DELL EMC

K-12 Security Whitepaper

www.dellemc.com/k12

Technology dependence

School districts are increasingly relying on digital technologies to facilitate the shift to a more student-centered learning model

Security risks

As technology usage increase so do security threats and risks to district networks and the personal data of students, teachers and administrators

Cybersecurit solutions

The Dell EMC security team can help you determine the best fit of any product and make the most effective and economical choice from the many available options

A proven, streamlined approach to securing systems and infrastructures in K–12 education

Digital intrusions, malware, ransomware and the risks of living in a connected world have come to K–12 education and are becoming more threatening as school districts make greater use of advanced technology. IT departments can be challenged by the complexities and urgencies of securing K–12 learning environments. However, a Cybersecurity Framework created by the National Institute of Standards and Technology (NIST) can help organize and simplify their security planning and implement the right measures.

Growing security risks as learning becomes more digital

School districts are increasingly relying on digital technologies to facilitate the shift to a more student-centered learning model. Giving students mobile computers to access a wealth of digital and online resources can help teachers tailor learning to each student's talents and challenges, and empowers students to lead their own learning. Technology also helps students and teachers collaborate with their peers, teachers and outside experts around the world to exchange ideas, experiences and insights.

As a result, school districts are managing a rapidly increasing number and variety of laptops, tablets and desktop computers to give students and teachers access to the digital resources they need to support teaching and learning.

At the same time, security threats and risks to district networks and the personal data of students, teachers and administrators have accompanied the proliferation of connected learning devices and applications. Data theft, digital intrusions, denial-of-service attacks, malware and ransomware have become more common and threatening as technologies used in learning and teaching have evolved. From a security perspective, every internet-connected device and online application or service for collaboration and file exchanges are vulnerable to attacks that specifically target educational environments. These compound the risks a user may be exposed to by simply visiting websites or sending and receiving messages and files.

Without a proactive strategy to address these security risks and maintain the integrity of your learning environment, you may be responding to incidents and threats after they happened, but you may not be able to forestall emerging cybersecurity liabilities. Over time, the gap between your security measures and evolving threats and risks may widen.

The ongoing wave of advancements in educational technology may increase your risk exposure even if you follow a well-planned approach to addressing today's security challenges. For example, some technology savvy students might under certain circumstances become hackers who pose a threat to data sources and school networks.

Applications for immersive technologies, including augmented and virtual reality, are slowly penetrating K–12 education, augmenting the potential vulnerabilities of your applications and networks. Increased sophistication in educational technologies may offer more opportunities for digital attackers, especially when innovations offering advanced, ground-breaking functionality come with comparatively weak security features, as is sometimes the case.

The ongoing wave of advancements in educational technology may increase your risk exposure even if you follow a well-planned approach to addressing today's security challenges.

Threats can be external or internal

As in the commercial realm, digital threat actors may be criminals who aim to profit by stealing personal and financial data or who want to sabotage school district operations by disrupting applications or networks. They could also be frustrated or disgruntled employees. In your school district, they might also be current or former students who want to challenge systems without wanting to damage them, or who are indeed malicious.

What is often overlooked is the security risk from people who have no malicious intent whatsoever—administrators, teachers, parents or outside groups using school facilities. These individuals may not catch phishing attempts through email or the more sophisticated social-engineering practices that have digital intruders pose as helpdesk workers or IT contractors to glean confidential information. In a frequent scenario, they may insert a USB drive they found outside of a school facility. What's more, students and teachers alike may not know the best practices for secure conduct online when they exchange files or use mobile apps.

The challenge of practicing systemic risk management

As an IT manager or technology planners in K–12 education, you have many opportunities to learn about the issues, risk-mitigation approaches and solutions for digital security. What's much harder is finding the time and resources to create a comprehensive security practice that helps you address the risks your school district experiences today and safeguard data and systems against newly emerging threats.

As a result, a key area of digital security such as user authentication and provisioning can become a patchwork of access, identification and software distribution measures and practices that may not work well together and, as a result, increase and complicate IT management workloads.

Regulatory compliance augments IT complexities

Compliance adds to the complexity of managing data and application security in K–12 education. Almost all states have introduced at least one student-data privacy bill, and many have enacted new student- privacy laws, requiring school districts to implement sound protection of student data. Several regulatory mandates already enforce secure management of student records—for example:

The Children's Internet Protection Act requires schools and libraries that receive federal funding to implement filtering systems to block specified websites.

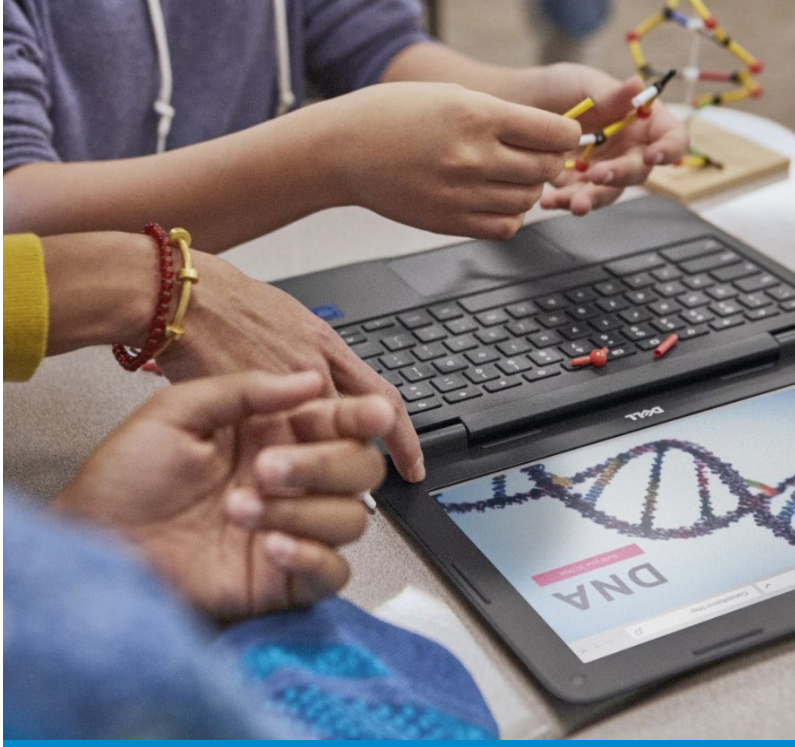
The Family Educational Rights and Privacy Act protects the privacy and right of access to students' educational records.

The Health Insurance Portability and Accountability Act demands security measures for personally identifiable medical information, which is often maintained by school districts for their students.

A complete framework for planning and implementing digital security

Given the complexity of digital security risks and challenges, the tasks of safeguarding data and systems may look overwhelming and endless to K–12 IT departments, which are often short on funding and resources. Training and awareness building for students, staff and teachers will mitigate some risks, but additional measures are needed to address the many possible liabilities. K–12 IT managers need to develop and implement comprehensive security strategies that respond to the specific security concerns in their district. This effort can become more manageable when it is structured by a comprehensive, practical framework that incorporates best practices and proven security expertise.

One such tool you can easily access and use practically was developed by the National Institute of Standards and Technology (NIST), an entity within the U.S. Department of Commerce. The NIST Cybersecurity Framework is designed to help organizations protect critical infrastructures. It was the outcome of a year-long collaboration between security and technology experts from academia, government and industry. First published in 2014, the NIST framework has evolved through multiple updates. The framework's risk-management approach is designed for organizations of all types and sizes. It comes with its own learning tools and offers a roadmap that can help you address the ongoing problem of escalating digital threats as technology evolves. The NIST Cybersecurity Framework has been adopted by a range of entities in state and local government and is recommended for adoption in K–12 education.



The NIST framework follows a repeatable, prioritized approach in providing standards, practices and guidelines to mitigate digital security risks and ensure compliance with governing regulations. Key to understanding and using it are five concurrent and continuous functions that serve as organizing principles for planning and implementing cybersecurity measures:

Identify: Organizations identify their digital assets, risks, vulnerabilities, security policies and risk management strategy.

Protect: Realize data security by means of identity and access management, protective technology and processes, maintenance and staff training.

Detect: Using detection tools and continuous monitoring, organizations become aware of the risks and potential damages caused by anomalous activities and events.

Respond: In a well-planned response, an organization manages the analysis, mitigation, process improvements and communications that help address digital security threats.

Recover: Following an incident, data and systems are restored to their desired state, and ongoing security planning boosts the resilience of systems and processes in case of a future threat.

Powerful, comprehensive, digital security for K–12 environments

When you define your approach to digital K–12 security based on the NIST framework, you can follow your organization's practices for project management and solution selection. Often, it makes sense to prioritize which risks and threats to address based on a school district's experience and documented vulnerabilities. If you address today the most dangerous risks and eliminate the most threatening vulnerabilities, you can likely implement a sound level of protection that you can refine as the learning environments and security liabilities change. The payoff in shoring up your applications and systems against any possible risk and vulnerability may be relatively small.

In selecting technology solutions to implement security measures, many school districts prefer mature, proven offerings from a single vendor instead of disparate products from multiple suppliers and the likely resulting integration and management challenges. Dell EMC, Dell Technologies and their strategically aligned businesses maintain a security research, development and innovation practice that offers a full spectrum of solutions to support the five pillars of the NIST framework.

Table 1 provides an overview of the most important cybersecurity products from Dell EMC and Dell Technologies and how they align with the NIST framework pillars. The solutions listed operate across K–12 networks and the devices used by students, teachers and administrators. By using a portion of these tools in a calibrated response to your school district's cybersecurity challenges, you can provide a complete security solution that fits smoothly into existing technology infrastructures. The Dell EMC security team can help you determine the best fit of any product and make the most effective and economical choice from the many available options. dolorrum consectia velitis andigenducid ut es doluptatem sim faccus dundem rem.

Table 1 - How security solutions from Dell EMC, Dell Technologies and Dell EMC partners align with the NIST Cybersecurity Framework

Dell Technologies Security Transformation		Products	Identify	Protect	Detect	Respond	Recover
Secure modern infrastructure - Secure systems - Endpoint protection - User access control - Network protection	1	Dell Endpoint Security Suite Enterprise is a comprehensive endpoint security suite that stops evolving attacks, simplifies endpoint security and exceeds regulatory compliance standards.		✓		✓	
	2	Dell Encryption Enterprise offers flexible, platform-agnostic encryption of data at rest granular policies and compliance reporting.		✓			
	3	Dell Data Guardian enables IT managers to protect, control and monitor data wherever it goes. The solution secures data in-motion and in-use with encryption and Enterprise Digital Rights Management (EDRM) practices.		✓		✓	
	4	Absolute safeguards students' devices and data through a persistent connection that enables IT managers to mitigate risks and apply remote security measures. Absolute also offers theft investigation services and aligns with the standards of the Safe Schools program.	✓	✓	✓	✓	✓
	5	Mozy delivers enterprise-class, cloud-based, secure backup, automatic sync and seamless recovery of data.					✓
	6	Dell EMC Cyber Recovery provides fast and complete recovery from malware and ransomware attacks, supports recovery planning and enables the isolation of environments to perform security measures.	✓	✓	✓	✓	✓
	7	RSA NetWitness Platform enables IT managers to rapidly detect and respond to any threat—on devices, in the cloud or across virtual enterprises.		✓	✓	✓	✓
	8	RSA SecureID Suite makes it possible to provide users with convenient, secure access to any application—from the cloud to the ground—from any device.		✓			
	9	VMware Workspace One is a digital workspace platform that delivers and manages any app on any device by integrating access control, application management and multi-platform endpoint management.	✓	✓	✓		
	10	VMware NSX Data Center is a network virtualization platform for the software-defined data centers. It delivers networking and security entirely through software, abstracted from the underlying physical infrastructure.	✓	✓			✓
	11	VMware AppDefense is a data-center endpoint security tool that protects applications running in virtualized environments. It registers changes to an application's typical and intended state and behavior and automatically responds to threats.	✓	✓	✓	✓	✓
	12	SonicWall offers a portfolio of devices that enable network firewalls, content control, unified threat management, spam prevention, virtual private networking and more. The company's solutions and services enable real-time breach detection and prevention, and help companies realize regulatory compliance.	✓	✓	✓	✓	✓
	13	Dell EMC Video Surveillance solutions enable comprehensive physical security for facilities and infrastructures of any size and complexity.		✓			
Advanced operations - Converged visibility - Threat intelligence and advanced analytics - Rapid response and remediation	7	RSA NetWitness Platform enables IT managers to rapidly detect and respond to any threat—on devices, in the cloud or across virtual enterprises.		✓	✓	✓	✓
	14	SecureWorks delivers managed security, security and risk consulting, incidence response and cloud security, all driven by threat intelligence.	✓	✓	✓	✓	✓
Unified risk management - Risk identification - Risk contextualization - Risk management	15	RSA Archer Suite enables proactive risk response with data-driven insights and a streamlined, short time-to-value approach.	✓	✓	✓	✓	✓
	16	RSA Risk and Compliance Services offers a single, integrated resource for security consulting and solution delivery to mitigate risk, ensure compliance and ensure the integrity of school districts' educational mission.	✓	✓	✓	✓	✓

Next steps and resources

To move forward with securing your K–12 learning environment, here are some actions you can take today:

- Contact your Dell EMC account representative or visit www.dellemc.com/k12
- See how Dell Technologies envisions security transformation
- Take a look at some of our K–12 customer experiences and success stories:
  - Pembina Trails School Division strengthens device security
  - Fort Mills Schools takes advantage of Dell Technologies solutions to strengthen data and IT security
  - Crosby ISD takes advantage of Dell EMC networking to enable effective teaching and digital learning
- The Consortium for School Networking (CoSN) provides guidance, assessment and planning tools through its Cybersecurity Initiative.
- The International Society for Technology in Education (ISTE) offers useful technology planning guidance and resources.
- The Readiness and Emergency Management for Schools Technical Assistance Center provides practical cybersecurity considerations for K-12 educational environments, including the NIST framework
- See how states, tribes and local jurisdictions work with the NIST framework.

---

[1] See www.coxblue.com/the-five-biggest-threats-to-k-12-network-security-for-the-2017-18-school-year/ or www.us.logicalis.com/news/logicalis-us-ids-five-of-the-top-it-security-challenges-k12-cios-face-every-day/ for typical summaries of the security challenges in K–12 education.

[2] See https://foresite.com/school-district-prepared-protect-student-data/.

[3] See www.nist.gov/cyberframework/framework for background and practical guidance.

Copyright © 2018 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Intel, the Intel logo, Xeon, Xeon inside are trademarks and registered trademarks of Intel Corporation in the U.S. and/or other countries. Other trademarks may be trademarks of their respective owners. This whitepaper is for informational purposes only. The contents and positions mentioned in this document were accurate at the point of publication, April 2018. Dell and EMC make no warranties — express or implied — in this case study. Part Number: XXXXXX

DELL EMC