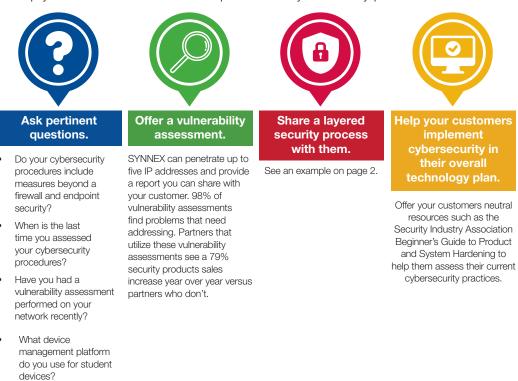# SYNNEX
GOVSolv™
EDUCATION

Cybersecurity Opportunities in Education

- According to the K-12 Cybersecurity Resource Center, U.S. public schools have experienced nearly 400 cybersecurity-related incidents since 2016, and with higher-education, the number rises.
- In 2017, K-12 and higher-education institutions reported 455 cybersecurity incidents, with 73 resulting in data disclosures. In fact, five major universities experienced data breaches larger than the Sony hack.

Help Your Customers Assess and Update Their Cybersecurity Practice

Both K-12 and higher-education institutions continue to struggle with securing their networks and devices as they implement more technology across campuses. Firewalls and endpoint security were typically the main cybersecurity items, but as data breaches and hacks continue to increase, these items simply aren't enough. Cybersecurity must be an ongoing process that is continually analyzed. Here's how to help your customers assess and update their cybersecurity practice.

Ask pertinent questions.

- Do your cybersecurity procedures include measures beyond a firewall and endpoint security?
- When is the last time you assessed your cybersecurity procedures?
- Have you had a vulnerability assessment performed on your network recently?
- What device management platform do you use for student devices?

Offer a vulnerability assessment.

SYNNEX can penetrate up to five IP addresses and provide a report you can share with your customer. 98% of vulnerability assessments find problems that need addressing. Partners that utilize these vulnerability assessments see a 79% security products sales increase year over year versus partners who don't.

Share a layered security process with them.

See an example on page 2.

Help your customers implement cybersecurity in their overall technology plan.

Offer your customers neutral resources such as the Security Industry Association Beginner's Guide to Product and System Hardening to help them assess their current cybersecurity practices.

The SYNNEX Difference

Our experienced team of subject matter experts provide the support you need to deliver comprehensive IT security solutions to your education customers.

- **Assessments:** We offer assessment services that help position you as a trusted advisor. Services include security assessments, complimentary vulnerability scans, penetration testing, risk analyses, and more.

- **Pre- and post-sale support:** We offer a wide range of pre-sales and post-sales support services, including pre-sales engineering, demos, implementation, ongoing technical support, and more.

- **Training:** We support you with ongoing technical training. Services include vendor-agnostic market overviews and vendor-specific product overviews for IT security. We also offer significant discounts on vendor and industry certification courses and exams.

Need help? Ready to get started?

For education-related questions, email education@synnex.com.

For vendor- and technical-specific questions, email cybersecurity@synnex.com.

SYNNEX
CORPORATION

SYNNEX
GOVSolv™
EDUCATION

Layer 1 – Network Security

Next-Gen Network Security. In addition to firewalls, consider granular packet inspection, application control, and intrusion prevention for more effective first-line defense.

Barracuda	Check Point	f5 Networks	FireEye	ForeScout	Fortinet
HPE	Juniper	Palo Alto	Symantec	WatchGuard	

Endpoint Security. Relying on machine-based learning, code-based scanning, security analytics, and advanced antivirus technology can help secure client systems.

Absolute	Avast	Check Point	Cylance	FileWave	FireEye	Fortinet
Guidance	Malwarebytes	Palo Alto	PC Matic	Symantec	Vipre	Webroot

Layer 2 – Device Security and Management

Web Security. Prevent attacks from the web by limiting employees' access to websites, blocking/allowing traffic based on URL category, or matching traffic based on URL category for policy enforcement.

Barracuda	Blocksi	Check Point	f5 Networks	FireEye	Fortinet
Palo Alto	PacketViper	Symantec	WatchGuard	Webroot	

Email Security. Layered defense against unwanted malware, antispam, and ransomware for web and email platforms.

Barracuda	Check Point	Cisco	Cofense	FireEye	Fortinet
Mimecast	Symantec	WatchGuard	Webroot		

Classroom Management Platforms. Manage devices at the district or classroom level by monitoring student activity, screen time, and potential threats. Applications also allow for device settings such as lock-out times, age-restricted filtering and email platforms.

Actiontec Classroom Commander	Chrome Education License	Blocksi	GoGuardian	HP Classroom Manager
Microsoft Intune				

Identity and Access Management. Safeguard devices and personally identifiable information with solutions such as multi-factor authentication and credential mapping.

Authen2cate	BeyondTrust	Check Point	CyberIoQ	f5 Networks
Fortinet	Gemalto	HID	Symantec	WatchGuard

Layer 3 – Data Security

Data Security. With federal and state policies related to securing student data, these solutions can encrypt and set boundaries for this sensitive information.

Check Point	Fortinet	Gemalto	Imperva	Micro Focus	SecurityFirst
Symantec	WatchGuard				

Secure Backup and Disaster Recovery. Source a wide range of solutions to back up data and ensure continuity of institution

Barracuda	Carbonite	Commvault	Dropbox	StorageCraft

SYNNEX
CORPORATION