Education

British Columbia School District 67

Case study

> “AppSense takes management to the next level… Before it was full control or no control. AppSense bridges that critical gap.”
>
> Danny Francisco,
> IT Manager, BC School District 67

Challenges

- BC School District 67 realized their tech-savvy users could cause disruption, they needed to securely lock-down the environment without reducing user capability and productivity or increasing overall IT support costs.
- Resource intensive applications consumed excessive CPU and reduced performance.

Solution

- AppSense Application Manager and AppSense Performance Manager components were deployed to proactively secure the environment and improve system performance.
- Later AppSense Environment Manager was deployed to all desktops to provide a suitable lock-down functionality without compromising user capability.

Benefits

- Prevent all unauthorized applications
- Achieved high levels of security while improving end-user productivity
- Decreased client re-imaging to once a year.
- Secured and simplified applications through lock-down capabilities
- Centralized security management for terminal servers, desktops and laptops
- Improve resource utilization to support more users per server
- Enhanced Citrix server and desktop performance
- Decreased overall IT support costs

BC School District 67 uses AppSense across Citrix, desktops and notebooks for 8,000 users

Organization

A technology pioneer, British Columbia School District 67 (Okanagan Skaha), is the province’s only district with a centralized fiber optic network, which it shares with the City of Penticon. The IT department services 7,500 students and 800 staff across three high schools, four middle schools and ten elementary schools.

Ensuring high level of security without compromising productivity

School District 67 supports 2,000 desktops, 14 Citrix Servers and 300 laptops. Ensuring security, stability and performance in such a diverse environment - particularly when so many of its users are tech savvy students - proved to be a tremendous challenge. With thousands of students, IT is just as worried about security breaches coming from inside the firewall as outside. Often, IT has to provide users with administrative rights in order to run required software. However, this is the quickest way that networks are exposed to potential threats.

Running unauthorized applications

In the past, spyware, adware and other malware could easily run on any terminal server or desktop client. When spyware ran, it would consume extra resources, slowing response times. To get rid of spyware and restore integrity, stability and performance, IT would have to re-image machines every single month.

Exposure of sensitive information

Students and teachers often share computers. In several instances, students installed keyloggers on computers right before teachers logged on, enabling them to capture the teachers’ keystrokes. As these were unknown, custom applications, reactive measures such as antivirus and application black lists were unable to provide protection. The IT department knew it needed to take extra precautions, but didn’t want to restrict students from using USB devices, which they had come to rely on. At the same time, IT didn’t want to expose their machines or network to malicious code downloaded from USB devices. IT either had to lock USB devices out completely or allow them to be used by everyone.

Desktop management

The IT department had to manage, policy and personalization on its Citrix thin client, desktop and laptop environments separately. There was no central way to administer policies, manage profiles or provide fixes. This reactive method to desktop management proved to be very time consuming.

User load and CPU limits

The School District wanted to optimize its thin-client servers by increasing user load without impacting quality of service. In addition, several critical applications consumed 100% CPU - resulting in significant performance hits and increased support calls, thus higher overall management costs. IT needed to control CPU consumption, ensure reliable performance and keep help desk calls down.

Flexible, granular system protection enhances user productivity

BC School District needed a solution that eliminated the threat of malware and user introduced applications, maintained productivity, and optimized network performance. They turned to AppSense Application Manager and AppSense Performance Manager to:

Balance security with end-user productivity

IT does not choke off end-user productivity, in fact, it enables users to work even more productively.

Education
British Columbia School District 67

> “ AppSense helps us achieve balance via flexibility and granularity. Their device management and user self-authorization features change the dynamics of how we manage IT security and make a big difference in our ability to secure endpoints while ensuring productivity of our users. It’s ideal for a dynamic organization like ours. ”

Danny Francisco,
IT Manager,
BC School District 67

Centralized management for citrix servers, desktops and laptops

AppSense’s ability to easily work across all client delivery mechanisms is a tremendous advantage. For instance, Microsoft’s built-in software restriction policies and drive mappings require a lot of administration. AppSense uses intuitive rules and memberships to deploy settings to all clients under one unified interface, making it highly scalable. It is a perfect solution for the district’s 300 laptops because its security settings are cached locally making them easier to enforce, and laptops always get the newest policies when they reconnect.

“AppSense enables us to easily manage a total, end-to-end solution. It’s a lot more customizable and granular than the built-in Microsoft capabilities. AppSense takes management to the next level,” said Francisco.

Enhance Citrix performance

School District 67 uses AppSense Performance Manager in its Citrix environment to increase user load/server and control the amount of CPU used by processor-intensive applications, resulting in a more stable, well-performing Citrix build and improved user density.

Usb device control

AppSense enables IT to restrict applications on USB drives, which is critical, as Francisco said, “We don’t want to lock out the convenience of users storing data on their thumb drives, but we don’t want them to put malicious code onto the network. With AppSense, they can use USB devices, but we can also control what they can execute.”

Self-authorization aids teacher productivity

With AppSense’s self-authorization capabilities, the system automatically notifies teachers prior to running something out of policy or unsanctioned by IT and asks them if they want to continue running it. As a result, teachers don’t wait to get access to applications they need, but also realize their actions are out of policy area and are monitored. If they’re unsure, self-authorization gives them pause to check with IT before executing. “Before it was full control or no control. AppSense bridges that critical gap.”

How it works

BC School District 67 started using AppSense Performance Manager and AppSense Application Manager in its Citrix environment. It then implemented AppSense solutions across their desktops and laptops, utilizing the single AppSense management console to control all desktops, regardless of how they are delivered to the user.

Moving forward

The School District is implementing AppSense Environment Manager primarily for locking down user interface. However, they plan to leverage even more of its rich features in the coming months.

“It’s a really exciting product; It’s a goldmine in itself,” Francisco commented. AppSense Environment Manager will enable IT to manage and control what users can see and do on the School District’s systems, such as which applications they see when they log on, their interactions with critical files like registry keys, or other processes or services, reducing the possibility of corruption even further.

Eliminate internal breaches

AppSense eliminated the chances of unintentional - and intentional - breaches, from within and outside the firewall. Even when students try to circumvent security policies they don’t succeed because AppSense security is “so deep and granular,” says Danny Francisco, IT manager for School District 67. Only authorized applications can run. Instead of ongoing re-imaging for security purposes, IT only re-images once a year for maintenance.

Technical overview

The BC School District 67 infrastructure consists of 14 Citrix Servers, all of which are HP enterprise class servers. In addition it has 2,000 desktops and 300 HP Tablets. All of the School District’s Citrix-based, desktop and laptop applications are protected and enhanced with AppSense solutions.

- AppSense Application Manager
- AppSense Environment Manager
- AppSense Performance Manager

About AppSense

AppSense is the global leader in User Environment Management (UEM) with over 3,000 enterprise customers worldwide that have deployed to over 7 million desktops. AppSense DesktopNow and DataNow enable IT teams to deliver the ultimate user experience and productivity across physical and virtual desktops while optimizing security and reducing operational and infrastructure costs. The company is headquartered in Sunnyvale, CA with offices around the world.