

CASE STUDY**Industry:** Dental Healthcare**Services:** Cybersecurity Services

How Endpoint Security Was Strengthened and Cyber Insurance Costs Reduced for Dental Group

After moving to Perimetra, Dental Group gained stronger endpoint detection, caught threats early, and improved insurability.

Executive Summary

Dental Group was operating with basic antivirus software while its billing team faced credential phishing attempts that could have exposed sensitive accounts and disrupted financial workflows. Perimetra upgraded the practice to EDR coverage, improving detection visibility and modernizing endpoint security. Within the first week, the new controls caught three phishing attempts, and the stronger posture helped lower the client's cyber insurance premium.

Challenges

- Dental Group relied on basic antivirus, leaving endpoints with limited visibility into modern phishing activity.
- Credential phishing attempts targeted the billing team, increasing the risk of stolen logins and disrupted financial workflows.
- The practice needed stronger security controls that could satisfy growing cyber insurance expectations.
- Leadership lacked confidence that legacy endpoint protection could identify threats quickly enough to reduce risk.
- Without modern detection coverage, the organization faced avoidable exposure around sensitive billing operations.

Perimetra's Approach

Key Actions:

- Perimetra assessed the client's existing endpoint protection baseline and identified gaps in legacy AV coverage.
- The team replaced basic antivirus with EDR coverage to improve detection depth across user devices.
- Endpoint monitoring was configured to surface suspicious credential theft activity affecting billing staff.
- Perimetra prioritized rapid rollout so new controls could begin protecting high-risk users immediately.
- The upgraded security posture was documented clearly to demonstrate stronger controls to the client's insurer.

Solutions

- Modernized endpoint protection with stronger detection and response capabilities than the previous AV setup.
- Expanded visibility into suspicious activity, helping the practice identify threats before accounts were compromised.
- Focused protection around phishing-driven credential theft risks affecting financially sensitive roles.
- Improved security maturity in a way that supported both day-to-day protection and insurer confidence.

The Result

- Within the first week, the new coverage caught three credential phishing attempts targeting the billing team.
- The practice gained earlier warning of phishing-related activity and reduced exposure to account compromise.
- Cyber insurers recognized the stronger endpoint posture and reduced the client's premium.
- Leadership had greater confidence that endpoint threats were being detected with more rigor than before.
- The organization moved from reactive baseline protection to a more resilient, insurable security posture.



"We switched from basic AV and within the first week Perimetra caught three credential phishing attempts targeting our billing team. Our cyber insurer reduced our premium after seeing the EDR coverage."

Sandra C.

Practice Manager, Dental Group

Strengthen Security Before Threats Escalate

See how modern endpoint security can reduce risk, improve insurability, and protect your highest-value users.

[Schedule A Consultation](#)