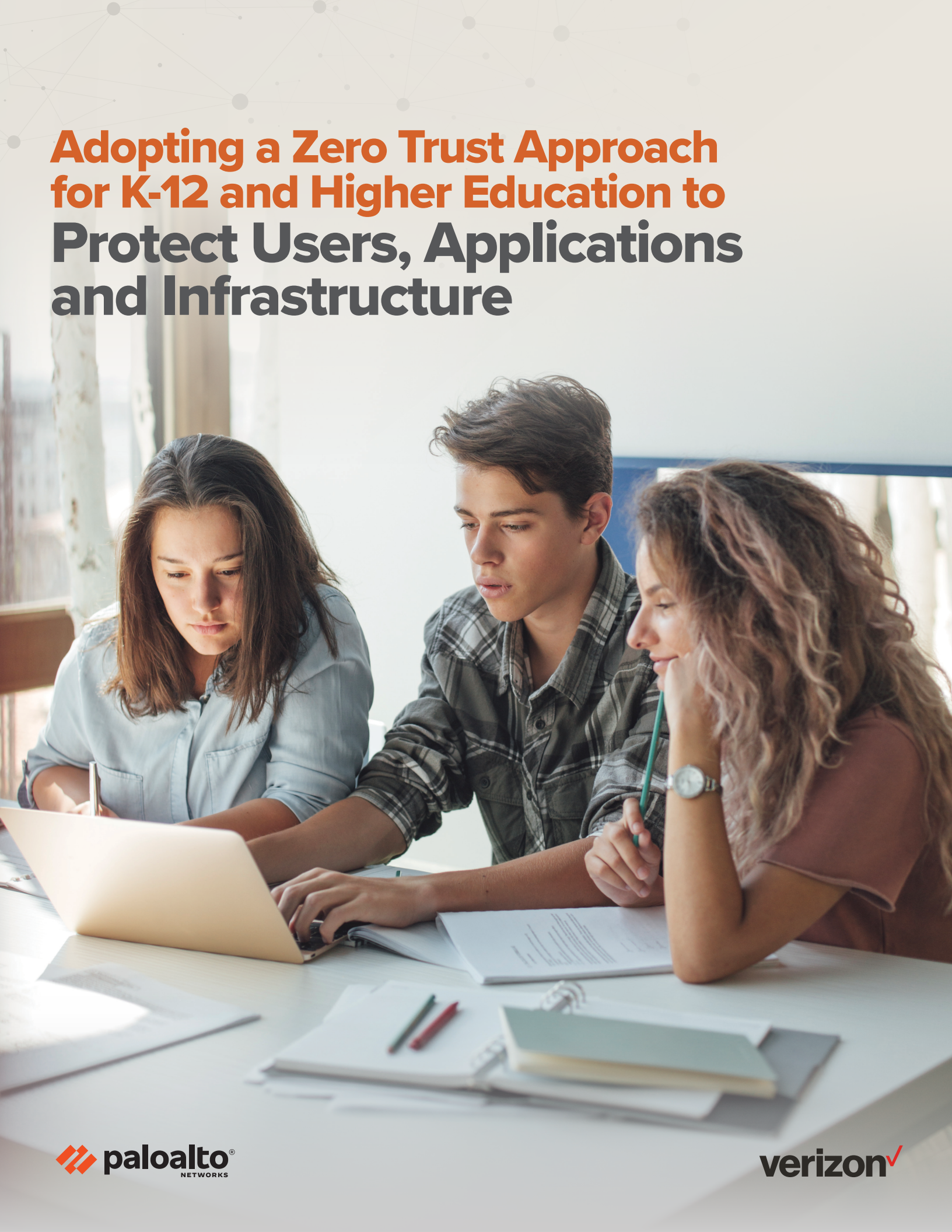
Adopting a Zero Trust Approach for K-12 and Higher Education to Protect Users, Applications and Infrastructure



paloalto NETWORKS

verizon

The past 18 months have likely changed K-12 and higher education permanently. Despite daunting challenges brought about by an unprecedented shift to remote learning, there were also silver linings. Sheer necessity spurred growth in virtual learning, new approaches to teaching, and greater technology proficiency among students and educators. At the same time, the federal government also approved new funding to build out network infrastructure that will help enable more innovative use of technology and more equitable access to broadband.

In the midst of this digital transformation, cybersecurity continues to be a top priority for school districts, community colleges and state universities. As education institutions digitize student information, adopt educational technology and conduct sensitive research online, they become more enticing targets for cybercriminals. According to the Cybersecurity and Infrastructure Security Agency (CISA), ransomware attacks on K-12 school systems have increased significantly since the start of the pandemic,[1] while ransomware attacks on colleges increased 100 percent between 2019 and 2020.[2]

At the same time, protecting users, data and resources has become increasingly complex. Traditional security approaches no longer fit emerging IT initiatives and cannot adequately scale to secure users, applications and infrastructure as organizations extend learning, administration and back-office processes beyond their physical campuses.

To maintain a strong security posture and minimize risk, proactive learning organizations must modernize their infrastructures to incorporate the principles of Zero Trust. This modern approach looks to eliminate implicit trust and leverages modern security tools and technologies to provide easy, scalable and consistent security regardless of where users, applications and infrastructure reside.

Protecting the Digital Schoolhouse

K-12 and higher education institutions face the following challenges:

Digitization of valuable data. The largest annual increases ever in educational technology investments were in 2020

Traditional security approaches no longer fit emerging IT initiatives and cannot adequately scale to secure users, applications and infrastructure as organizations extend learning, administration and back-office processes beyond their physical campuses.

and 2021 in higher education.[3] These technologies are often cloud-based and can expand the threat surface. In addition, Personally Identifiable Information (PII) in student information systems, student health records and other sources can be very lucrative for cybercriminals, fetching, on average, $250 per record.[4]

Accelerated adoption of remote/hybrid learning. To accommodate student and parental demand, 20 percent of K-12 districts have adopted, plan to adopt or are considering online instruction post-pandemic.[5] In higher education, 77 percent of chief online officers expect a major acceleration in online learning.[6]

Remote/hybrid workforces. On-campus and remote administrative staff need to move flexibly and securely on and off the campus network. Without consistent and comprehensive end-to-end security controls, these workers can be inadvertent vectors for attack. Forty-two percent of schools have students or staff that circumvent cybersecurity protections, and 41 percent of recent higher education cybersecurity incidents were caused by social engineering attacks such as phishing.[7]

Constantly evolving threat landscape. With thousands of new phishing attacks with malicious website addresses created daily, traditional Uniform Resource Locator (URL) filtering databases are unable to keep up. Additionally, cybercriminals increasingly attack the Domain Name System (DNS) infrastructure to infiltrate networks, steal data, hijack websites and spread malware. Eighty percent of malware exploits DNS infrastructure to execute attacks,[8] yet most web security solutions do not protect against DNS-layer threats.

Zero Trust for Identity-Based Access Control

Zero Trust is a strategic approach that helps K-12 and higher education organizations prevent successful data breaches. Rooted in the principle of "never trust, always verify," Zero Trust is designed to protect modern digital environments by leveraging network segmentation, preventing lateral movement, providing threat prevention and simplifying granular user-access control by leveraging information derived from Identity, Credential and Access Management (ICAM) systems.

Zero Trust strategically aims to minimize the risk of breaches by consistently verifying all users, devices, applications and data based on context and user activity. Zero Trust Network Access (ZTNA) extends this strategy to provide remote access to applications and services based on defined access control

Achieving Zero Trust is often perceived as costly and complex. However, Zero Trust can easily be built upon existing infrastructure and often with existing technology.

policies that combine role-based, granular, encrypted access controls with post-connect threat monitoring. This approach further extends the concept of Zero Trust by enabling both on-premises and remote educators, students and administrative staff to interact securely with both enterprise applications and internet-based or Software-as-a-Service (SaaS) applications.

Achieving Zero Trust is often perceived as costly and complex. However, Zero Trust can easily be built upon existing infrastructure and often with existing technology. As educational institutions identify opportunities to incorporate the principles of Zero Trust, it is important to understand there are no Zero Trust products. Rather, Zero Trust is an integral part of a modern cybersecurity architectural approach that enables complete end-to-end visibility and rich policy-based controls to mitigate even the most sophisticated threats. Leading cybersecurity solution providers now incorporate the tenets of Zero Trust into comprehensive, end-to-end platform architectures to address even more use cases. This approach offers K-12 and higher educational organizations several advantages, including:

- **Providing context-based access** that encompasses all users, all devices, all applications and all workloads. Context-based access includes verifying each user's identity and privileges as well as the integrity and risk profile of their device and the applications or resources they're attempting to access. Based on these attributes, access is granted or denied. This capability requires technology that enables education institutions to centrally authenticate and authorize users from a single point, regardless of where their user identity stores are located (e.g., on premises, in the cloud or in a hybrid scenario). It also requires an integrated Cloud Access Security Broker (CASB) so students, educators and administrators can securely access SaaS applications and other resources that exist outside the organization's firewall.

- **Providing uncompromising security** by continuously examining all content to prevent both known and unknown malicious activity in real time. This capability requires traditional website crawling technology as well as advanced URL filtering. Advanced URL filtering

uses inline machine learning to examine actual website content and detect and deflect previously unknown attacks (i.e., zero day attacks). Expanded DNS security capabilities that help detect websites that have been hijacked or otherwise compromised by cybercriminals also provides safer access for students, educators and administrative staff.

Enabling global and consistent access security everywhere regardless of the location of a user, device or application. The technology required for this capability includes physical, virtual Next-Generation Firewalls (NGFW) and cloud-native NGFWs that leverage artificial intelligence and machine learning to enable context-based access on premises, in the cloud, in remote work environments or across campuses. It also requires an open, programmable and highly scalable platform that can automatically shape bandwidth, prioritize network traffic and allocate resources as needed to ensure security functions are highly available and optimized for performance. Additionally, a Zero Trust model that emphasizes the adherence to the principles of Zero Trust Network Access (ZTNA) for applications, can also be achieved with a Secure Access Service Edge (SASE) platform. SASE solutions represent a convergence of secure network transport with a cloud-native security stack that includes, but is not limited to, the following core components: ZTNA, CASB, Secure Web Gateway, Firewall-as-a-Service (FWaaS) and Software Defined Wide Area Network (SD-WAN).

Seizing the Moment

As education institutions transform to meet the needs of today's digital virtual learning environment and prepare for the schools of tomorrow, Zero Trust will become an important strategy to protect users and resources in the extended learning environment. With federal stimulus funding supplementing many IT and cybersecurity budgets, now is an ideal time to invest in Zero Trust security solutions that enable students, educators and administrative staff to engage more securely regardless of where they — or the resources they use — are located.

Enabling Secure Access to High-Value Content Across Multiple Campuses

When a major higher education institution needed to protect its networks, cloud applications and high-value data against massive malware and DNS-based attacks, it implemented a Zero Trust solution to deliver virtual next-generation firewall (NGFW) protection across its main campus and 23 satellite campuses. Each virtual NGFW delivers cloud-based threat prevention, advanced URL filtering, secure remote user identity and access control, and consolidated network security management. Using the solution, this institution is well-positioned to strongly and efficiently protect $25 million per year of U.S. defense research intellectual property (IP); high-value research and engineering data; cloud applications used for budgeting, procurement and other administrative functions; and more than 100,000 end users.

This paper was written and produced by the Center for Digital Education Content Studio, with information and input from Palo Alto Networks and Verizon.

1. *Government Technology. CISA and NCSA Advise K-12 on Future Cybersecurity Threats. March 2021.*
2. *Blue Voyant. State of Education 2021 Report. https://www.bluevoyant.com/resources/cybersecurity-in-higher-education/*
3. *Quality Matters and Eduventures® Research. 2021. https://www.qualitymatters.org/qa-resources/resource-center/articles-resources/CHLOE-project*
4. *IBM/Ponemon Institute. Cost of a Data Breach Report 2020. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/*
5. *Rand Corporation. https://www.rand.org/pubs/research_reports/RRA956-1.html*
6. *Quality Matters and Eduventures® Research. 2021. https://www.qualitymatters.org/qa-resources/resource-center/articles-resources/CHLOE-project*
7. *Impact. 15 Cybersecurity in Education Stats You Should Know. https://www.impactmybiz.com/blog/cybersecurity-in-education-stats/*
8. *Palo Alto Networks. Stop Attackers from Using DNS Against You. Accessed August 2021. https://www.paloaltonetworks.com/resources/whitepapers/stop-attackers-from-using-dns-against-you*

Produced by:

CENTER FOR DIGITAL EDUCATION

The Center for Digital Education is a national research and advisory institute specializing in K-12 and higher education technology trends, policy and funding. The Center provides education and industry leaders with decision support and actionable insight to help effectively incorporate new technologies in the 21st century.
www.centerdigitaled.com

For:

paloalto® NETWORKS

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting thousands of government and education organizations across their clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before, and we are passionate about protecting the services, systems, and data that drive government. For more information, visit paloaltonetworks.com or our State & Local Government page **paloaltonetworks.com/security-for/government/government-state-local.**

verizon

Verizon Communications Inc. (NYSE, Nasdaq: VZ) was formed on June 30, 2000 and is one of the world's leading providers of technology, communications, information and entertainment products and services. Headquartered in New York City and with a presence around the world, Verizon generated revenues of $128.3 billion in 2020. The company offers data, video and voice services and solutions on its award-winning networks and platforms, delivering on customers' demand for mobility, reliable network connectivity, security and control.
www.verizon.com/business/solutions/public-sector/state-local-government

IMAGES PROVIDED BY SHUTTERSTOCK.COM