Simplicity and Effectiveness for this School District

|  |
| --- |
| **New City School District**  New City School District is a large, K-12 school district in the Mountain West that serves nearly 8,000 students.  **Requirements**  As a large school district, New City was on the receiving end of a massive amount of phishing attacks. Their EOP protection was struggling against impersonation and BEC attacks. They needed a solution that prevented malicious emails from reaching the inbox, and one that fits within their limited budget.  **Cloud Suite**  Microsoft 365  **Previous Email Security Solution**  Microsoft EOP |

Background

John Waldman† is the IT Director for New City School District, a large, K-12 school district in a city in the Mountain West.

The district was having difficulties stopping malicious emails, particularly those from spoofed users, from reaching end-user inboxes. “Phishing has just been killing us,” he says. “If we don’t improve our email security, we’re in trouble.”

Waldman had Microsoft EOP in their environment. Despite that, he found that scores of phishing emails were hitting their environment. Malicious emails get through to the inbox. East-west attacks occurred from compromised accounts. Malware and ransomware were of particular concern.

Waldman had several requirements for a new email security solution.

* It needed to be cost-effective. As a public school district, funds were limited.
* A new solution had to do a better job of preventing phishing, particularly those from spoofed accounts.
* It needed to give him insight into all the attacks targeting his network, so he could act accordingly.

“It’s Time To Improve”

EOP caused Waldman a lot of issues.

The major one was internal spoofing. An email will appear to come from a school employee or student. But one or two letters will be off.

“It appears to come from an inside user, but it’s not an inside user,” he says. “They’ll say, hey, are you busy?”

These attacks are difficult to stop. Business Email Compromise attacks (BEC) are rising in popularity and they are difficult to protect against. [Gartner found](https://www.gartner.com/document/3982230) that BECs increased by nearly 100% in 2019 and through 2023, predicts that BEC attacks will continue to double each year, at a cost of over $5 billion to its victims.

BEC attacks are popular because they are simple to execute. By spoofing a trusted user it requires no malware or malicious URL to convince a recipient to share valuable information or send significant amounts of money.

“They’ll say, ‘I need a favor from you,’” says Waldman. “Give me a call or send me your number. And it’s always a gift card thing, right?

Gift cards are a particular BEC-related scourge. Gift card BEC scams are actually quite popular. It works when someone, pretending to be a higher-up, asks the end-user to get a gift card and send it to them. Gift cards are harder to track than other forms of payment. The [Internet Crime Complaint Center tracked a 1,240% increase](https://www.ic3.gov/media/2018/181024.aspx) in 2018 of these types of attacks.

He was also concerned about student accounts. He noticed how hackers used students as an avenue into the larger organization. “They get into student accounts and then they horizontally navigate across to other platforms and hopefully hit an elevated account and boom, get some money,” he says.

Securing sensitive data is incredibly important. For one, school districts are one of the most targeted sectors. [According to one report,](https://www.tripwire.com/state-of-security/security-data-protection/successful-ransomware-attacks-on-education-sector-grew-388-in-q3-2020/) ransomware attacks on schools increased by 388% in the third quarter of 2020. In 2020, [1,681 schools and universities were hit with ransomware, accounting for nearly 75% of all reported ransomware cases in the US](https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/).  And, according to the Multi-State Information Sharing and Analysis Center (MS-ISAC), a federally-funded organization that helps improve cybersecurity for state and local governments, [ransomware attacks on K-12 schools are projected to increase by 86% in 2021.](https://www.washingtonpost.com/politics/2021/07/12/cybersecurity-202-schools-are-another-prime-ransomware-target/)

Educators hold tons of sensitive information about students. From birthdays to allergies, medical conditions to family histories, educators are tasked with ingesting this information for all their students and then protecting it from getting out. Attackers are looking for all the rich data that schools hold. Social security numbers; addresses; medical information—it’s all there. The law that governs it is called the Family Educational Rights and Privacy Act, or FERPA. Since the law was first introduced in 1974, a lot has changed. Now, teachers and educators have tons of tools at their disposal to share information. Leakage of that data exposes schools to violations of FERPA, among other issues.

When thinking of a new email security solution, Waldman needed better security. But he also needed it at a reasonable price point.

“You Solved the Phishing Problem for Us”

First, with a limited budget, Waldman was concerned about pricing. After he heard from a few friends in the industry about Avanan’s special education pricing, he was intrigued. Its customized pricing makes for the efficient protection of all on campus.

Then, on a POC, the technology made Avanan a perfect match.

First, he saw how Avanan handles BEC attacks. Avanan has all the protections needed to stop BEC attacks. That includes machine learning algorithms that combine with a role-based, contextual analysis of previous conversations to identify what ATP had been missing.

Deployment-day analysis of one year’s worth of email conversations to build a trusted reputation network. It includes the scanning and quarantining of internal email and files in real-time, protecting against east-west attacks and insider threats.

“This is fantastic,” he said.

Beyond that, he was impressed with the easy-to-use reporting features. In the Mail Explorer dashboard, Avanan’s True AI will show you exactly why it made the decision it did.

“Before, I had to dig really deep to find out information,” he says. “Now, it’s all in front of me, easy-to-use, digest, and take action with.”

Between attractive pricing, reliable protection and ease of use, Avanan was a home run for Waldman. “It’s been all I could ask for,” he says. “You guys really did solve the phishing problem for us.”

“Now, We Know Our Email is Fully Protected”

John Waldman is the head of IT for a large school district. Within their Microsoft EOP environment, his staff and students were being inundated with phishing and Business Email compromise attacks.

He needed a solution that did a better job of stopping BEC attacks, and he needed a solution that could do so at a price that fit his budget. Beyond that, he required easy-to-use features that saved him time and frustration.

“With Avanan,” he says, “now, we know our email is fully protected.”

†Company and individual names have been changed, but are available as a reference customer.