Safeguarding schools

COMPREHENSIVE SECURITY FOR EDUCATION

IMPLEMENTING A COMPREHENSIVE SECURITY STRATEGY

In this book:

Safeguarding technology in schools and beyond.

Today, digital devices are ubiquitous. And for schools, it's no different. From tablets in the classroom and bring-your-own-device policies to take-home programs for school-owned notebooks, digital resources are now an essential component in personalized learning. The implementation of cloud computing, too, adds another layer of complexity. These new technologies and programs are improving outcomes and helping students achieve their goals. However, new paradigms bring new risks. As schools modernize, and digital data increases, so does the potential vulnerability. Any place information is collected, stored, used, or transmitted can become a potential area of theft, loss, or attack.

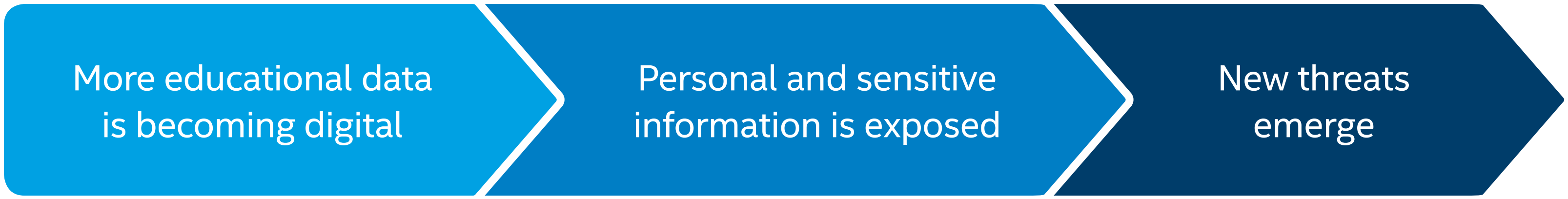
For educators, the potential consequences are great, particularly where children's privacy is concerned. The issue of safeguarding sensitive information therefore becomes critical.

IMPLEMENTING A COMPREHENSIVE SECURITY STRATEGY (CONT.)

Every school needs a comprehensive privacy and security strategy, and educators have a responsibility to ensure the security of data for both the students and the school. But with all these complexities, and scarce resources available to many districts, it can be difficult to implement these safeguards. Even with policies in place, there are no guarantees that students or educators will follow the security protocols required of them. It's no wonder some schools don't know where to begin.

Intel understands the importance of rigorous protection, and knows that the right combination of hardware and software can offer educators the security and privacy strategy their schools need.

This book will explore best practices for establishing a comprehensive security strategy for your educational organization.


More educational data is becoming digital

Personal and sensitive information is exposed

New threats emerge

In this book:

- Identity Management
- Data Protection
- Network Security
- Cloud Security and Data Ownership

DESIGNED FOR SECURITY

In this book:

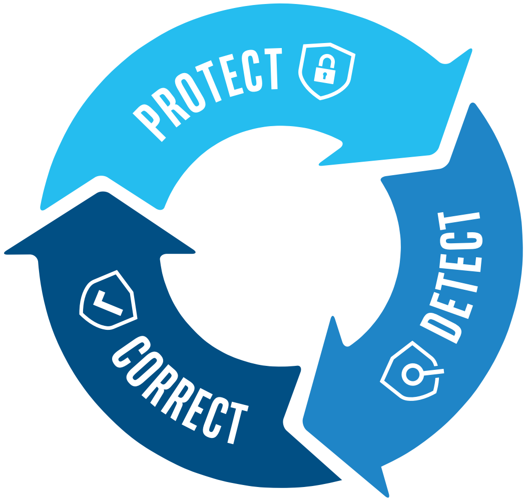
- Identity Management
- Data Protection
- Network Security
- Cloud Security and Data Ownership

Three key aspects of the threat-defense lifecycle.

1. Protect. Firewalls, virus software, data encryption, and identity management solutions keep attacks from occurring, and help avoid damage if a breach occurs.

2. Detect. Intrusion detection solutions proactively watch for signs of an attack, enabling a faster response to an impending or ongoing breach.

3. Correct. Rapid response to a breach is essential to mitigate damage. Solutions that automate the detection and response functions can decrease risk while reducing the burdens on busy IT staff.



IDENTITY MANAGEMENT

MORE DEVICES = MORE VULNERABILITY

As our lives become increasingly intertwined with and reliant upon digital information, we must take measures to secure our personal information. Social security numbers, addresses, driver's license numbers, financial history, and other personal data can all be used by thieves and hackers to falsify an individual's identity, steal money, or commit other crimes.

And when it comes to safeguarding the identities of minors, vigilance is imperative. K-12 school administrators and technology leaders have the unique responsibility of enacting policies that will maintain student and faculty privacy and security.

MORE DEVICES = MORE VULNERABILITY (CONT.)

With all this access that digital devices provide to email, social media, school grading systems and learning management systems, **any lapse in security can represent an opportunity for identity theft or system compromise.** This goes well beyond just school-owned technology—many students have their own phones and/or tablets, and these devices need to be secure too. Schools must implement BYOD controls and education programs for children. School leaders must also implement security controls that protect the institution's data and systems, as well as any device or system the student accesses in the course of their learning journey. And this must all be done in compliance with federal and state data governance laws, rules, and regulations.

In this book:

- **Identity Management**
- Data Protection
- Network Security
- Cloud Security and Data Ownership

87% OF PARENTS WORRY that their children's education e-records are at risk from hacking and data or device theft[1]

MORE DEVICES = MORE VULNERABILITY (CONT.)

The increasingly sophisticated efforts of hackers warrant a fresh look at modern protections to safeguard all data in the K-12 setting. As even big businesses have proven vulnerable to these attacks, schools must remain vigilant. School leadership and district CIOs must not only secure all student and employee credentials, but also continually assess their organization's risk posture and invest in reasonable and appropriate safeguards.

Even those schools that are currently exceeding compliance regulations must work to put clear policies in place, create student and teacher awareness, and deploy technology to protect against advanced attacks. This keeps educators ahead of the curve, and allows them to focus on their core mission of providing a safe education experience.

327

CYBER THREATS EACH MINUTE

means approximately 5 per second[2]

BREACHES TAKE MANY FORMS

PHISHING AND ACCESS

Users receive spoof emails that fool them into visiting malicious websites or downloading malware.

Example:
Denver public schools tricked by phishing scam

KEY LOGGING & RAM/SCREEN SCRAPING

Malware captures unencrypted keystrokes and reads screen buffers/memory.

Example:
Target breach compromises consumers' information

MAN IN THE MIDDLE (MITM)

A third party hijacks a user's logon session in order to capture credentials and data.

Example:
Yik Yak MITM hack (Give the dog a bone)

BRUTE FORCE

Personal information is used to falsify an individual's identity.

Example:
Hampshire school hack attack puts 20,000 at risk

STOLEN CREDENTIALS

Information is obtained through physical or electronic theft.

Example:
Hackers raid school coffers for $3M

SOLUTIONS THAT SIMPLIFY SECURITY

In this book:

Comprehensive tools ensure students' security and privacy.

Intel® Identity Protection Technology (Intel® IPT) is a suite of authentication and online access technologies designed to deliver web properties, users, and enterprises stronger, hardware-based security. Embedded into Intel's platforms for better ease of use, Intel® IPT also provides cost savings compared to traditional hardware or SMS authentication like key fobs.

With a multifactor authentication framework that allows teachers and students to log in easily to their cloud-based accounts, Intel® IPT also enables school districts to manage different authentication methods, including two-factor authentication with dynamic one-time password (OTP) tokens, display protection PIN entry protection with protected transaction display (PTD), and hardware-protected certificates with public key infrastructure (PKI).

Hardware-based **MULTI-FACETED** security offers comprehensive **IDENTITY PROTECTION.**

DATA PROTECTION

ENCRYPTION IS KEY

In this book:

Keeping private information private.

When most people think about securing personal information, they typically look at the kinds of information that could lead to identity theft: social security and credit card numbers, date of birth, bank records, and family names. But with so much of our information being moved into the digital domain, we have to redefine what we consider to be sensitive. Things like payroll information, medical records, family income statements, and health records must also be protected from exposure. Educators have a special mandate to extend this protection to their students and peers. This is an area of growing concern, as sensitive information is now routinely kept online in educational settings.

ENCRYPTION IS KEY (CONT.)

Today, it's not enough to lock down data in only one location. Any sound security strategy requires that data be protected anywhere there are potential vulnerabilities, and data encryption is required to protect classified or highly valued data assets. This means that school and district IT departments should be deploying managed data protection solutions while also actively managing their encryption policies.

Three important areas to consider for encryption.

- Protecting data at rest: on the hard drive of a student's laptop, on a district-owned server, or stored away in the cloud
- Protecting data in motion: moving across the network or through Wi-Fi between devices and locations
- Protecting data in process: actively filtering through the CPU which can at times be bogged down, and even require decryption before and re-encryption after the compute cycle

In this book:

FEWER THAN 1 IN 3 EDUCATORS

say they are very confident that they protect student data and privacy[3]

SOLUTIONS THAT SIMPLIFY SECURITY

Effective technologies can guard against these vulnerabilities, and ensure both strong encryption and good performance while the data is being processed. Intel's AES-NI (Advanced Encryption Standard New Instruction) is built into the actual processor, which allows for improved encryption of the data and accelerated processing speed for data that is already encrypted.

Found in Intel® Xeon® processor-based servers and Intel® Core™ processor-based PCs, AES-NI makes the benefits available on student devices as well as in the data center. **Intel® Secure Key plus AES-NI** ensures strong keys and powerful random number generation for optimal encryption of sensitive data.

SOLUTIONS THAT SIMPLIFY SECURITY (CONT.)

Intel® Data Protection Technology

Failure to properly ensure the security and privacy of student and school data can have devastating consequences for schools, from identity theft and financial losses to bad publicity.

Intel understands the variety of ways in which students access data in the education environment, and offers the kind of protection that keeps everything safe, everywhere, every time. World-class silicon security features offer end-to-end protection of sensitive data—from the student's device, through to the data center, and all the way into the cloud.

NETWORK SECURITY

PROTECTING DATA IN MOTION

In this book:

Today, education extends beyond the classroom, and data doesn’t stay in one place. We count on automatic downloads for updates and software patches, access to storage that’s hosted elsewhere, and a multitude of other benefits that rely on data moving over both known and unknown networks. But beyond offering convenience, this constant movement of data offers opportunities for cybercriminals to intercept it while it’s in motion. This kind of exposure has contributed to a drastic rise in the attention paid to network security in all sectors, particularly in education.

POTENTIAL DATA EXPOSURE

In the age of digital content, schools are reliant upon multiple compute environments for assessments, grading systems, learning management systems, and more. The technology in the classroom may be connected to a school or district data center, or to a public or private cloud. And in most cases, the district data center itself will be connected to the cloud. Today's learning environment also extends into the home, with personal Wi-Fi networks, internet providers, and everything else that comes between the home and school servers or the cloud services that students are accessing.

14.7 MILLION EDUCATIONAL RECORDS have been compromised since 2005[4]

SOLUTIONS THAT SIMPLIFY SECURITY

Strong encryption + network protection = solid security.

While data encryption is as important for the network as it is for personal computing devices and network servers, there are additional steps that can be taken to secure a network. The first is to create a secure VPN connection, leveraging client identity protection technology with hardened tokens.

While data encryption is as important for the network as it is for personal computing devices and network servers, there are additional steps that can be taken to secure a network. The first is to create a secure VPN connection, leveraging client identity protection technology with hardened tokens.

Available from multiple third-party vendors, this easy-to-install software is integrated with the latest Intel® vPro™ platforms. Combined with Intel® Identity Protection Technology, it provides hardware-level token security that schools need.

SOLUTIONS THAT SIMPLIFY SECURITY (CONT.)

The next step is addressing the network itself, with a security product that monitors the network, blocks malicious activity, prevents stealth attacks, and detects malware while it's in motion. It's also critical that all solutions be compatible with network capabilities. Whether it's 1GigE, 10GigE, or faster, network security should have the ability to scale with the speed of the data on the network. Intel has addressed these requirements, and offers solutions that work to close security holes and adapt to network topology.

The technology used in K-12 education delivery is growing at a remarkable rate. As school workloads become fully digitized, more sensitive data will pass across multiple networks, and new threat areas will arise. School CIOs must create modern security strategies that address network needs, including the additional connections made via mobile devices, laptops, and servers. A well-designed, comprehensive network security solution keeps data safe in a data-driven, cloud-based, mobile world.

In this book:

CLOUD SECURITY AND DATA OWNERSHIP

PROTECTING DATA WHILE AT HOME AND AWAY

In this book:

Cloud computing has revolutionized the way education is delivered. No longer is information confined to the school library—now an entire world of content is just a click away. Collaboration, instant assessments, analytics, and adaptive and individualized learning capabilities are all readily available to educators through the cloud. The ability to access these network and data assets through the cloud creates convenience, but it also establishes a greater need for privacy and security.

Steps to ensuring cloud security and privacy on-and off-premise.

A critical component of cloud security goes beyond the kinds of solutions that can be purchased and implemented, and it applies as much to the end user as it does to the IT staff: education around the proper implementation of online safety practices.

INTEGRATED SECURITY SOLUTIONS WORK TOGETHER to protect students, keep data safe, and combat cyberattacks.

PROTECTING DATA WHILE AT HOME AND AWAY (CONT.)

From an IT perspective, this means properly encrypting data, implementing a hybrid cloud environment that keeps the most sensitive information on-premise, and validating the SLAs of the cloud provider to ensure that they meet the school's security and privacy requirements. For students, faculty, and staff, ongoing training and awareness can instill a culture of security. With requirements for strong passwords, and guidance on identifying phishing emails and improving other security habits, schools can mitigate risks and greatly improve security.

- Have a solid cloud strategy that includes a hybrid cloud infrastructure, for control over what is on- or off-premise.
- Validate the SLAs with cloud providers to ensure that your requirements of data ownership and privacy are met.
- Ensure strong encryption of data.
- Use Intel® Xeon®-based servers with enabled security features (TXT, AES-NI) for data centers and cloud providers.

In this book:

SOLUTIONS THAT SIMPLIFY SECURITY

An important piece of this solution, however, is the underlying hardware, and the role it plays in the overall security and privacy environment. Many new security applications are designed to take advantage of the latest hardware security features, which means that **if your organization is still using old servers, you may not be seeing all the benefits of new security software.** It is a combination of software and hardware that optimizes security.

A solid, secure IT infrastructure with Intel® hardware and software together offers integrated protection, from servers to end-point devices.

Intel® Trusted Execution Technology, or TXT is a powerful security feature for protecting key assets. TXT ensures a trusted state—once you boot up a new VM in the cloud, TXT guarantees that it is uncompromised. This makes it possible to apply security policies to establish that certain workloads only run on these trusted server environments, or that they only be executed in certain secure locations. The latter is useful when policies dictate that certain types of data cannot be moved out of a specified region.

SOLUTIONS THAT SIMPLIFY SECURITY (CONT.)

With both public and private cloud environments, it's important to understand both the security software capabilities and the supporting hardware. There are a number of cloud providers who use Intel TXT for enhanced security, so it can be beneficial to find a provider that does.

Most schools are required to keep a minimum level of security in place, as mandated by regulatory compliance (this can vary by region, state, or country), but **with the right tools, schools can exceed the minimum regulations.** As the cloud continues to be utilized in education and other sectors, optimized security can help students and faculty remain safe online.

ADVANCED THREAT INTELLIGENCE

Faster identification of unknown threats in the cloud or network.

For education institutions with dynamic data centers and networks, Apache Spot[5] is an advanced threat detection solution that runs on Apache Hadoop. Using big data analytics that perform at cloud scale, Apache Spot provides a new level of visibility into the network. It can analyze billions of events to detect unknown threats and insider threats, and provide actionable insights into operational and security threats.

Apache Spot uses machine learning as a filter for separating bad traffic from benign, and characterizes the unique behavior of network traffic. A proven process of context enrichment, noise filtering, whitelisting, and heuristics is also applied to network data to produce a shortlist of likely security threats.

Intel® architecture-based advanced analytics solutions are the efficient and effective way to capture, process, analyze, and store vast amounts of data of all types to detect suspicious connections or insider attack patterns.

10X

THE INSIGHT

for

1/10

THE COST

BEST PRACTICES

BEST PRACTICES

Developing an IT Security Strategy for K-12 Education.

Security and privacy issues are not only more critical than ever—they're also more complex. With budgets stretched to the breaking point, how can schools implement a comprehensive privacy and security strategy that makes the most of scarce resources?

- **Engage stakeholders** in discussions to broaden understanding of security risks, and develop an integrated approach to managing those risks.
- **Conduct a risk assessment** to identify security gaps. Establish priorities to address gaps, factoring in issues such as the likelihood of a security event, and how serious the consequences would be were it to occur. Then, develop an implementation plan that aligns processes, policies, and technologies.
- **Train everyone** who uses digital resources. Educate students on digital citizenship, and help them understand that they are building their digital identity with every action they take online.
- **Establish a security chief** to lead the creation of a security-aware school culture. The security chief also keeps up with the latest federal and state regulatory requirements, and works with stakeholders to protect digital resources and drive student outcomes.

In this book:

BEST PRACTICES (CONT.)

- **Practice minimalism.** Don't collect and store more data than you need. This helps reduce storage costs as you safeguard that data.
- **Develop policies** that spell out what data can be stored on teacher and administrator laptops. Implement strong security measures to protect any sensitive data.
- **Address security and privacy concerns** in all contracts with third parties. Collect and share only the data necessary to provide the desired level of service.
- **Examine the security implications** of all purchases, including mobile devices. For example, will devices have mature management software available? Are any security and privacy protections built in?
- **Choose robust, proven security solutions** that are easy to use. Solutions that simplify IT operations can enhance IT productivity and reduce costs.
- **Make a living program.** Create a cycle of continuous improvements based on lessons learned. Continue to evolve your security strategy as threats and compliance requirements evolve, and new solutions become available.

Digital data and resources are essential to providing each student with a personalized learning experience that improves outcomes and helps them achieve their life goals. By choosing devices and systems based on Intel® technologies and implementing a robust privacy and security strategy, your school system can safeguard privacy and protect assets while delivering the full educational benefits of digital technologies.

For more information and resources visit **intel.com/edusecurity**

Footnotes

[1] Beyond the Fear Factor, Sept. 2015 at http://www.studentprivacysymposium.org/assets/Beyond-the-Fear-Factor_Sep-2015.pdf p 12 accessed Dec. 12, 2015

[2] “McAfee Labs Threat Report”, November 2015 at http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-nov-2015.pdf accessed March 9, 2016

[3] The Shift to Digital: Market Trends in Education to Watch in 2015, Center for Digital Education Webinar, page 17, at http://www.slideshare.net/jonyoffie/center-for-digital-education-education-market-forecast-2015-webinar accessed October 13, 2016

[4] http://www.infosecwriters.com/Papers/SEdwards_k-12.pdf pg 2, accessed Mar. 9, 2016

[5] Apache Spot http://spot.apache.org/ accessed October 26, 2016