SILVERFORT

CASE STUDY

West Valley School District Extends MFA Protection to All Faculty Users While Securing Service Accounts

West Valley School District 208 strives to help all students become responsible and productive citizens, effective communicators, creative problem-solvers and life-long learners. Through mutual support and the combined efforts of their families, schools and community, they provide a safe, high-quality learning environment in which each student experiences success every day.

BASED
Yakima, Washington, US

INDUSTRY
Education

EMPLOYEES
800 staff and 5,250 students

ENVIRONMENT
On-prem Active Directory, O365, SQL servers, legacy applications, privileged admin accounts

The Challenge: MFA Protection to All Users

- Comply with MFA requirements for cyber insurance
- Limit and protect service accounts with excessive privileges
- Secure access requests to network equipment

The Results: Extending MFA Protection to All Users and Resources

- Renewed cyber insurance policy
- End-to-end service account protection with access policies
- MFA protection for all network devices

The Challenge

Complying With New Cyber Insurance MFA Requirements

Identity security is a cornerstone in K12 education, driven by the profound sensitivity of student data and the burgeoning dependence on digital learning platforms. As the educational landscape evolves, so do the threats posed by malicious actors. Recognizing these ongoing risks, West Valley School District's cyber insurance provider tightened their MFA requirements for customers seeking to renew their policy.

"Our cyber insurer mandated a solution that would enable MFA protection and authentication for all district staff with email access. Until we were able to implement a solution that could help us meet the MFA requirements of our cyber insurance policy, we were unable to renew our policy at the lower price we desired," said Jeremy Cox, Director of Information Technology at West Valley School District.

West Valley School District examined a variety of MFA solutions to help them comply with the new requirements and renew their cyber insurance policy.

> "Throughout our search, we concluded that we needed an identity solution tailored for K12 education, emphasizing simplicity and effectiveness as our guiding principles."

Improved Protection of Service Accounts and Access to Network Equipment

In addition to implementing MFA protection for all staff and students, West Valley School District sought to enhance the real-time protection of their service accounts. "We sought a solution that would give us complete protection of our 55 service accounts. With some accounts carrying excessive privileges, the delicate balance between access control and maintaining functionality posed a significant challenge," said Cox.

Similar to other education districts where IT teams usually have limited resources, being able to automate the process of protecting their service accounts was key for the West Valley School District.

> "We had limited resources to devote to ensuring each service account was properly protected. We needed an automated process to help us protect these accounts from potential security threats."

Additionally, West Valley School District needed to protect access requests to their network devices. “We recognized the need for users to authenticate when accessing network equipment, including switches, SAN, and security camera servers, yet the means to enforce this authentication remained unachievable,” said Cox.

After searching for an identity security solution, West Valley School District discovered Silverfort and realized it was the right solution for their identity protection needs. “We initially chose Silverfort because they helped us checkmark our cyber insurance policy requirement, but during the demo and POC we found its service account protection capabilities were exactly what we were looking for, “ says Cox.

The Solution

Quick Deployment Led to Insurance Policy Renewal and Compliance Regulations

As a result of deploying Silverfort and applying access policies to all user authentication requests, West Valley School District lowered the pricing of their cyber insurance policy. “By quickly deploying Silverfort across our environments, we added MFA protection to our entire user base and applied security controls to our service accounts. This strengthened the security and functionality of our staff accounts while protecting our service accounts,” said Cox.

> “By improving our security posture with Silverfort, we decreased the cost of our cyber insurance policy.”

In addition to renewing its cyber insurance policy, West Valley School District met educational compliance regulations with the help of Silverfort. “Silverfort played a pivotal role in our compliance journey, ensuring adherence to regulations like FERPA by providing secure access with MFA protection on our educational resources,” stated Cox.

Service Account Protection and Secure Access to Network Devices

It was quickly apparent that Silverfort’s capabilities were exactly what West Valley School District was looking for to address its service account protection gaps. “Once we saw the functionality of Silverfort’s service account protection, we knew we needed this feature as we have 55 service accounts, including several with excessive privileges,” said Cox.

Since implementing Silverfort's service account capabilities, West Valley School District is confident knowing its service accounts are being continuously monitored and protected.

"With Silverfort, we have gained granular visibility into each service account's source, destination, and authentication protocol," said Cox.

> "Even if the service account has privileged access, Silverfort offers us real-time monitoring and protection of these accounts. This capability has been extremely valuable for our overall identity security strategy."

Through Silverfort's seamless integration with Active Directory, West Valley School District has effectively extended MFA protection across all their on-prem network devices, which has bolstered their overall security posture.

"With Silverfort, all network devices are capable of leveraging AD authentications and are protected with MFA. Across all our environments, Silverfort extended MFA protection to over 100+ network switches, 4 firewalls, 4 SANs, server BIOS management systems (iDrac, iLO, etc.), phone systems, Student Information System (SIS), district email, and more," said Cox.

> "Now that we have detailed information regarding the types of authentication (NTLM, LDAP, etc.), we can make informed decisions to limit access or make adjustments to our systems to disable the less secure authentication types."

Before Silverfort, we could not see how our users were authenticating across our environments. Using this data, we have detected and corrected misconfigurations," stated Cox.