CROWDSTRIKE

Wireline Competition Bureau Seeks Comment on Requests To Allow the Use of E-Rate Funds for Advanced or Next-Generation Firewalls and Other Network Security Services

WC Docket No. 13-184

February 13, 2023

I. INTRODUCTION

In response to the Federal Communication Commission ("FCC") Wireline Competition Bureau's comment period on "Allow[ing] the Use of E-Rate Funds for Advanced or Next-Generation Firewalls and Other Network Security Services" ("public notice") CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

We appreciate the FCC's efforts to better protect the sensitive data from K-12 schools and to ensure that students pursue education without disruption from cyber attacks. Cybersecurity threats are evolving and increasing across all sectors, and the education sector is among the more heavily-targeted. Illustrative of this, in CrowdStrike's 2022 *Global Threat Report*, we observed a 82% increase in ransomware-related data leaks (from 2021 - 2022), frequently affecting educational institutions and other public sector entities.[1]

[1] 2022 *Global Threat Report*, CrowdStrike, https://www.crowdstrike.com/global-threat-report/

Malicious actors are opportunistic and in many instances do not discriminate in their targeting. In fact, ransomware is one of the most common types of attacks affecting schools, and those campaigns seek to leverage the coercive effects of school disruptions.

Today, almost all forms of K-12 education have some type of online component. The E-Rate program has successfully given many schools the funds to procure the technologies needed to make use of new ways of learning. Through the annual E-Rate eligible services list (ESL) proceedings, the FCC has received requests for the E-Rate program to support advanced or next-generation firewalls and services, as well as other network security services. CrowdStrike supports the expansion of the ESL to include next-generation firewalls and services and recommends the FCC go a step further to include other cybersecurity security tools on the ESL list.

While we do not have feedback on every question in the public notice, we do want to offer responses to several questions along with overarching comments that may be of value to the FCC as it considers expanding the scope of E-Rate.

A. Cybersecurity is a necessary part of connectivity.

Given that so much of education has moved online, schools cannot continue to procure technologies – using E-Rate – without corollary cybersecurity investments. The public notice states: "Although some parties previously have advocated to expand E-Rate support for anti-virus and anti-spam software, intrusion protection, and intrusion prevention devices, the Commission has declined to do so in the context of various E-Rate proceedings to ensure that limited E-Rate funds are directed to the E-Rate program's primary purpose of providing connectivity to and within schools and libraries." CrowdStrike believes this logic is flawed and the FCC is correct in reconsidering this matter in this public notice. There cannot be connectivity in today's cyber threat landscape without accompanying cybersecurity measures.

B. Definition of Advanced or Next-Generation Firewalls and Services.

With regard to question 8, the E-Rate program currently defines "firewall" as:

> "a hardware and software combination that sits at the boundary between an organization's network and the outside world, and protects the network against unauthorized access or intrusions."

We strongly recommend an updated definition that, at a minimum, includes a more expansive set of security technologies. The suggested definition from E-Rate program stakeholders including CoSN, Alliance for Excellence in Education, State Educational Technology Directors Association, Council of the Great City Schools, State E-Rate Coordinators' Alliance, and Schools, and Health & Libraries Broadband Coalition serves this purpose adequately. They recommend including all firewall and related features (e.g., next generation firewall protection, endpoint protection, and advanced security) and to update the definition of broadband to include cybersecurity.

Notably, emerging security technologies like those referenced above, which augment, substitute, or strengthen traditional firewall capabilities, offer many benefits for users. Benefits include automated control of network traffic which enables temporary access restrictions to known compromised websites. Furthermore, they leverage artificial intelligence and machine learning to automatically update allow- and block-lists to protect networks with no actions needed from the schools.

C. Eligible Equipment and Services.

Firewalls are one piece of a cybersecurity strategy, but they are not enough on their own to stop a cybersecurity attack. Firewalls do not protect against phishing campaigns, stolen credentials, or many types of malware attacks. The best-in-class security tools evolve regularly. In regards to question 9, CrowdStrike recommends that the FCC update the ESL to include tools that are not overly prescriptive so that schools can choose the best security practices for their level of risk. CrowdStrike recommends the following tools and themes be added to the ESL which would more comprehensively protect internet-connected school devices.

- Endpoint Detection and Response (EDR): EDR is the cybersecurity approach to defending endpoints such as desktops, laptops, and mobile devices from malicious activity. Given that schools have so many connected devices, EDR would be helpful in identifying and preventing threats and enabling threat hunting activities in case adversaries gain unauthorized access.

- Zero Trust: Due to fundamental problems with today's widely-used authentication architectures, organizations must incorporate new security protections focused on authentication. Zero Trust design concepts radically reduce or prevent lateral movement and privilege escalation during a compromise. Implementing a Zero Trust strategy can include, but is not limited to, EDR, Multi-Factor Authentication, and logging capabilities.

- Identity Protection and Authentication: As schools embark on a digital transformation to remote learning, Bring-Your-Own-Device policies become commonplace, cloud services multiply, and enterprise boundaries continue to erode. This trend increases the risk of relying upon traditional authentication methods and further weakens obsolescent legacy security technologies. Identity-centric approaches to security use a combination of real-time authentication traffic analysis and machine learning analytics to quickly determine and respond to identity-based attacks.

It is also worth noting that the best cybersecurity tools will not work to their full potential unless there are people who are trained to implement, operationalize, and maintain them. Given that there is a nation-wide shortage of cybersecurity talent, some schools may lack the cybersecurity staffing and maturity to effectively run a cybersecurity program and should consider managed service providers to achieve their security goals. Managed service providers should be added to the ESL as the necessary advanced cybersecurity tools are added.

D. Alignment with other agency guidance.

Following an increase of cybersecurity attacks on schools, Congress passed the K-12 Cybersecurity Act of 2021. Part of the Act required the Cybersecurity and Infrastructure Security Agency (CISA) to develop a report on the cybersecurity risks schools face along with accompanying recommendations. This report was recently released and CISA's recommendations include prioritize near-term investments in alignment with CISA's Cross-Sector Cybersecurity Performance Goals (CPG), over the long-term develop a cybersecurity plan that leverages the NIST Cybersecurity

Framework, and minimize the burden of security by migrating IT services to more secure cloud versions.[2]

CrowdStrike believes that adding next-generation security technologies, outlined above to the ESL will allow schools to meet the recommendations outlined by CISA. The CPG and NIST Cybersecurity Framework mentioned in CISA's recommendations both call for a risk-based cybersecurity plan that uses strategies such as Zero Trust and Identity Protection while leveraging tools such as cloud-based security platforms and EDR. Expanding the ESL will allow for greater harmonization among government agency activities.

III. CONCLUSION

The FCC's public notic represents a thoughtful attempt to listen to stakeholder feedback and to strengthen security outcomes in a complex legal and policy environment. As the FCC moves forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that any proposed rule updates focus on principles, and are flexible, rather than prescriptive requirements. Further, we recommend these updates include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike®, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

[2] *K-12 Protecting Our Future Report*, CISA, https://www.cisa.gov/protecting-our-future-partnering-safeguard-k-12-organizations-cybersecurity-threats

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.

CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley CIPP/E	**Robert Sheldon**
VP & Counsel, Privacy and Cyber Policy	Director, Public Policy & Strategy

Email: policy@crowdstrike.com

***