DELL EMC

Higher Education Security Whitepaper

www.dellemc.com/hied

Campus cybersecurity threats

With practically every student and faculty member using one or several mobile devices to access information and software applications, many entry points for a potential cyberattack are presented, in addition to the servers and stationary devices in an institution's data center and networks.

Other potential risks include:

- Gaming consoles used by students
- Poorly secured mobile devices
- Wearable devices
- AR and VR devices

Cybersecurity in higher education: a systemic, sustainable approach

Cybersecurity in higher education is a challenge of increasing complexity and dramatic consequence. The stakes are high as threat actors launch sophisticated attacks to steal information or disrupt operations. Cyber espionage is particularly prominent in higher education, which experiences threats and attacks comparable to or greater than those in commercial industry. IT departments may not be sufficiently resourced and funded to keep up with digital threats and often lack a comprehensive approach to ensuring optimal security. The Cybersecurity Framework created by the National Institute of Standards and Technology, already in use in some higher-education institutions, can help IT security managers plan for and realize strong network and data security to make the most effective use of their resources.

Shifting security risks as digital technology advances higher education

The complex business and educational operations of universities and colleges connect directly to digital and physical security concerns and vulnerabilities. Like a business enterprise, these institutions manage people, finances and facilities. The number of employees may reach into the thousands, ranging from academic faculty and researchers to groundskeepers and janitors. Finance management may include donors and complex funding approaches not common in businesses. Facilities can sprawl across multiple campuses with buildings of varying ages built for educational purposes or to support scientific research. These employees and resources are served and managed by a wide range of applications and data stores on the networks of educational institutions, which present many potential attack points for digital malfeasance.

However, there is also the frequently large population of students that use network resources and applications as they participate in educational programs or research projects that involve sensitive data and intellectual property. Generally using a variety of devices of their own, students represent additional challenges that need to be considered in an institution's security planning. When they live in campus housing, they may be using network resources for their studies and for personal pursuits such as gaming, social media or creative endeavors, adding to the breadth of scenarios that need to be included in cybersecurity.

The complex business and educational operations of universities and colleges connect directly to digital and physical security concerns and vulnerabilities.

Technological innovation and complexity present many potential attack routes

For malicious actors looking to steal valuable data and disrupt networks, higher education is fertile ground. Fast growth and disparate technologies have, in many institutions, resulted in security practices that can barely keep up with day-to-day operations, let alone stay ahead of sophisticated cybersecurity attacks and exploits. With practically every student and faculty member using one or several mobile devices to access information and software applications, many entry points for a potential cyberattack are presented, in addition to the servers and stationary devices in an institution's data center and networks. Wearable devices, often used by faculty, administration and staff for fitness and health monitoring, present another vulnerability. So, do gaming consoles used by students, which are typically not managed and secured on a university network and offer potential access to a person's identity and account details.

Poorly secured mobile devices are one of the risks to cybersecurity in higher education frequently mentioned by experts, but there are many others. They include weaknesses in the security of cloud infrastructures, gaps in data governance, and risky, inconsistent practices in identity and access management and user provisioning. Some digital attackers focus on the educational systems used by many colleges and universities to manage students, employees and programs, or they acquire specialized skills in hacking the enterprise resource planning (ERP) systems used to run operations.

Learning and instruction in higher education benefit from the best of technological innovation and creativity. Students use their institution's digital labs and workstations in data-rich, digitally enabled projects and programs to learn about such disciplines as engineering, geoscience, architecture, medicine, economic modeling and social studies. They learn in classrooms, but also individually—anywhere and anytime. They collaborate in maker spaces. Often, they engage in projects with their peers on other campuses anywhere in the world. In addition to higher-education networks, applications and resources for learning and collaboration, the intellectual property associated with research are often available around the clock and from any location through private, public and hybrid cloud infrastructures. All these resources and activities offer attackers many vulnerabilities and access points to steal personal or research-related data or to interfere with processes and operations. At the same time, awareness of cybersecurity concerns in students is generally low, and user education efforts are often rudimentary. [4]

Security risks in digitally extended reality

In recent years, augmented reality (AR) and virtual reality (VR) have become increasingly prominent in higher education. Students and instructors have incorporated AR and VR into the learning environment, for instance, to facilitate anatomic study, enable realistic intercampus collaborations, develop graphical media and animation, deliver distance learning and bring data models to life. These technologies present their own set of digital risks in addition to ones already mentioned. Attackers may use AR and VR devices to gain access to collaboration tools and data stores and steal information or plant ransomware and other malicious code in an institution's network. When students use their personal head-mounted displays and similar AR and VR devices, they may inadvertently bypass common authentication mechanisms and create an opportunity to exploit a vulnerability.

Many AR and VR systems make attacks easier because they lack encryption for network connections, which are common in communications and learning applications. Unauthorized users can copy or duplicate somebody's avatar and use it to penetrate systems. The sensors, cameras and microphones in AR and VR can also provide opportunities to access paths into network resources that should be private or protected, expose personal biometric data or disclose conversations.

Increasing complexities in realizing higher-ed cybersecurity

Today's cybercriminals and hackers targeting higher-education applications and systems are, for the most part, well-trained experts with an arsenal of sophisticated tools. Many of them are fully equipped to exploit innovative educational technologies and bypass resistance even from highly educated, tech-savvy users. As in the commercial realm, many digital threat actors in higher education will be criminals who hope to profit from the sale or exploitation of personal, financial and research data. Others may be ambitious hackers with an interest in navigating around security protocols and damaging applications and systems. They could also be current or former students, instructors or disgruntled employees whose personal agenda motivates them to attack an institution's systems. Finally, some threat actors see opportunity in penetrating an educational network and using it as a launchpad for malicious phishing schemes targeting other networks.

Chief information security officers (CISO) and managers in higher education also need to be aware of the security risk from people who have no malicious intent—students, administrators, staff and faculty from their own college or university, or visiting from other institutions. Visitors may also include vendors or members of the public attending events and programs. These individuals may not catch well-disguised email phishing attempts or spot the sophisticated social-engineering practices that digital intruders often use to pose as help-desk workers or IT contractors to glean confidential information.

Many times, curiosity and inattention override awareness and training when users insert a USB drive they may have found outside of a school facility or borrowed from another person. In addition, students and instructors may not know the best practices for secure conduct online when they exchange files or use mobile apps. To make their user communities more security conscious, IT departments in some universities are performing outreach and educational initiatives. These can be effective in the short term and yield even better results when they are part of a comprehensive security strategy.

Regulatory compliance augments security challenges

Higher education is subject to a staggering array of regulatory mandates that impact educational and business operations. Compliance frequently involves implementing data management, digital systems and IT processes as regulations enforce how information is stored, shared and protected. As regulatory frameworks evolve, and new ones come into existence, the standards for the protection of controlled unclassified information (CUI) have been redefined with additional requirements that are changing how universities and colleges need to manage and protect data related to contracts and grants issued by federal government agencies. Compliance has a direct impact on institutional research and, in turn, on the ability of an institution to attract faculty and students.

When it comes to regulatory compliance, information security officers and managers in higher education are at a disadvantage compared to cyberattackers and criminals, who don't need to comply with anything. Flawed compliance can result in financial penalties and the loss of contracts and funding. Achieving compliance demands significant investments of budgets and resources. Compliance-related risk management can augment the security of educational applications and IT infrastructures, but, unless it is tied to a comprehensive security strategy, it may expose exploitable vulnerabilities—especially in the protection and management of personal and financial information—that require additional budget and effort to address.

82% of the IT managers state that they require students to take cybersecurity training at least once a year, but only **35%** of the students confirm this.

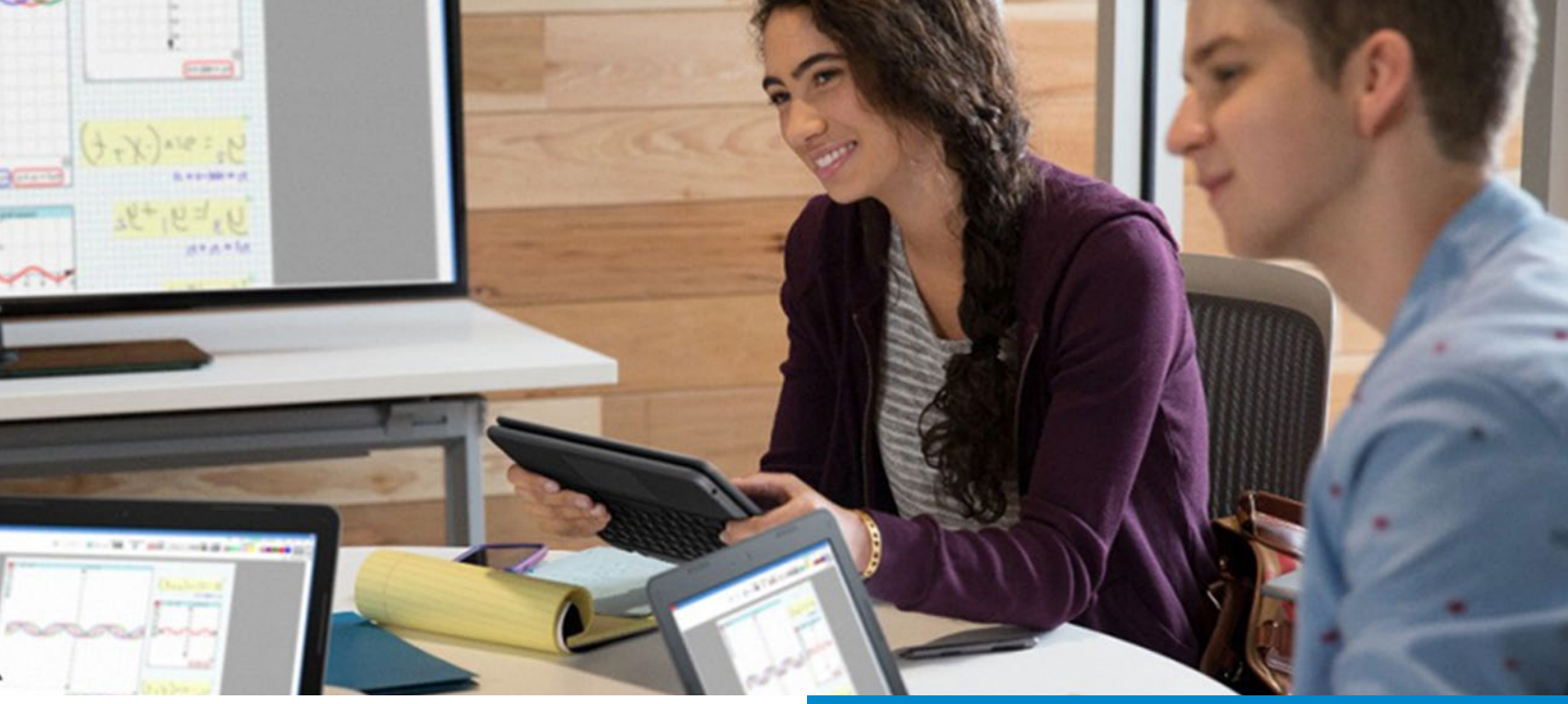
76% of the students reported engaging in high-risk behaviors

The challenge of practicing systemic risk and security management

The security and risk awareness of CIOs, CTOs and CISOs in higher education is generally high. They understand how increasingly sophisticated cyberattacks, and the criminals who initiate them, can damage an institution's ability to deliver educational programs and conduct research, both of which may include groundbreaking innovations. They know how institutional reputation and professional careers can suffer when data breaches or other security failures happen. At the same time, the confidence of some information security officers and managers in the effectiveness of their security efforts and educational programs is low. In a recent survey, less than half of the responding IT professionals indicated that their institutions follow common-sense, campus-wide security practices, and 76 percent of the students reported engaging in high-risk behaviors. There is also a disconnect between students and IT: 82 percent of the IT managers state that they require students to take cybersecurity training at least once a year, but only 35 percent of the students confirm this.

In many universities and colleges, budgeting and IT resourcing to insure digital security are insufficient to keep up with evolving and emerging threats. Often, budgets and resources for cybersecurity are not as well prioritized as enabling innovative or data-rich learning scenarios, leaving IT to make do with very little. IT departments become reactive to yesterday's and today's risks and security challenges, but they are unable to be proactive in securing their environments against the most advanced attacks. Key areas 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.

Given the never-ending surge of ever-more sophisticated threats and challenges to digital security, the tasks of safeguarding data and systems may look overwhelmingly complex to CIOs, CTOs and their teams. The effort of developing and implementing comprehensive security strategies that respond to institutions' specific security concerns can become more manageable and outcome-oriented when it is structured by a comprehensive, practical framework that incorporates best practices and proven security expertise.



A complete framework for planning and implementing digital security

The National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce, has developed one such comprehensive tool for realizing effective security in complex organizations. The NIST Cybersecurity Framework, which helps organizations protect critical infrastructures, 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. Its risk-management approach is designed for organizations of all types and sizes. It comes with its own learning and explorative resources and offers a roadmap that can help organizations address the ongoing problem of escalating digital threats as technology evolves. The NIST Cybersecurity Framework is in use in a broad range of agencies in state and local government and has been successfully adopted in higher education.

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

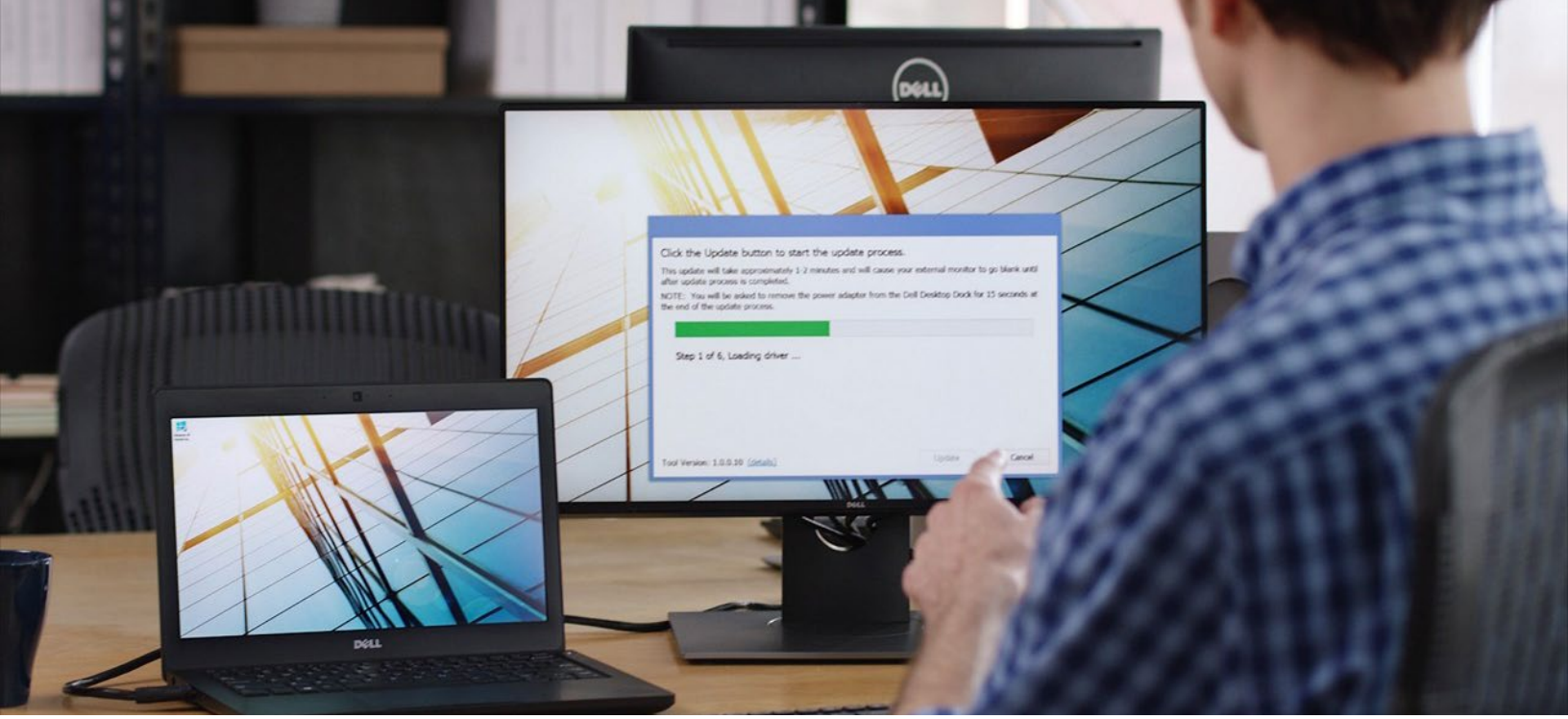
Identify: Organizations identify their digital assets, risks, vulnerabilities, security policies and risk management strategy.

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.



NIST framework cybersecurity success stories in higher education

The Biological Sciences Division (BSD) of the University of Chicago adopted the NIST Cybersecurity Framework across 23 departments, where more than 5,000 faculty and staff members are employed. Like many universities and colleges, the BSD needs to demonstrate compliance with multiple regulatory mandates and satisfy comprehensive cybersecurity requirements. Harmonizing cybersecurity expectations and goals among the 23 departments was a major part of the effort.

By using the NIST framework, the managers of the BSD cybersecurity program identified the security outcomes they wanted to accomplish for the entire division and enabled each department to define its own approach to achieving those outcomes. For the entire division, they prioritized security objectives and developed a roadmap that indicates the resources and activities needed to close security gaps.

Carnegie Mellon University (CMU) in Pittsburgh, Pennsylvania, is a target-rich environment at risk for cyberattacks and exploits. At CMU, 13,000 faculty and staff and close to 35,000 students work and study on five campuses. In addition to offering educational programs, CMU conducts research in various disciplines such as social science, health and life sciences, and engineering. Its complex network is optimized for large data transfers, and much of the information traveling on it is sensitive and valuable. Financial and administrative departments and processes also involve personal and proprietary data whose theft or inappropriate use could be devastating to individuals and the institution.

CMU information security managers began using the NIST framework as soon as its first version became public. They used the framework to plan and perform an inventory of all five campuses' data and system assets along with their potential risks. They documented past security events and threats and current practices for protecting data and systems. Then they prioritized assets and risks and designed CMU-wide asset and vulnerability management programs that are more robust, goal-driven and consistent than previous practices. These efforts will increase cybersecurity at CMU and make it easier for IT to manage and evolve it.

Powerful, comprehensive, cybersecurity for higher education

When CISOs and IT security managers define their approach to digital security in higher education based on the NIST framework, they can follow their organization's practices for project management and solution selection. Often, it's best to prioritize which risks and threats to address based on the institution's past record and the documented vulnerabilities to systems and the many data stores that could be attractive targets—including information related to scientific and other research, organizational finance and personal details.

By addressing the most dangerous risks and eliminating the most threatening vulnerabilities as soon as can be accomplished, security managers can likely implement a strong starting level of protection that they can refine and harden as individual and collaborative learning technologies and security liabilities change. No security solution, no matter how powerful, can protect a network from every possible attack or exploitation of vulnerability, and new threats are developed and launched every day. However, if CISOs take stock of their institution's history of security threats and breaches, they can identify, prioritize and address the most glaring vulnerabilities and risks.

In selecting technology solutions to implement security measures, many higher-education institutions prefer mature, proven offerings from a single vendor with educational expertise instead of disparate products from multiple suppliers, which can result in integration and management challenges. In its security practice, Dell EMC has for many years performed research and development, and engaged in partnerships and collaborations with other technology companies, to gain the ability to serve as such a single provider of security and data protection solutions for universities and other educational institutions.

At the same time, Dell EMC conducts ongoing research to optimize and deliver solutions that enable colleges and universities to pursue their mission and achieve the educational outcomes they seek. The educational and security technology disciplines at Dell EMC are fully aligned. Security, client, server, networking, storage and other solutions from Dell EMC are complementary and interoperable in higher-education environments. Dell EMC security and education experts work with educational institutions to help them plan and implement environments that are both highly secure and can facilitate effective, innovative teaching and research as well as studying.

Security and data protection solutions provided by Dell EMC support the five pillars of the NIST framework. Table 1 gives an overview of Dell EMC cybersecurity products and how they align with the NIST framework pillars. The solutions listed operate across higher-education networks and the devices used by students, faculty, staff and administrators. By using a subset of these tools in a calibrated response to your institution's cybersecurity challenges, you can provide a comprehensive security solution that fits smoothly into existing technology infrastructures. The Dell EMC education 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.

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.	✓	✓	✓	✓	✓

It's worth noting that many of the servers, client computers and other devices in the Dell EMC portfolio run on Intel processors and take advantage of their security features. Intel realizes that the traditional practice of using software tools to protect software applications cannot address the security and privacy threats directed at users and digital systems. Instead, it incorporates security capabilities directly into the processors that run computing devices. As you work within the NIST framework to neutralize potential cyberthreats and exploits and to achieve trusted computing, the security enablement delivered by Intel can help safeguard every layer of computing and network operations.

Next steps and resources

To move forward with securing your higher-ed learning environment, here are some actions you can take today:

- Contact your Dell EMC account representative or reach us through the Dell EMC higher-education page.
- See how Dell Technologies envisions security transformation.
- Learn more about Dell EMC solutions for higher education.
- Take a look at our higher-ed customer success stories.
- Take advantage of EDUCAUSE, a nonprofit organization that facilitates events and offers resources to increase the value of IT's contribution to higher education, including programs on cybersecurity and compliance.

[1] See https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

[2] See www.govtech.com/education/higher-ed/8-Cybersecurity-Challenges-Facing-Higher-Education.html

[3] See https://www.forbes.com/sites/forbestechcouncil/2017/08/21/what-cyberthreats-do-higher-education-institutions-face/#311f86f1640d

[4] See https://www.insidehighered.com/news/2017/11/22/university-gets-personal-its-students-about-cybersecurity for background and how one institution tried to address the problem.

[5] See https://er.educause.edu/articles/2018/5/securing-your-reality-addressing-security-and-privacy-in-virtual-and-augmented-reality-applications for a summary.

[6] See https://edtechmagazine.com/higher/article/2018/04/As-Hacking-Efforts-Mature-Higher-Education-Will-See-More-Sophisticated-Threats-

[7] See www.higheredcompliance.org/matrix/ for an overview.

[8] See https://www.archives.gov/cui/registry/policy-guidance.

[9] See https://mytechdecisions.com/network-security/infographic-cybersecurity-beliefs-higher-education-students-staff/

[10] See https://www.nist.gov/cyberframework/framework for background and practical guidance.

[11] See https://www.nist.gov/cyberframework/success-stories/university-chicago

[12] See https://resources.sei.cmu.edu/asset_files/Podcast/2015_016_100_446049.pdf