Ivanti Enables Secure K-12 Technology

Ivanti Solutions Brief

ivanti

SOLUTION BRIEF

Ivanti Enables Secure K-12 Technology

Gain Control of IT Assets for a Secure and Optimized K-12 IT Infrastructure

Emerging Security Concerns for K-12

Of all challenges facing K-12 school districts in the digital era, managing cybersecurity risk is among the most serious and fastest-growing.

The rapid proliferation of devices such as laptops, Chromebooks, and iPads and the adoption of e-learning models have compounded the threat of attack. As technology has grown more central to the educational experience, bad actors have homed in on schools as prime targets for an expanding array of increasingly sophisticated cyber-attacks.

The Growing Threat Space

Education is consistently ranked among the top five or six industries threatened by cyber-crime. In fact, Microsoft's threat analysis data indicates that Education is the number one industry targeted for attack, with attacks against schools reflecting up to 83% of all recorded cyberattacks.[1]

Meanwhile, the Multi-State Information Sharing and Analysis Center (MS-ISAC) reports that 57% Of ransomware incidents involve K-12 schools.[2] So it's no surprise that the Center for Internet Security predicted an 86% rise in K-12 cyberattacks for the current school year.[3]

Devices and Risk

Contributing to the risk elevation is the introduction of external devices onto school networks. According to the Center for Internet Security, 85% Of educational institutions allow students, teachers, and faculty to use personal devices on school networks.[4]

But mobile and personally owned devices are only part of the problem. The Texas Education Agency reports

ivanti.com

Ivanti Enables Secure K-12 Technology

Gain Control of IT Assets for a Secure and Optimized K-12 IT Infrastructure

Emerging Security Concerns for K-12

Of all challenges facing K-12 school districts in the digital era, managing cybersecurity risk is among the most serious and fastest-growing.

The rapid proliferation of devices such as laptops, Chromebooks, and iPads and the adoption of e-learning models have compounded the threat of attack. As technology has grown more central to the educational experience, bad actors have homed in on schools as prime targets for an expanding array of increasingly sophisticated cyber-attacks.

The Growing Threat Space

Education is consistently ranked among the top five or six industries threatened by cyber-crime. In fact, Microsoft's threat analysis data indicates that Education is the number one industry targeted for attack, with attacks against schools reflecting up to 83% of all recorded cyberattacks.[1]

Meanwhile, the Multi-State Information Sharing and Analysis Center (MS-ISAC) reports that 57% Of ransomware incidents involve K-12 schools.[2] So it's no surprise that the Center for Internet Security predicted an 86% rise in K-12 cyberattacks for the current school year.[3]

Devices and Risk

Contributing to the risk elevation is the introduction of external devices onto school networks. According to the Center for Internet Security, 85% Of educational institutions allow students, teachers, and faculty to use personal devices on school networks.[4]

But mobile and personally owned devices are only part of the problem. The Texas Education Agency reports

that out of some 4.5 million devices used in schools statewide, 22% of devices checked out in an average school district are non-recoverable.[5] Untracked and unrecoverable devices are a significant cost and threat for the school system.

Classroom management and collaborative work has been revolutionized by ChromeOS. Teachers use Chromebooks to manage their classrooms and assign work to their students. Chromebooks also have built-in tools for collaborative work, which make it easier for students to work together on group projects. Managing Chromebooks/ChromeOS doesn't have to be a pain for IT and Cyber teams.

Student Privacy

Safeguarding data privacy and students: As more students take school-issued mobile devices home with them, data privacy is an increasing concern. With the prevalence of software as a service (SaaS) in K-12 education, there's legitimate concern about students' data being stored on remote servers. Compliance with Family Educational Rights and Privacy Act (FERPA), Children's Internet Protection Act (CIPA), and the Children's Online Privacy Protection Rule (COPPA) is important to ensure students are protected.

New and Persistent Challenges

While keeping students, educators, and school's IT systems safe and protecting privacy remains a top priority for K-12 administrative bodies, these new threats emerge within a landscape of familiar challenges for schools. K-12 school districts face the same funding and resource issues they always have. And while security policy is set at the school board level, security-impacting decisions are made every day by administrative staff, teachers, and students.

Why Are Schools Vulnerable?

As noted above, some districts are reporting that more than 20% of devices issued to students are listed as either unknown, missing or lost, opening large attack surface vulnerabilities.

It is important to recognize that some 95% of cybersecurity breaches are due to human error.[4] Putting devices into the hands of children makes for an effective learning environment, along with a dramatic increase in the probability of the kind of human error occurring that leads to a breach.

Today technology is integrated not only into learning activities, but in much of a school's day-to-day operations. Attacks focused on disruption have major impacts on productivity, typically with the goal of taking the school offline for hours or days at a time.

How Are Schools Impacted?

Ransomware and malware often Infect unknown and mismanaged devices using a disguised approach, preventing users from accessing their network or files. This typically results in significant disruption and downtime.

Phishing attacks typically infect devices using an embedded web link or malicious code. This is a file or attachment disguised to look legitimate, which launches a background process or exploits a known vulnerability.

In addition to these major disruptions, many schools suffer from poor overall user experiences related to the maturity of the IT processes and infrastructure that are in place. Lack of process maturity leads to poor device lifecycle management and cyber hygiene issues. Even in the absence of cyber-attacks, students and educators bear the brunt of these gaps.

What's the Remedy?

In light of these challenges, many districts are adopting a three-pronged strategy to secure their environments and create a better learning experience:

1. **Invest in an Asset Management Solution**
   Secure technology to ensure school administration can track, manage, and secure devices at all times.
2. **Streamline the experience**
   Use Modern Device Management to provision devices out of the box for Students and Teachers, publish education apps, and protect student privacy in an increasingly cyber risk world.
3. **Policies & Procedures**
   Develop standard rules of engagement and sign off procedures for students and parents.
4. **Modern Device Management**
   An effective MDM can limit what applications can be loaded and used on a school owned and issued device and can remove the data and applications if the device is not in compliance with policies around latest check-in, or if the device is determined to be lost, or missing.
5. **Training**
   Provide basic training and simplify user experience focused on teachers and IT Staff including guidelines around keeping devices safe and protected.

Solution Benefits

- Ability to manage any endpoint used by students, teachers, and faculty from a single pane of glass.
- Ongoing tracking and monitoring of devices mitigates attack risk and protects students.
- Asset Management reduces staff time on manual tracking and data coordination, increasing staff focus on education.
- Avoiding loss of devices reduces overall device spend per year and ensures all devices are managed and secured.
- Students get a better experience, with increased access to devices and more secure data.
- Ability to track school-owned technology devices and staff provides a frictionless and simplified device.

Securing Assets and Mobile Devices for K-12 Environments

To support K-12 school districts looking to implement such a strategy, Ivanti introduces a product and services package to help schools gain control of their IT asset investments and secure the learning environment. The package includes three major components:

1. **Ivanti Neurons for ITAM**
2. **Ivanti Neurons Bundle**
3. **Ivanti Professional Services**

Let's take a look at each.

Ivanti Neurons for ITAM

- Consolidates your IT asset data and lets you track, configure, optimize and strategically manage your assets through their full lifecycle.

Ivanti Neurons for ITAM consolidates your IT asset data and lets you track, configure, optimize and strategically manage your assets through their full lifecycle. The solution's configurable design helps you define and follow your own workflows or implement out-of-the-box processes.

Ivanti Neurons for MDM

In environments with increasing demand for devices, applications and platforms, Ivanti Neurons for MDM is your single solution to manage iOS, iPadOS, Android, macOS, ChromeOS and Windows devices.

IN MDM quickly and easily onboard devices and provision them over the air with all the apps, settings and security configurations they need. Specially for school cycles where device churn is high, automated provisioning and lifecycle management is paramount. Learn more

Ivanti Neurons Bundle

- Includes Ivanti Neurons for Discovery, Workspace, and Spend Intelligence.
- Provides actionable asset information in minutes.
- Enables first line staff to resolve issues immediately.
- Provides instant insights into software landscape and application spend.

Ivanti Neurons for Discovery delivers accurate and actionable asset information in minutes. Automatically discover and map the linkages between key assets with the services and applications that depend on those assets.

Ivanti Neurons Workspace provides a 360-degree view of devices, users, applications, and services, with real-time data. This allows first-line analysts to resolve issues previously escalated to specialists. User and device views cut complexity, long wait times and high escalation costs, resulting in faster end user resolutions and greater productivity.

Ivanti Neurons for Spend Intelligence provides instant insights into your software landscape and application spend for on-premises, cloud, and edge environments. It helps you improve operational speed, asset visibility, and utilization, and cut costs. Obtain detailed analysis within minutes, presented in engaging dashboards of your licenses, purchases, and instances so you can track your purchase history, upcoming license renewals, contract expirations, and ongoing spend more effectively.

Ivanti Professional Services

- Provide seamless implementation of device lifecycle management.
- Enable new asset discovery and management processes to provide security and a better student and staff experience.

About Ivanti

Ivanti elevates and secures Everywhere Work so that people and organizations can thrive. We make technology work for people, not the other way around. Today's employees use a wide range of corporate and personal devices to access IT applications and data over multiple networks to stay productive, wherever and however they work. Ivanti is the only technology company that finds, manages and protects every IT asset and endpoint in an organization. Over 40,000 customers, including 88 of the Fortune 100, have chosen Ivanti to help them deliver an excellent digital employee experience and improve IT and security team productivity and efficiency. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit ivanti.com

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com

1. https://www.microsoft.com/en-us/wdsi/threats
2. https://www.cisa.gov/uscert/ncas/alerts/aa20-345a
3. https://edscoop.com/cyber-incidents-k12-schools-expected-rise-86-percent/
4. https://edscoop.com/cyber-incidents-k12-schools-expected-rise-86-percent/
5. https://www.khou.com/article/news/investigations/10-million-computers-hot-spots-missing-schooldistricts/285-d42b6f4d-edfa-486a-a007-842c1f97c087

ivanti

Thank you for downloading this Ivanti solutions brief! Carahsoft is the distributor for Ivanti education solutions.

To learn how to take the next step toward acquiring Ivanti's solutions, please check out the following resources and information:

For additional resources:
carah.io/ivantiresources

For upcoming events:
carah.io/ivantievents

For additional Ivanti solutions:
carah.io/ivanti

For additional education solutions:
carah.io/ivanti

To set up a meeting:
ivanti@carahsoft.com
833-587-5570

To purchase, check out the contract vehicles available for procurement:
carah.io/ivanticontracts