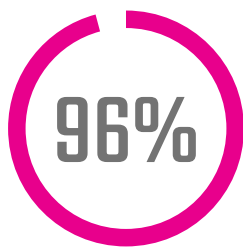# EASTERN CARVER COUNTY SCHOOLS

stealthbits
NOW PART OF **netwrix**

Background

Eastern Carver County Schools comprises 10,000 students and 1,800 staff members at multiple public high schools, middle schools, and elementary schools serving the growing suburbs of Minneapolis/St. Paul, Minnesota area. These schools offer standards-based personalized learning experiences grounded in flexibility for how each individual learns.

96% Teaching staff are excellent or good.
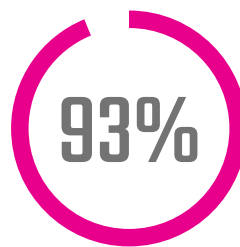
93% Quality of education is excellent or good.

Problem:

Driven by massive increases in data breaches in the industry, Eastern Carver County Schools, over the last 4 years, has engaged in multiple audits and pen tests with external auditors to verify their security posture. Those exercises exposed some weaknesses like the ability of a Red Team to gain access to critical systems EVERYTIME because of over provisioned privileged access. Craig Larsen, Information Systems Administrator at Eastern Carver County Schools reveals, "We knew for a couple years we needed to do something. We already use password managers, and multi-factor authentication products, but the more we looked, the more we needed a privileged access management solution."

Challenge:

Solution evaluators were torn between difficult-to-implement, yet effective privileged access management (PAM) solutions and the relatively-easy-to-deploy (but not as effective) password manager offerings. As Eastern Carver County Schools and Craig were evaluating solutions, the importance of a just-in-time (JIT) privileged access solution rose to the top and narrowed the field of vendors. But PAM solutions tended to result in complicated, elaborate, and expensive projects, all things the limited IT staff wanted to avoid. Soon they came in contact with Stealthbits Technologies and Stealthbits Privileged Activity Manager® (SbPAM), and things changed!

"The important part here is that this is not about privileged accounts which are used by systems, as we now have very complex passwords for these systems and have good processes to manage these unique accounts. What I am talking about are the admins of our systems who have privileges to those systems attached to their accounts. We have tried strategies such as the traditional "A" accounts, but this still leaves accounts with privileges sitting around which can be and are used in places where they shouldn't, resulting in a great big trail for anyone to follow directly into our systems and gain access."

Solution:

From the time Craig and team began evaluating SbPAM, they knew it was different. "We looked at several PAM products, many having been around for a number of years, but they often fall very short when it comes to admins and the accounts they use to get access to systems," said Craig Larsen.

Craig offers the main reasons they deployed SbPAM. "What was so intriguing about SbPAM is that we can truly manage the access to our systems to the level of least privilege. The concept of temporary elevation, or just-in-time access, make so much sense as the admin is granted access on the fly and access is removed when no longer needed. On top of this, you also have the RDP proxy and included the monitoring and logging."

Craig also found other uses for just-in-time access for other systems:

- Network Switch Management
- Camera Access
- VMware vCenter
- Commvault/backup software

"Stealthbits' services were clean, on-time, and under budget," gushes Craig. "Honestly, SbPAM is so simple to install and get running that we probably could have done it ourselves. We would highly recommend SbPAM for anyone looking for a better, easier way to manage privilege accounts."

"Overall we are very pleased with what we are seeing and SbPAM is going a long ways to help us maintain least privilege access for my systems admins."

- Craig Larsen, Information Systems Administrator

NEXT STEPS

To learn more about Stealthbits, visit www.Stealthbits.com

Schedule a Demo
Stealthbits.com/demo

Download a Free Trial
Stealthbits.com/free-trial

Contact Us
info@Stealthbits.com