WHITE PAPER

Cloud Security for K-12 Education

How can school systems make the most of cloud computing while maintaining security, privacy, and compliance? Intel edtech experts describe issues and solutions.

Introduction: Embracing the Cloud While Maintaining Security

Cloud computing offers broad benefits for K-12 education. It can enhance teaching and learning by enabling students and teachers to access a wealth of educational resources—to work, collaborate, communicate, and share when and where they need to. Cloud computing can give edtech staff more time to focus on strategic uses of technology, and allow them to respond faster to requests from educators. Clouds can enable school systems to operate with greater efficiency, cost-effectiveness, and agility.

However, school systems operate in a regulated environment. They deal with minors. They use and store a wide range of highly sensitive data. Cloud computing presents school systems with new questions and concerns relating to data privacy, security, and regulatory compliance.

In the rush to embrace cloud computing, it can be easy to give short shrift to these matters—or to assume that a cloud service provider will handle anything related to security. Either course of action increases the risks of cloud computing, threatening to expose sensitive data, damage trust in the school system, and incur fines from regulatory agencies.

This paper is intended to help school systems take advantage of cloud computing while maintaining data privacy, security, and compliance. Designed for K-12 IT leaders, this paper:

- **Provides an overview** of cloud security and compliance issues
- **Shares strategies** for addressing them
- **Describes Intel® Security solutions** that can help you strengthen security, trust, and compliance in the cloud—and reap cloud computing's rewards

Cloud Security Overview

Cloud infrastructures—built on shared servers and operating in virtualized, multi-tenant environments—can create attractive targets for malicious entities. Moving information beyond the secure perimeter of the school or district can diminish IT's visibility and control over the environment. Without appropriate safeguards, cloud services may violate regulatory requirements governing the confidentiality and use of student data.

Table of Contents

Public, Private, or Hybrid?

Private clouds are dedicated to a single organization. A private cloud may be a virtual environment you establish on your own premises, or established and managed by an external cloud service provider and running in its data center. In a private cloud, each customer organization has dedicated hardware and software, and resources are not shared with other clients. Customers have more control over the type of infrastructure on which their application runs.

Public clouds are multitenant environments established and managed by external cloud service providers and run in their data centers. Infrastructure and resources are shared among multiple customers as determined by the CSP. Each individual server may run multiple virtual machines, often from many different customers.

Hybrid clouds combine the two models. You might keep highly sensitive workloads and applications in your on-premises private cloud, and shift those with less-sensitive data to a public cloud. A hybrid cloud delivery model can help maintain control and security while enabling school systems to enjoy the educational and operational benefits of public cloud services and infrastructure.

Cloud security encompasses the policies, technologies, and controls you implement to protect data, infrastructure, and assets from attack and to enable regulatory compliance. It should be a top-of-mind concern for IT leaders whether your school system uses software-based cloud services such as Google Apps for Education,* a public cloud such as Amazon Web Services,* or a hybrid cloud that blends private and public delivery models. (See sidebar, Public, Private, or Hybrid?)

Cloud security focuses on:

- **Safeguarding information and assets,** which may include legally protected information and other sensitive data ranging from student assessment and medical data, to family financial data, and staff and teachers' personnel files
- **Maintaining the privacy and confidentiality of data,** including protecting students and others from identity theft and other forms of fraud
- **Complying with statutory and regulatory requirements** governing the protection of minors, the use and handling of student information, and other issues
- **Avoiding** any disruptions to teaching and learning and ensuring technology investments are available to support learning and teaching every day

Comprehensive Planning, Layered Solutions

No single technology can ensure a secure cloud environment. Rather, security results from a holistic approach, with layered solutions that form a durable security net or grid by linking:

- **Users –** teachers, students, parents, administrators and other staff
- **Applications –** student information systems, e-text books, adaptive learning resources, and others
- **Infrastructure –** servers, storage, networks, and gateways

To avoid gaps that put confidential data and assets at risk, you'll need to evaluate cloud security in the context of your overall security strategy. Look for end-to-end solutions that encompass the three key functions shown in Figure 1:

- **Protecting** data and assets from attack or theft
- **Detecting** any breaches that occur despite your efforts
- **Correcting** the damage and recovering from the attack

Since cloud breaches can result from activities on mobile devices or other client computers, your cloud security strategy should address client security as well as cloud-specific solutions. Human behavior often contributes to security breaches, so your cloud security strategy should include educating students, teachers, and staff on security best practices. Basic policies, such as requiring virus protection and anti-malware on all mobile systems and ensuring that only teachers, students, and parents or legal guardians can see certain data, can play a key role in protecting your cloud environment as well as any other infrastructure.

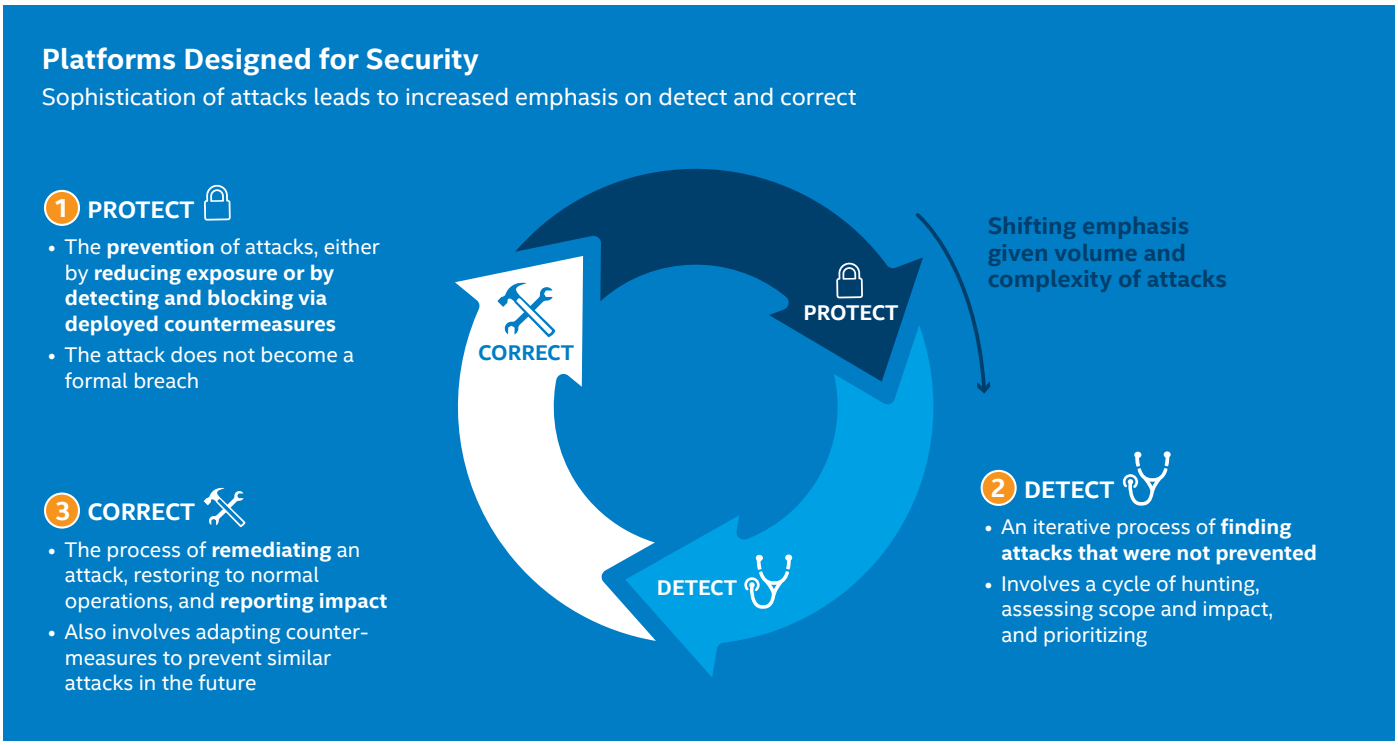

Figure 1. Intel® Platforms Are Designed for Security. Security solutions can help prevent attacks and make it easier to detect and recover from a breach.

The Cloud Security Alliance has identified 10 security categories that align with the Protect-Detect-Correct framework and can help you safeguard digital assets in the cloud (Table 1). Later in this paper, we'll describe solutions from Intel and McAfee that offer technologies that address cloud and client security.

TABLE 1. CLOUD-BASED SECURITY CATEGORIES[1]

CATEGORY	TYPE	DEFINITION
Identity and access management	Protect	Manage access to resources by verifying identities and granting the appropriate level of access
Data loss prevention	Protect	Monitor, protect, and verify the security of data at rest, in motion, and in use in an external cloud or on premises
Web security	Protect, Detect, Correct	Filtering or redirecting web traffic to prevent malware from entering the school system via web browsing or other web-related activities; remediating attacks
E-mail security	Protect, Detect, Correct	Controlling e-mail to protect the school system from phishing, malicious attachments, spam, and related threats
Security assessments	Detect	Conduct internal or external audits of infrastructure, applications, and compliance to assess adherence to standards
Intrusion management	Detect, Correct	Identify and react to intrusions or policy violations
Security information and event management	Detect	Track log and event information and provide real-time reports and alerts on activities that may require intervention
Encryption	Protect	Use cryptographic algorithms to enable only the intended target of a document to read it
Business continuity and disaster recovery	Protect, Detect, Correct	Ensure required services remain available despite natural or man-made disruptions
Network security	Protect, Detect, Correct	Safeguard the continuity and integrity of network traffic and services

Issues and Challenges

As with traditional devices and platforms, cloud environments and data must be protected from malicious outsiders as well as from inadvertent or intentional actions by students or staff. Among the issues to be addressed:

Identity and Access Management

Utilizing cloud services or cloud-based infrastructure means school systems can no longer take a closed-perimeter approach to security. Instead of relying on firewalls as single points of control, security practices and technologies must provide control points for client devices and application programming interfaces (APIs) accessing the cloud and edge systems. Existing organizational identification and authentication frameworks may not extend into the cloud. If these schemes are based on unique username/password combinations for individual applications, they can represent a weak link in the security chain. Gateway appliances that manage identities and APIs at the network edge can help ensure that only authorized users gain access to resources on a public or private cloud. PCs, laptops, and other clients with identity protection technology and antivirus solutions can enhance security throughout the environment.

Protection of Data

Protecting sensitive student data and assessment records is one of the most fundamental responsibilities of educational organizations, and one of the most tightly regulated.

Data stored or used in a public cloud typically resides in a multi-tenant environment, sharing virtualized server space with other cloud users. Cloud service providers (CSPs) implement rigorous isolation mechanisms to separate memory, storage, and routing between tenants. However, there is a risk of contamination if the isolation mechanisms fail or a malware attack is successful. Cloud computing also presents a risk of insecure or incomplete data deletion when a school system terminates a CSP's services. Implementing a hybrid cloud can enable school systems to keep their most sensitive data on premises while enjoying the educational and operational benefits of public cloud services and infrastructure for less sensitive data. Encrypting sensitive data can help protect it wherever it resides or is used.

Protection Against Malware

For cybercriminals, virtualized cloud infrastructures offer an even larger potential attack surface than a traditional data center. Onslaughts using malware and rootkits can infect cloud system components such as hypervisors, BIOSes, and operating systems and spread throughout the environment. In addition to access-control gateways and other security measures, protecting a cloud from malware requires establishing roots of trust to verify the integrity of system elements.

Visibility and Trust

In cloud infrastructures, school systems relinquish direct control over many aspects of security, shifting responsibilities onto the cloud provider. IT leaders must ensure they have adequate visibility to manage cloud resources, as well as to verify that applications and data are secure and that they comply with statutory and regulatory requirements.

Regulatory Compliance and Auditability

Privacy laws and regulations differ at national, regional, and local levels, making compliance a potentially complicated issue for cloud computing. In the United States, school systems must comply with Federal standards such as the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), and the Protection of Pupil Rights Amendment (PRRA), as well as the Health Insurance Portability and Accountability Act (HIPAA) for students' medical data, and any local and state requirements. In the European Union (EU), some countries require that certain data never cross national borders. Other jurisdictions stipulate special handling of certain types of data, restricting transmittal across provincial or state boundaries or requiring documentation of security controls. To fulfill compliance requirements, cloud providers and school systems may need to provide audit records demonstrating that features such as encryption, security controls, and geo-location are being applied as specified.

School Systems at Risk

The Privacy Rights Clearinghouse, a California nonprofit corporation and advocacy group, tracks publicly disclosed data breaches for multiple industries in the United States. Its records indicate that more than 750 such breaches have occurred in the education sector since 2005—an average of more than one a week. These breaches affected nearly 15 million records, and included attacks through external malware, insider information theft, lost or stolen devices, and other methods.[2]

In a 2011 survey of more than 100 K-12 IT security personnel or consultants,[3] 84 percent said their school system had experienced one or more breaches, either malware attacks or instances of unauthorized information access, during the previous year. Forty-nine percent had experienced 2-5 breaches, and 15 percent had experienced six or more.

In 2015, the privacy of thousands of records was breached when an employee of educational billing service company left a laptop in a locked car. The laptop, which was password-protected but not encrypted, included social security and Medicaid IT numbers, putting students, staff, and teachers at risk.[4]

Intel® Technologies: Your Cloud Security Foundation

Intel Security provides comprehensive technologies and services to help school systems create better-protected clouds, both in the local data center and off premises.[5] Intel Security also offers solutions that can better protect tablets, laptops, and other mobile devices, since these platforms are often the conduit through which malicious software enters the K-12 network and cloud environment.

Intel Security solutions combine McAfee's security expertise with Intel's long-time leadership in platform technologies, to provide hardware-enhanced solutions for some of the most important challenges for K-12 cloud computing. These solutions offer tamper-resistant capabilities to improve identity and access management, promote pervasive data encryption, provide more secure data movement, measure platform integrity, and build higher assurance into compliance efforts.

Here are examples of key Intel capabilities for secure cloud and client computing.

Protecting Data

Data encryption, which makes data unusable if compromised, helps safeguard data as it moves in and out of the cloud and is used within the cloud.

The Advanced Encryption Standard (AES) algorithm is typically used for encryption, but AES relies on compute-intensive algorithms that can impact network performance and create computing logjams, particularly when used to protect the massive volumes of data that pass to and from the cloud.

Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) mitigates these performance penalties. Built into select Intel® Xeon® processors and other Intel processors, Intel AES-NI strengthens and accelerates the execution of AES encryption algorithms, delivering faster, more robust data protection for cloud computing.[5]

Intel has also developed capabilities to speed key aspects of the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) browser security protocols, which are used to assure safe communications over the Internet. TLS and SSL protocols are critical for secure cloud computing, preventing undetected content tampering or "eavesdropping" on content as it's transferred over the Internet. These protocols are also widely used for secure web browsing (HTTPS), electronic mail, instant messaging, and voice over IP. Reflecting its commitment to open standards, Intel has contributed its TLS/SSL improvements to the open-source protocol OpenSSL*. This enables any software that incorporates OpenSSL to automatically take advantage of these Intel® platform advancements when running on an Intel Xeon processor E5 or E7 family-based platform.

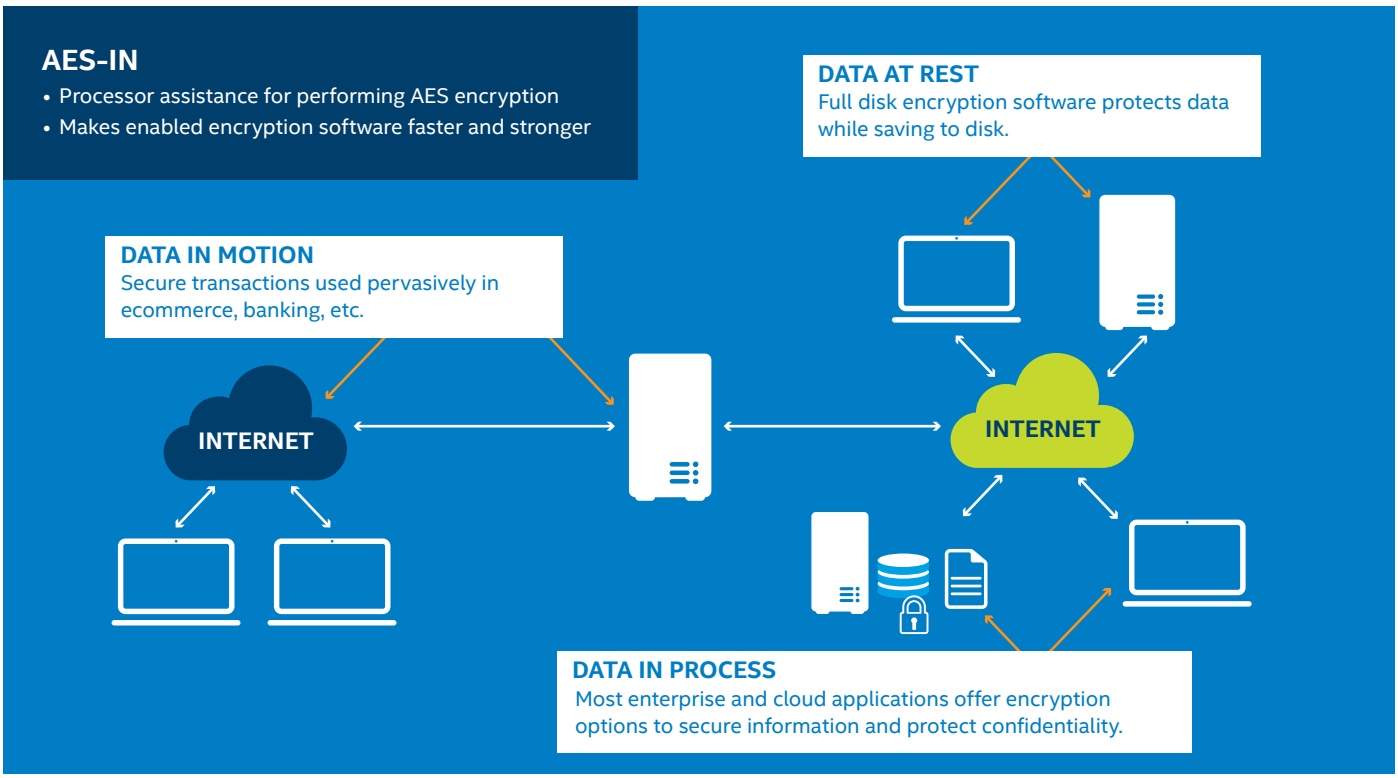

Figure 2. Protecting Data in the Cloud with Intel® AES-NI . Encryption can help protect sensitive data when it's at rest, in use, or in transit.

By using Intel Xeon processor-based platforms for cloud computing, school systems can accelerate data encryption, secure session initiations, and bulk-data transfers. This can contribute to better utilization of network resources and pervasive data protection to and from the cloud without compromising network performance.

Enhancing Trust, Visibility, and Compliance

External clouds push the perimeter of the school system beyond the traditional data center, and create a larger attack surface for malware and other exploits. The threats against these larger, virtualized surfaces can involve malware assaults at the application level, as well as attacks against lower-level components in the platform itself.

To enhance security and compliance in the cloud, Intel Xeon processors include Intel® Trusted Execution Technology (Intel® TXT), which helps ensure system integrity by establishing a hardware root of trust at the level of the chipset and CPU.[5] This root of trust provides a solid foundation upon which to build secure virtual platforms and pools of trusted computing. This lets you or your CSP substantially reduce the security risks of virtualized cloud infrastructure by restricting sensitive workloads to these trusted compute pools.

Intel TXT measures platform components such as the BIOS and hypervisor in their "known good" state. These trusted measurements are stored in hardware and compared to boot-time measurements made during subsequent launch sequences. If the measurements don't match, Intel TXT can block the launch of the platform, mitigating boot-level attacks.

These capabilities and others provided by Intel TXT can significantly enhance your on-premises or external cloud. For example, in addition to establishing a safe environment for launching virtual machines (VMs), Intel TXT can help IT shops strengthen compliance and security by:

- Improving insight and visibility into the underlying infrastructure, including verifying that VMs have launched in a trusted environment.
- Enforcing security policies such as one requiring that VMs identified as related to sensitive workloads will only be migrated between hosts that have undergone a verified launch.
- Ensuring that applications dealing with sensitive data run only in isolated environments on dedicated resources managed by the underlying platform.
- Protecting communication between input devices (such as mice and keyboards) and execution environments to guard against the data being compromised by unauthorized software processes.
- Scrubbing memory during environment shutdown to guard against memory snooping or reset attacks in a shared-resource environment.
- Improving compliance through information that helps document what's happening in the cloud environment and verify that security policies are set, monitored, and certified.

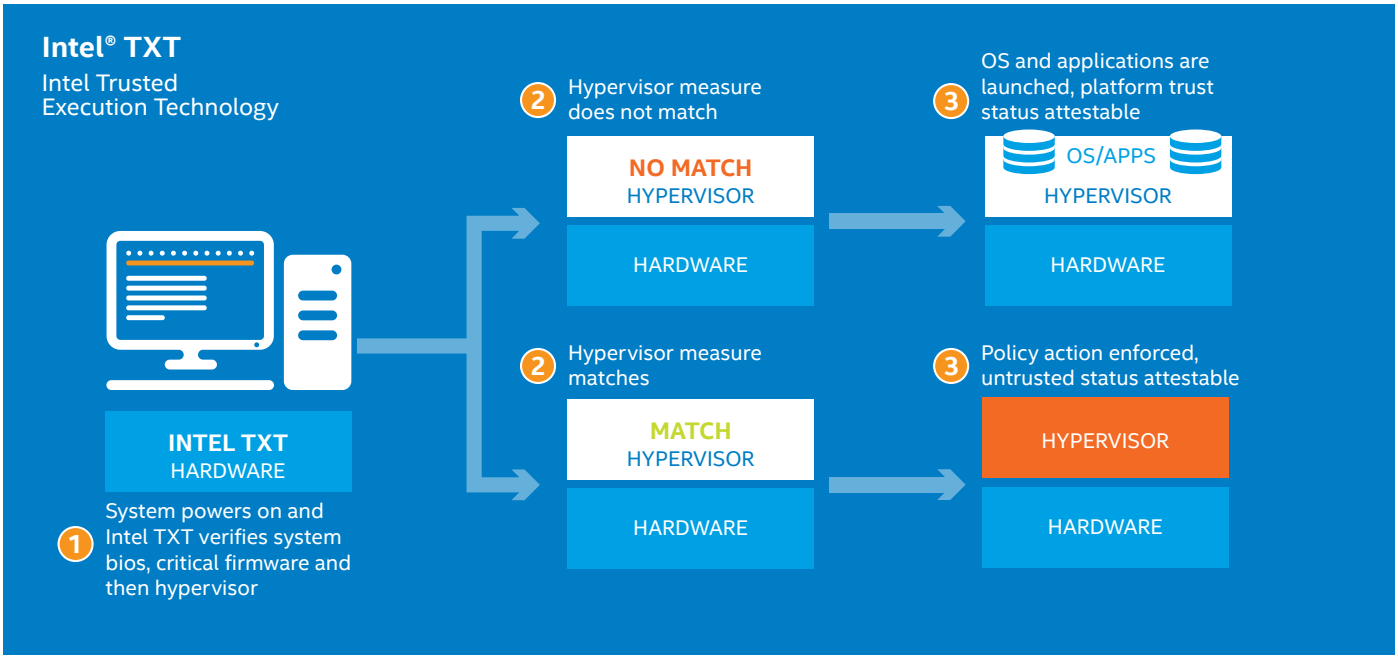

Figure 3. Enhancing Trust, Visibility, and Compliance with Intel® Trusted Execution Technology. Among its hardware-assisted security capabilities, Intel® TXT can help ensure that sensitive workloads run on trusted servers and within specified geographic boundaries.

Securing Client Computers

Student computers are often the pathway through which data on a cloud or network is compromised. This is particularly true in bring-your-own-device (BYOD) environments if IT leaders fail to establish and enforce reasonable policies or to educate students, teachers, and staff on security best practices. Basic policies can include that BYOD systems as well as school-issued devices run up-to-date antivirus software. Training can reinforce cyber safety practices such as not sharing cloud passwords, and ways to protect thumb drives and other mobile media. In addition to enhancing district security, this can provide valuable training for students as they become as digital citizens.

For district-supplied systems, devices should be chosen with an eye to the availability of mature mobile device management (MDM) and security technologies. MDM solutions that enable IT staff to manage devices remotely can strengthen security by making it easier to keep software up to date and to install the latest security patches.

Intel Security offers a wide range of solutions to help school systems better protect their client computers. For example:

- Laptops with select Intel® Core™ processors may also include Intel AES-NI, offering hardware-assisted performance for encryption and decryption on the client system.
- McAfee VirusScan* Enterprise safeguards systems and files from viruses and other security risks. It detects and removes malware, and configures antivirus policies to manage quarantined items. With mobile threats rising sharply,[6] McAfee VirusScan Mobile Security offers welcome protection for smart phones and tablets.
- Tablets and other platforms with Intel® Identity Protection Technology (Intel® IPT) help provide a simple, tamper-resistant method for protecting access to sensitive data in the cloud or elsewhere. Intel® IPT can be a key component in two-factor authentication solutions.

Collaborating with Cloud Service Providers

Although public clouds can present larger and more inviting attack surfaces, the risks are mitigated by leading-edge cloud service providers, who generally have greater expertise and resources than even large school systems can afford. A well-designed and expertly managed external cloud, based on Intel® technologies and coupled with your on-premises private cloud, can provide a cost-effective way to meet educational needs and keep pace with security threats that are growing faster than IT budgets.

However, cloud security is not something you can assume a cloud service provider will automatically provide at the level you require. Depending on the cloud delivery model and services deployed, cloud security will generally be a shared responsibility between school systems and their cloud providers. So, it's important to spell out what security and compliance services you require, to verify what the CSP will deliver, and to make security an important part of your CSP selection process.

In addition to factors such as data ownership, liability, portability, and others, your conversations with cloud service providers should explore security-related questions such as:

- What role will the CSP play in performing incident response, including attack analysis, containment, data preservation, remediation, and service continuity?
- What data will they collect and what audits will they perform to assist you in demonstrating regulatory compliance? Can they guarantee that local data remains local, if that's required? Can they ensure that student data is handled appropriately, including being deleted and disposed of correctly?
- How frequently do they perform regular penetration testing?
- How will they monitor traffic patterns and report on attempted attacks, whether from a student, teacher, CSP employee, or external actor?
- How will they help you provide users with a single sign-on experience for both public and private clouds?
- What data management tools will you use? Will they provide sufficient visibility to determine that policies are being enforced and compliance requirements are being met? Will they give you "single pane of glass" visibility and convenience to manage both internal and external cloud services?

Security and data privacy should also be central to contract negotiations with educational service providers. Make sure you understand what student data they collect, how robust their internal security technologies and processes are, and how they will respond if their cloud infrastructure is breached.

Taking Advantage of Intel® Security Innovations

Security is a critical enabler for the digital world. As the company whose technologies are at the heart of that connected world, Intel has made deep commitments to making the digital world a secure and effective one. Across the most powerful clouds to tablets, PCs, smartphones, and beyond, Intel is moving security from discrete solutions to an integrated approach as pervasive as computing itself.

Just as Intel processors deliver higher performance with each new generation, each generation of Intel Xeon processor-based platforms delivers functionality that increases their ability to protect data and infrastructure in the face of growing threats and regulation. Intel security experts also work with open source developers, cloud service providers, and other industry players to accelerate the development of robust, secure clouds. It's all designed to help your school system do more in the digital world without adding risk.

By basing your private clouds on the latest Intel Xeon processors, investing in security technologies, and choosing cloud providers that build their infrastructure on these processors, your IT department can be prepared to deliver reliable, industry-leading performance while enhancing security and compliance. To take maximum advantage of Intel Security innovations for cloud computing:

- Build your internal clouds and infrastructure on Intel Xeon processors.
- Specify Intel Xeon processors in your Request for Proposals (RFPs) for external cloud infrastructure, including data security gateways. By ensuring that workloads run on Intel Xeon processors, you gain reliable, industry-leading performance and security enhancements.
- Use the Intel® Cloud Finder search function to identify infrastructure-as-a-service providers that meet your specific requirements.

Learn More

Work with Intel Education to implement a secure and effective framework for cloud computing. Intel can provide guidance and resources to help you advance your cloud projects—and achieve your educational technology objectives.

Learn more about Intel technologies to enhance cloud security.

Read the Intel Education brief, Hybrid Cloud in Education.

[1] Adapted from Cloud Security Alliance Security as a Service Working Group, Defined Categories of Service 2011. https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf.

[2] Privacy Rights Clearinghouse, Chronology of Data Breaches, http://www.privacyrights.org/data-breach/new.

[3] Panda Security, Kindergarten-12 Education IT Security Study, March 2011. http://www.pandasecurity.com/mediacenter/src/uploads/2011/03/Panda-K12-Education-IT-Security-Study_03.23.11.pdf.

[4] Infosec Writers, K-12 Information Security Breaches, September 2015. Downloadable from http://www.infosecwriters.com/articles/2015/09/11/k-12-information-security-breaches.

[5] No computer system can provide absolute security under all conditions. Built-in security features available on select Intel® processors may require additional software, hardware, services, and/or an Internet connection. Results may vary depending upon configuration. Consult your system manufacturer for more details. For more information visit www.intel.com/technology/security.

[6] Infosec Writers, K-12 Information Security Breaches, September 2015. Downloadable from http://www.infosecwriters.com/articles/2015/09/11/k-12-information-security-breaches.

Printed in USA 0316/MM/HBD/PDF ♻ Please Recycle 334155-001US