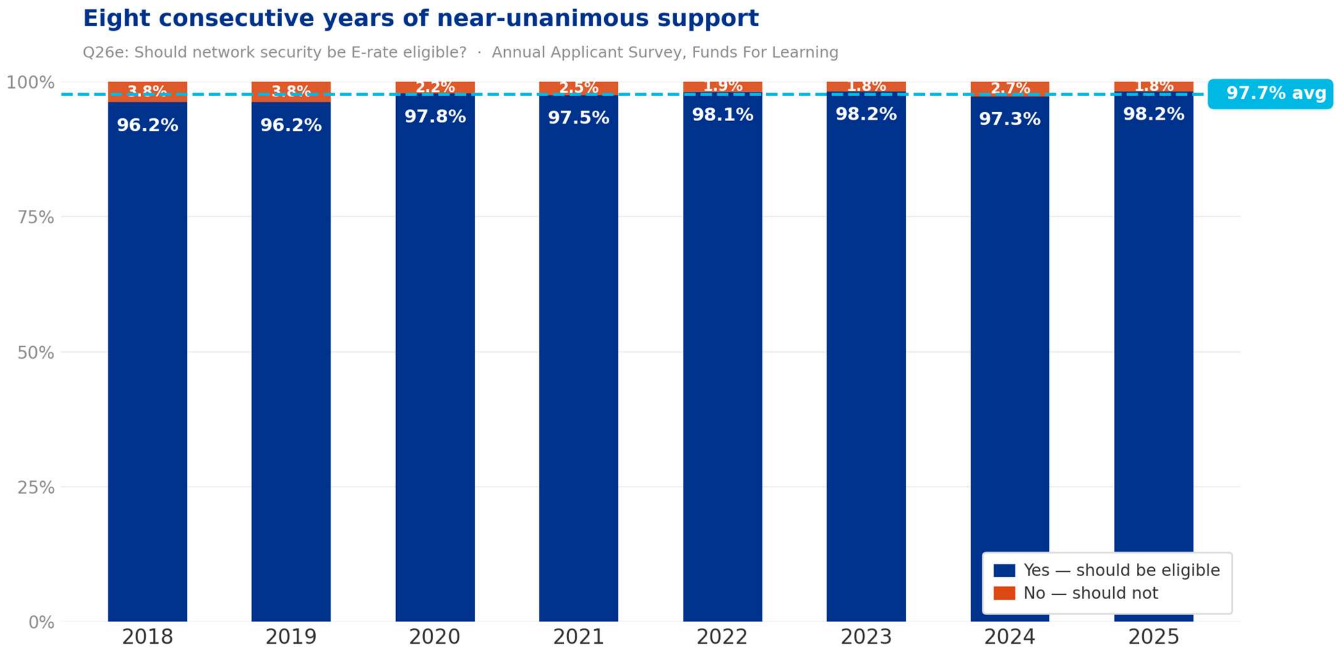
Source 4: E-rate Category 2 Firewall Funding (FY2020–2025)

Using its E-rate Manager® tool, FFL obtained and analyzed six years of E-rate Category 2 firewall FRN (Funding Request Number) data. The dataset includes 14,988 individual FRN line items, of which 12,933 reached ‘Funded’ status. Analysis covers funding amounts, participant demographics, vendor/make distribution, state-level patterns, and discount rate distribution.

Section 3: Sustained, Near-Unanimous Demand (2018–2025)

Q26e: Should Network Security Be E-rate Eligible?

This question asks respondents whether they support expanding E-rate eligibility to include "network security and network management goods and services." It has been included in every survey since 2018. Across all eight years and 13,525 total responses, an average of 97.7% of respondents said yes, a level of support that has remained above 96% in every single year.

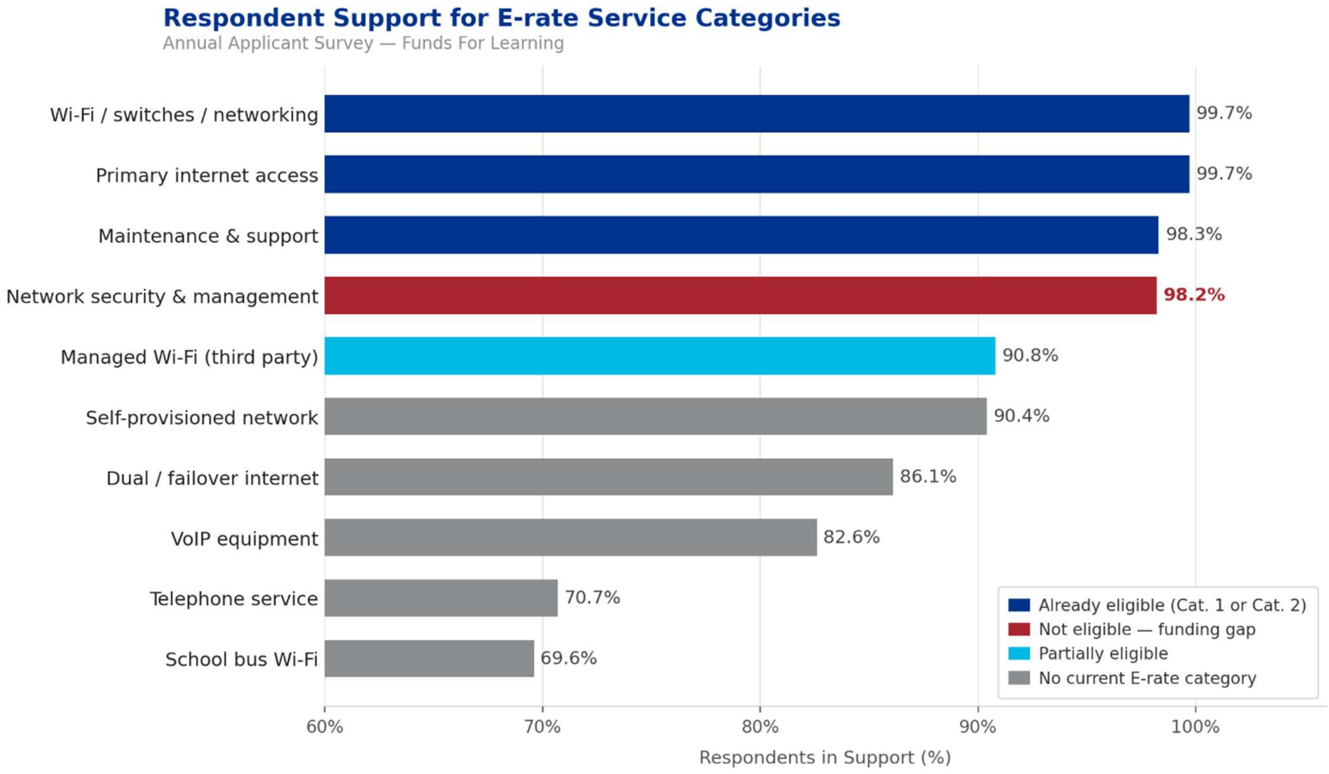


FFL ANALYSIS

The 97.7% eight-year average is arguably the strongest sustained policy signal in the entire E-rate survey history. This isn't a trending issue. It was nearly unanimous from the very first year it was asked and has never moved below 96%. The ceiling was hit almost immediately; there was simply nowhere higher to go.

2025 Eligible Services List Rankings

In 2025, respondents ranked 10 services by their support for E-rate eligibility. Network security placed 4th, essentially tied with services that are already funded.



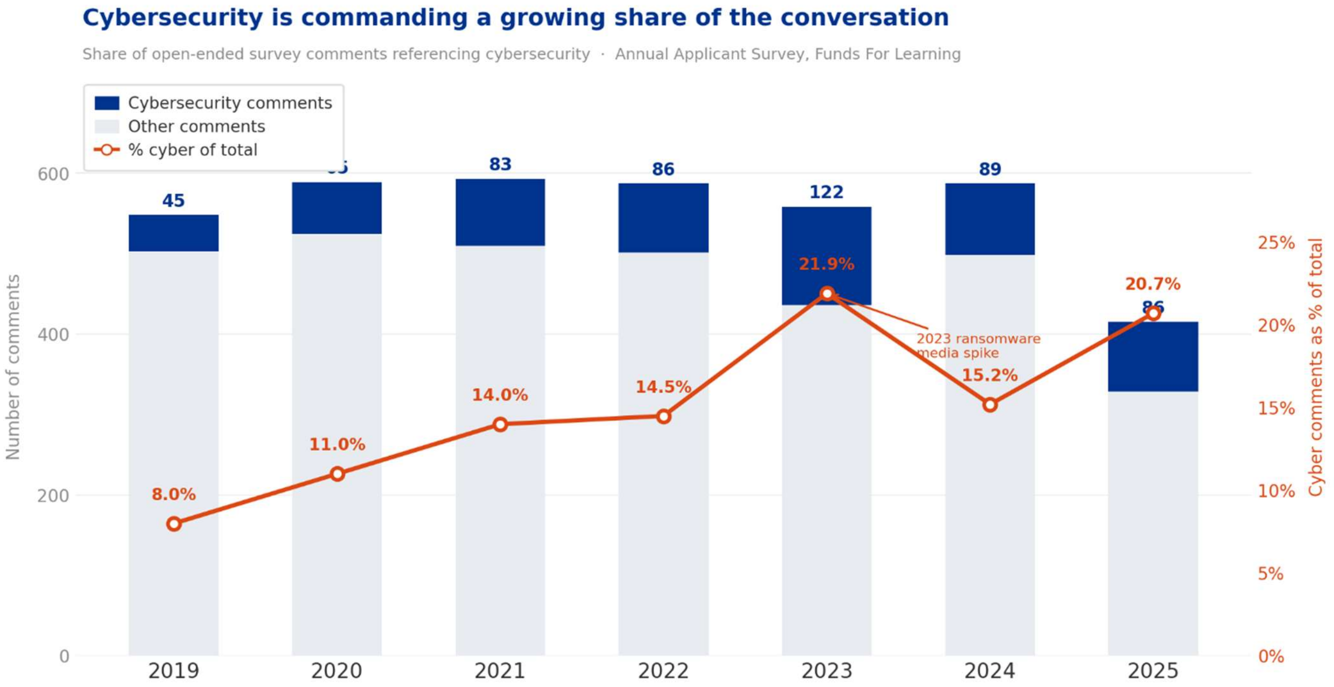
POLICY IMPLICATION

Network security is separated from the ‘already eligible’ tier by just 0.1 percentage points. The policy argument for its exclusion has always been tenuous; this data makes it essentially untenable.

Section 4: What Applicants Are Actually Saying (2019–2025)

Volume & Trend

When respondents write in their own words about E-rate priorities, cybersecurity surfaces with increasing frequency. Of the 3,877 open-ended comments collected between 2019 and 2025, 15% referenced network security or cybersecurity concerns.



FFL ANALYSIS

The 2023 spike to 21.9% aligns precisely with the period of peak ransomware coverage in education media and congressional attention on K-12 cybersecurity. Notably, 2025's share (20.7%) remains nearly as elevated, suggesting the urgency has become structural, not episodic.

Recurring Themes

1. The Firewall Problem

The single most common specific complaint across all years. Applicants describe an illogical situation: hardware is eligible, but the software subscriptions and advanced features that make that hardware useful are not. Comments specifically call out IPS, UTM, threat prevention, and next-generation functionality being denied while the physical appliance is funded.

> *“We can get the firewall funded but not the subscription that makes it work. A firewall without threat intelligence updates is just expensive hardware.”*
>
> *-- Survey respondent, 2022*

2. CIPA Compliance Contradiction

Multiple respondents point out that CIPA compliance is a requirement for receiving E-rate funding, yet the content filtering tools needed to achieve that compliance are not fully eligible. This is seen as contradictory program design.

3. Escalating Threat Sophistication

Early comments (2019–2020) focused on firewalls and DDoS protection. By 2021–2022, ransomware became a dominant term. By 2023–2025, applicants were naming specific technologies: EDR, SIEM, MFA/2FA, zero-trust frameworks, and penetration testing. The sophistication of requests tracks the broader industry conversation almost exactly.

> *“We were hit with ransomware last spring. We had a basic firewall funded through E-rate. We needed an EDR solution, incident response support, and MFA. None of it was eligible. We paid out of pocket or went without.”*
>
> *-- Survey respondent, 2023*

FFL ANALYSIS

The evolution of comment language from 2019 to 2025 mirrors the broader K-12 security threat landscape almost exactly. Early respondents asked for firewalls. Later respondents named EDR vendors and zero-trust frameworks. This is not a static or abstract concern. It is an active, escalating operational challenge that applicants are tracking in real time. The program’s eligibility structure has not kept pace.

4. The Small District Problem

Many of the most urgent comments come from one- or two-person IT shops. These districts lack the scale to justify enterprise security contracts on their own, making E-rate their only realistic pathway to funded protection.

> *“I am a one-person IT department for 4 schools. I cannot afford the tools my students need without E-rate. The pilot is a good start but $200M nationally doesn’t help my district in a meaningful way.”*
>
> *-- Survey respondent, 2024*

5. Cyber Insurance Mandates (2023–2025)

A new driver emerged in the 2023–2025 comment period: insurance carriers requiring specific security tools as a condition of coverage. This creates a mandated cost with no current funding pathway, and applicants find this particularly frustrating.

> *“Our insurance now requires MFA and endpoint protection. These aren’t optional -- we lose coverage without them. But E-rate won’t pay for them. Where do we get the money?”*
>
> *-- Survey respondent, 2025*

6. The Pilot as Down Payment

2024 and 2025 comments reference the pilot program specifically. The recurring sentiment is appreciation combined with urgency: the need is now, the funding cap is far below demand, and applicants are anxious about what happens when the pilot ends.

> *“The $200M pilot is a step forward but it’s a tiny fraction of what is needed. The need is now, not after the pilot concludes.”*
>
> *-- Survey respondent, 2024*

Appendix: Applicant Voices on Cybersecurity

The six thematic excerpts above represent a small fraction of the full record. The companion Appendix, “Applicant Voices on Cybersecurity,” presents all 660 cybersecurity-related survey comments verbatim, organized in two parts:

- Part A: Featured Voices. Twenty representative comments in five themes (The Unfunded Mandate, The Budget Squeeze, The Human Cost, and others), each with brief editorial context.
- Part B: Complete Record. All 660 comments presented verbatim, grouped by survey year (2019–2025).

Section 5: Cybersecurity Pilot Program - Phase 2 Analysis

Phase 2 at a Glance

614 unique applicants | 737 applications | 3,422 FRN line items | 50 states represented

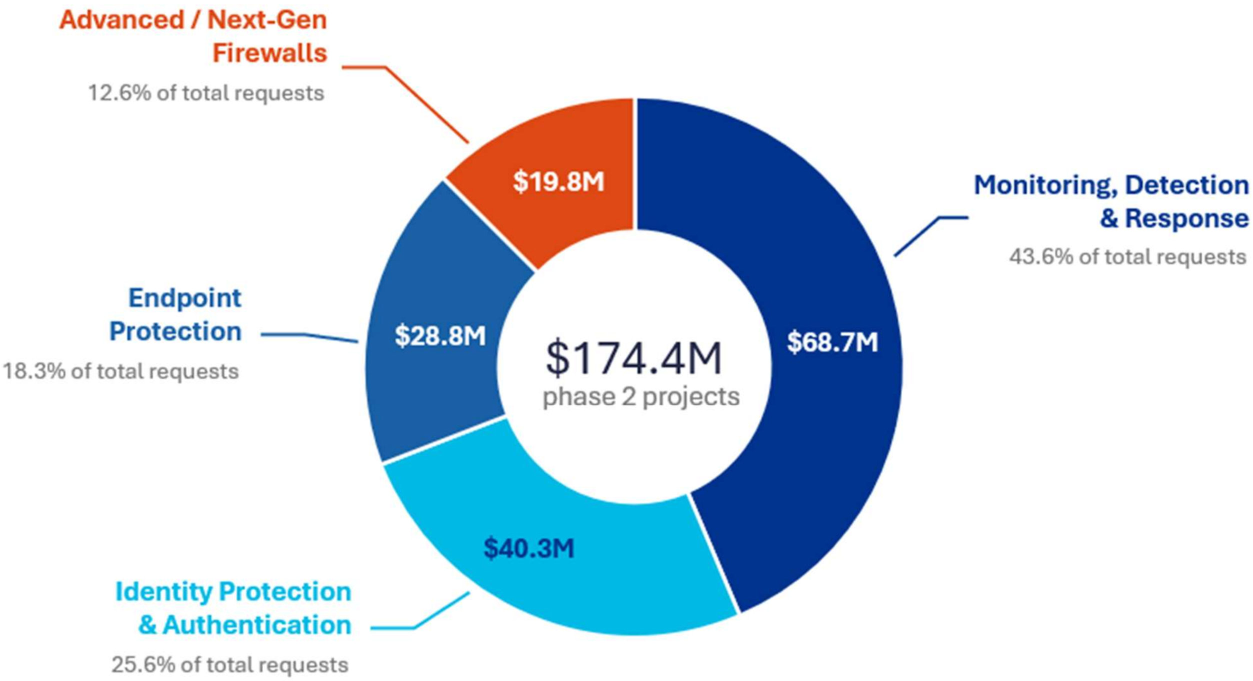
$174.4 M total pre-discount | $157.5M requested

Note: Phase 1 drew ~2,700 applicants requesting $3.7B. Phase 2 is a selected subset. Demand figures here significantly understate total program need.

Funding by Service Category

Monitoring & Detection commands the largest share of pilot demand

Share of total $ requested | FCC Cybersecurity Pilot Program, Phase 2



FFL ANALYSIS

Monitoring, detection, and response is the largest category by FRN count and dollar volume. This is a meaningful signal: schools are not simply trying to buy hardware. They are seeking active, managed security services.

The $3.7B Phase 1 figure is the single most important number in the cybersecurity funding debate. It is approximately 90 times the annual E-rate firewall line-item costs, and it came from applicants who had to navigate a new, unfamiliar application process with no guarantee of funding. Actual latent demand, from schools that didn't apply because they were skeptical of success, is almost certainly higher still.

POLICY IMPLICATION

99.6% of Phase 2 pilot applicants qualify at the 90% discount rate. This is not a coincidence. It reflects the concentrated, disproportionate cyber-vulnerability of the highest-poverty schools. Any permanent program that does not preserve or strengthen this equity priority will fail the schools that need it most. The existing discount structure is not the problem. The funding level and eligibility scope are.

Section 6: E-rate Firewall Funding: The Existing Baseline (FY2020–FY2025)

Before the cybersecurity pilot existed, the only portion of E-rate that addressed cybersecurity at all was the narrow eligibility of "basic" firewall hardware under Category 2. This section analyzes six years of that funding in detail, not just as historical context, but as a lens for understanding both what the existing program delivers and the structural constraints that limit it.

Firewall Funding at a Glance (FY2020–FY2025)

~7,750 unique applicants funded | ~10,600 funded FRNs

Firewall line-item costs: $241.3M one-time + $4.9M recurring = $246.2M total (~$41M/year avg) These figures reflect firewall-specific line items. Some FRNs also included other eligible services; costs here represent only the firewall portion.

Funding Levels by Year

Fiscal Year	Unique Applicants	Funded FRNs	Total Firewall Cost (All Records)
FY2020	1,803	1,979	$37.0M
FY2021	1,645	1,770	$34.6M
FY2022	1,567	1,744	$34.0M
FY2023	1,478	1,578	$38.1M
FY2024	1,572	1,643	$56.6M
FY2025	1,769	1,879	$45.8M
Total	**7,751***	**10,613**	**$246.2M**

**Unique across all years; individual applicants may have received funding in multiple fiscal years. Dollar figures represent firewall-specific line-item costs across all FRN statuses (funded, cancelled, denied, pending), including both eligible and ineligible cost components. Where an FRN bundled firewalls with other services, only the firewall line items are counted here.*

FFL ANALYSIS

The FY2024 spike in average firewall line-item cost per FRN (+68% vs. FY2022) is significant. It likely reflects two converging forces: schools finally replacing hardware that had been deferred through the COVID years, and the rising cost of security-grade appliances as basic hardware increasingly incorporates features that schools actually need. The FY2025 partial reversion may reflect some normalization, but the trend line since FY2022 is clearly upward. Annual funding will need to grow to keep pace with per-unit costs, let alone to expand to more participants.

The ‘Basic Firewall’ Restriction: Suppressed Demand

The E-rate program currently funds only “basic” firewall functionality under Category 2. Advanced features, including intrusion prevention systems (IPS), unified threat management (UTM), deep packet inspection, threat intelligence subscriptions, and next-generation firewall (NGFW) capabilities, are generally ineligible or require complex cost-allocation to fund the eligible portion.

This creates two compounding distortions in the data:

- Demand suppression: Applicants who need advanced firewall capabilities may not apply at all, knowing that the eligible portion of their costs will be small or disputed. The ~1,600–1,800 funded applicants per year represents a fraction of the 20,000+ annual E-rate participants.

- Undercounting of real need: When the pilot opened advanced/next-gen firewalls as a distinct eligible category, it drew 662 FRNs from Phase 2 alone, a cohort of only 614 applicants. That’s more firewall FRNs per applicant than the standard E-rate program generates, because applicants finally had a vehicle to fund what they actually need.

POLICY IMPLICATION

The firewall data does not show a program meeting demand. It shows a program where demand has been structurally discouraged by eligibility rules. Approximately $41M/year in firewall line-item spending sounds meaningful until you compare it to $3.7B in Phase 1 pilot demand.

Contextualizing Firewall Funding Against Pilot Demand

Metric	Value	Context
Annual E-rate firewall line-item costs (avg, all statuses)	~$41M	Firewall line-item baseline;
Total 6-year gross firewall demand	$246.2M	$241.3M one-time + $4.9M recurring;
Phase 2 pilot pre-discount requests	$174.4M	Per applicant funding caps limit reporting of true demand
Phase 1 pilot total demand	$3.7B	~15x total 6-year gross firewall demand, from ~2,700 applicants in one window
Firewall one-time costs ruled ineligible	25.3%	$61M stripped from eligible pool by the basic firewall restriction

POLICY IMPLICATION

The E-rate firewall data is not evidence that the program is working. It is evidence that a structurally constrained program is nonetheless reaching the right schools with the wrong tools. The $3.7B in Phase 1 pilot demand arrived in a single application window, from applicants navigating a new process, with no assurance of funding. The true gap between what schools need and what E-rate currently provides for cybersecurity is enormous. A permanent program needs to be sized accordingly.

Section 7: Conclusions & Policy Recommendations

Conclusions

The demand case is closed.

Eight years of survey data, $3.7 billion in Phase 1 pilot requests, and six years of constrained firewall funding all point in the same direction. Schools need cybersecurity support. The question is structural, not evidentiary.

The existing program is reaching the right schools with the wrong tools.

The firewall data confirms that E-rate is successfully targeting the highest-need applicants. Over 56% of funded firewall FRNs come from the 80% and 85% discount tiers. But the ‘basic firewall’ restriction means those schools are being funded for partial solutions.

The gap between current funding and actual need is approximately 30:1.

$3.7 billion in Phase 1 demand versus ~$41 million in annual firewall line-item costs. Even accounting for the pilot’s selection effects and the firewall data’s structural limitations, this ratio indicates systemic under-investment at a scale that marginal adjustments will not address.

Schools are moving faster than the program.

Comment themes now include insurance mandates, EDR, SIEM, zero-trust architecture, and penetration testing. The program is discussing basic firewalls while applicants are managing sophisticated, evolving threats. The sophistication gap widens every year.

The managed services shift is real and requires administrative adaptation.

Demand is heavily oriented toward ongoing services, including monitoring, detection, and identity management, not just hardware. USAC’s compliance and invoicing frameworks were built for equipment procurement. A permanent program must address this structural mismatch.

Policy Recommendations

1. Make the Cybersecurity Pilot Permanent and Scale Funding Commensurately

The pilot should not end without a successor program. Phase 1 demand of $3.7 billion from a single application window establishes the minimum floor of need. Annual cybersecurity funding should be set significantly above the current $41M firewall line-item baseline; $1 billion annually would serve roughly 27% of demonstrated Phase 1 demand.

2. Eliminate the ‘Basic Firewall’ Restriction

The distinction between ‘basic’ and ‘advanced’ firewalls is technically obsolete and administratively counterproductive. Modern firewall products are inherently next-generation. Eligibility should cover fully functional firewalls, including the software subscriptions and threat intelligence services that make them effective.

3. Adopt the Four-Category Service Framework

The pilot's four service categories, monitoring/detection, identity protection, advanced firewalls, and endpoint protection, reflect where schools are actually spending. These should form the foundation of a permanent eligibility structure, potentially with a fifth category for incident response and professional security services.

4. Preserve the Equity Priority

Any permanent program should maintain or strengthen the current discount structure that prioritizes high-poverty schools. The existing firewall data demonstrates that the mechanism works as intended. The problem is the funding level and eligibility scope, not the targeting.

5. Develop MSSP-Appropriate Compliance Frameworks

USAC should develop invoicing, audit, and reporting protocols specifically designed for managed security services, in parallel with any rulemaking for a permanent program. Applying hardware procurement compliance standards to ongoing managed services creates friction that disadvantages the very service types most needed by schools.

6. Require Disclosure of Phase 1 Demand Data

The FCC should make the line-item Phase 1 demand data publicly available, either in full or in aggregated form. The current gap, where Phase 1 totals are known but service-type breakdowns are not, limits the quality of evidence available to policymakers and advocates. Transparency strengthens the case for a well-designed permanent program.

DATA SOURCES & LIMITATIONS

- **Annual Survey:** Self-selected respondents; not a random sample of all E-rate applicants. Response rates and counts vary by year. Trends are directionally reliable but should not be interpreted as precise population statistics.
- **Pilot Phase 2 Data:** Phase 2 applicants were selected by the FCC from Phase 1 pool; the selection criteria are not fully public. Phase 2 data should not be treated as a representative sample of all K-12 cybersecurity demand.
- **Firewall Data:** Covers only the demand captured on E-rate applications. Real demand is suppressed by the limited eligibility of firewalls. Actual demand is likely much higher, as indicated in the Phase 1 data.
- **Phase 1 Demand:** The $3.7 billion figure is derived from FCC public statements. Line-item detail was not released and is not available for independent verification. This figure is used for context only.

Published by Funds For Learning • fundsforlearning.com • March 2026