

CASE STUDY

How a K-12 School District Validates Its Defenses Between Annual Pentests with Picus

A US public school district protects students, staff and systems with a small security team and a budget that covers one penetration test a year. It runs two EDR platforms side by side, and the security specialist’s worry was simple: what isn’t alerting?

With Picus Breach and Attack Simulation (BAS), the team tests endpoints and the network continuously against current threats, including campaigns aimed at education, and deploys the vendor-specific fixes Picus provides. Simulations caught an older endpoint stopping fewer than 40 percent of attacks, and a short Autonomous Penetration Testing trial found an account exposed to Kerberoasting, since fixed and re-tested.

Industry:

Education (K-12)



Products:

- Breach and Attack Simulation (BAS)
- Autonomous Penetration Testing

About the company

The organization is a US public K-12 school district. Its small security team protects students, staff and district systems under an annual cybersecurity audit, with NIST-aligned reporting to district leadership and the school board. It has run Picus since 2024.

Problem:

Two EDRs, but What Gets Through?

“One of the fears I have when we see alerts is what is it not alerting? What are we not seeing? Because we’ve had times where one tool will catch something but the other didn’t even alert on it. And vice versa,” said the Information Security Specialist.

The district runs two EDR platforms side by side, along with a next-generation firewall. Each produces its own alerts, and neither shows what the other missed. Between annual penetration tests, there was no consistent way to confirm which attacks would be blocked, which would be seen, and which would get through.

The team focused on two priorities:

- Test both EDRs and the firewall against current, real-world techniques continuously, not once a year.
- Turn each finding into a fix the team can deploy, re-test and show to leadership.

Challenges and Results:

- Two EDRs side by side, with no proof of what each catches**
→ Continuous endpoint and network simulations against both
- One pentest a year, set by budget**
→ Continuous validation between annual assessments
- Weak endpoints hidden in the fleet**
→ Older endpoint found stopping under 40% of attacks
- CVE patches with no second line of defense**
→ Vendor-specific rule deployed alongside the patch
- Active Directory exposure untested between pentests**
→ Autonomous pentesting found a Kerberoastable account, fixed and re-tested
- New threat reports with no quick way to test them**
→ AI Threat Builder turns threat intel into simulations
- Findings hard to show to leadership**
→ Clear findings with fix verification through retesting, ready for the executive sponsor

Solution:

Testing Both EDRs Continuously, Fixing What Gets Through

Rather than adding another security control tool to the stack, the team used **Picus Breach and Attack Simulation (BAS)** to test the ones it already ran.

Picus BAS safely runs real attacker techniques against the controls already in place across Windows, Linux, macOS and Kubernetes environments, with every result mapped to MITRE ATT&CK. The **Picus Threat Library** is continuously updated by Picus Labs with new threats, and Picus AI Threat Builder turns new threat intelligence into custom simulations in minutes, so the team can test against what attackers are doing right now. For each gap, the **Picus Mitigation Library** provides a ready-to-apply, vendor-specific fix, and the team re-runs the test to confirm the gap is closed.



"Y'all's documentation is really good. It helped me catch up to speed pretty quick." The Information Security Specialist

Outcome:

Findings the Team Could Fix, Re-Test and Show

Picus detection analytics correlate EDR and firewall alerts with each simulation, so the team can see which attacks were blocked, which were only detected or logged, and which were missed entirely.

With that visibility, the first runs revealed a wide gap in protection between endpoints. An older Windows 10 machine stopped fewer than 40 percent of simulated attacks and missed almost every defense evasion technique. A newer endpoint blocked all of them, plus the file encryption step, though privilege escalation still got through.

Finding gaps is only half the job. Each one feeds a fix-and-retest loop, and the same loop works for endpoint gaps and new vulnerabilities. For a Notepad++ CVE, the team ran the simulation, deployed the matching vendor-specific rule, and updated the software. **"It was just kind of more of a double coverage. You had a preventative control in place along with your actual patching,"** the Information Security Specialist said.

The results are also easy to share. PDF summaries go to leadership and CSV detail to the technical team, and the specialist has walked the executive sponsor through a full cycle live: simulate, deploy the rule, re-run, confirm. **"I can deploy it, let it run, show we patched and it's no longer exploitable."**



"Being able after the fact to go and look at, okay, this is where we could have prevented this. This is what we can put in place through Picus to be able to prevent it," the Information Security Specialist said. *For a small district team with one pentest a year, that is the difference between hoping a control works and showing it does.*



Picus Security, a leading exposure validation company, **proves what attackers can exploit and what your defenses stop**, then closes real gaps with ready-to-deploy fixes and re-validates to confirm, at the machine speed today's AI threats demand. The Picus Platform spans [Breach and Attack Simulation](#), [Autonomous Penetration Testing](#) and [Exposure Validation](#), unified by [Picus Swarm](#), a swarm of AI agents that runs the whole validation loop continuously with human oversight. With 75+ integrations, it reaches across on-prem, hybrid cloud, and endpoint environments. Trusted by many Fortune 500 enterprises, Picus was named a 2026 Gartner Peer Insights Customers' Choice for Adversarial Exposure Validation and is recognized as an Innovation Leader in the Frost Radar for Automated Security Validation.