



Waubonsee Community College Ensures Secure Use of Safe Cloud Apps by Thousands of Users

The global pandemic has challenged educational institutions everywhere to keep their data secure, even as users work remotely with unmanaged apps and devices. At Waubonsee Community College west of Chicago, IT experts are taking a proactive approach to data security with the Netskope Security Cloud platform. Now, as the college adapts to changing times, students can choose to study in classrooms or remotely.

How Can a College Minimize Data Risk in a Hybrid Learning and Work Environment?

Seeking a balance between preventing the spread of COVID-19 and providing high-quality in-person instruction, Waubonsee Community College offered students a choice of remote or classroom learning. For Senior Information Security Manager Tarun Trivedi, this meant greater oversight of the apps that students and faculty were using and how they were accessing and storing data. "Being remote, we've increased our vigilance," he says. "We want to ensure faculty and staff are not downloading sensitive content to their laptops."

Waubonsee's CIO places a great emphasis on compliance and industry best practices. So, Trivedi wanted to be proactive in stemming the risks of data privacy infringements and data exfiltration, as well as other threats that might exploit vulnerabilities on user devices. He and his team also needed an efficient and effective way to screen cloud apps for security risks and to ensure compliance with security policies. In-person coaching for the thousands of scattered users was not an option.



We wanted to be proactive about stopping threats before they occur. With the Netskope client, we can constantly monitor alerts and incidents. And the data protection provides automatic notification of any exposure of personally identifiable information."

Tarun Trivedi, Senior Information Security Manager,
Waubonsee Community College



Profile

Industry



Higher Education

Region



North America

Students



8,665

Revenue



\$74.4 Million

Website Link

Challenges

- Hybrid learning increased risk of data loss and exposure.
- Users were unaware of unsafe data and app use practices.
- IT leaders sought a proactive approach to data security.

Solutions

- Netskope CASB monitors data at rest and in motion.
- Netskope CCI assesses SaaS risk, supporting use policies.
- Real-time coaching manages user behaviors to safer alternatives.

Results

- Reduced risk to data when offering hybrid study options.
- Greater user awareness of security best practices.
- Improved security posture and ensure compliance.



Tapping the Breadth and Depth of the Netskope Security Cloud Platform

Waubonsee uses the Cloud Access Security Broker (CASB) function within the Netskope Security Cloud platform to scan some 2,500+ cloud apps to see if they are being accessed from managed devices.

To enable this broad app use visibility, the Netskope client is installed on every managed device, “We wanted to be proactive about stopping threats before they occur,” Trivedi explains. “With the Netskope client, we can constantly monitor alerts and incidents. And the data protection is a huge benefit in that it provides automatic notification of any exposure of personally identifiable information.”

The security team is making use of the Netskope Cloud Confidence Index (CCI) as a tool for devising cloud app usage policies. It helps Trivedi weigh the risks of the apps users want against the value the apps provide.

To help ensure that everyone is using apps and data according to the college’s policy, Waubonsee is leveraging the real-time coaching feature of Netskope’s Security Cloud platform. “We had individuals trying to circumvent the established policies,” Trivedi says. “We needed to stop faculty and staff from purchasing SaaS solutions and uploading data to unknown vendors. I did not find any other solution provider besides Netskope that offered this type of policy control and real-time coaching service.”

Trivedi and his team are currently exploring the data loss prevention (DLP) features of the Netskope Security Cloud platform to prevent users from moving copyrighted data or personally identifiable information (PII) from Waubonsee’s protected managed infrastructure to unauthorized locations in public clouds or via SaaS to personal devices.

Maintaining Stable Security Posture as Community of Users Changes

When Waubonsee Community College welcomes a new class of students each semester, its extensive cloud app monitoring capabilities and attention to best practices enable the institution to keep its promise to students—to choose when, where, and how they take classes—in a secure and compliant manner.

As students, faculty, and staff come and go, the various features of the Netskope Security Cloud platform will help Trivedi and his team ensure consistency in security policy enforcement and compliance with data privacy regulations.

Looking back at the Netskope implementation, Trivedi notes that he is happy to have found a technology partner that aligns with Waubonsee’s proactive approach to data protection. “With all the security and privacy-related products I had that are ahead of the curve,” he says, “it’s good to have a partnership with a company like Netskope that keeps up with the trends.”



We needed to stop faculty and staff from purchasing SaaS solutions and uploading data to unknown vendors. I did not find any other solution provider besides Netskope that offered this type of policy control and real-time coaching service.”

Tarun Trivedi, Senior Information Security Manager, Waubonsee Community College



Netskope, the SASE leader, safely and quickly connects users directly to the internet, any application, and their infrastructure from any device, on or off the network. With CASB, SWG, and ZTNA built natively in a single platform, Netskope is fast everywhere, data-centric, and cloud-smart, all while enabling good digital citizenship and providing a lower total-cost-of-ownership. **To learn more, visit [netskope.com](https://www.netskope.com)**