Ivanti Enables Secure K-12 Asset Environments

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 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 non-school 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. One school district in Texas reported that 22% of devices checked out have gone missing.[5] Chances are that many if not most of these missing devices will prove unrecoverable. In addition to the

costs associated with such losses, untracked devices can provide a foot in the door for cybercriminals looking for an easy way in.

New and Persistent Challenges

While keeping systems safe and protecting the privacy of students, educators, and schools remains a top priority for K-12 administrative bodies, these new threats emerge within a landscape of familiar challenges. 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.[6] Wide distribution of devices to any population, including students, can only increase 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 a trojan or embedded web link. This is a file or attachment disguised to look legitimate, which prevents users from accessing the network or files.

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. **Policies & Procedures**
   Develop standard rules of engagement and sign off procedures for students and parents.
3. **Training**
   Provide basic training and simplify user experience focused on teachers and IT Staff including guidelines around keeping devices safe and protected.

Securing Assets 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

- Reduces risk, improves efficiency and helps control costs related to managing IT assets.

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 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

Solution Benefits

- Ongoing tracking and monitoring of devices mitigates attack risk
- 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 lifecycle
- Streamlined process increases teaching and learning time

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

Ivanti Professional Services can not only help your schools discover and manage all your devices, we will help you implement a whole new process for managing hardware and software assets throughout their lifecycle.

Are you ready to stop the firefighting and get back to learning? Find out how simple it will be to cut costs and reduce risks associated with lost, missing and unused assets.

Call us today.

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 96 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. 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-school-districts/285-d42b6f4d-edfa-486a-a007-842c1f97c087
6. https://thehackernews.com/2021/02/why-human-error-is-1-cyber-security.html