

SAMPLE DELIVERABLE

24/7 Threat Monitoring: Monthly Summary

What was watched, what was blocked, and what mattered: a sample 30-day monitoring report.

SAMPLE Fictional demonstration data · Prepared by Arcline

PREPARED FOR

Brightwell Dental Group

Dental / healthcare (HIPAA-covered entity) · 3 locations · 38 staff · 5 servers

Monitoring period: 2026-07-01 to 2026-07-31 · All data stays on the practice's own infrastructure

01 What we watch

COVERED	WHAT'S MONITORED
Endpoints (38 workstations)	Endpoint protection, patch status, and integrity of critical files
Servers (5)	System and authentication logs, backup job status
Network (3 sites)	Firewall, VPN, and intrusion attempts at the edge
Email	Phishing and spam filtering, spoofing (DMARC) reports
Critical data	Access to the practice-management database and patient records

02 The month in numbers

12,480 SECURITY EVENTS COLLECTED	214 THREATS BLOCKED AUTOMATICALLY	3 INCIDENTS INVESTIGATED
0 CONFIRMED COMPROMISES	4 min AVG. ALERT-TO-TRIAGE TIME	99.98% MONITORING UPTIME

03 Notable events

The events this month that involved real activity, in chronological order. Everything else was handled automatically by the monitoring stack.

2026-07-03 02:14	Brute-force attempt against the VPN portal HIGH ACCESS Repeated failed sign-in attempts from a single overseas IP targeting the remote-access portal. ACTION TAKEN Blocked after three attempts; source address geo-blocked at the firewall. No account affected.
2026-07-07 11:40	Phishing email reported by the front desk MEDIUM EMAIL A staff member reported a suspicious email claiming to be from a supply vendor. No one clicked the link. ACTION TAKEN Email quarantined, sender domain flagged, and a reminder sent to all staff.
2026-07-11 19:22	Malware quarantined on a workstation MEDIUM MALWARE Endpoint protection detected and blocked a downloader-style payload on one front-office workstation. ACTION TAKEN File quarantined; workstation scanned clean; no data accessed.

2026-07-18
09:05

Critical file change alert (investigated) LOW

INTEGRITY An alert fired when the practice-management backup file changed outside the normal schedule.

ACTION TAKEN Verified as the legitimate nightly backup job. No action needed.

2026-07-23
15:50

Ransomware-style behavior blocked HIGH

RANSOMWARE Endpoint protection blocked an attempt to encrypt files in bulk on one workstation (the pattern ransomware uses).

ACTION TAKEN Process terminated; workstation isolated and scanned; confirmed no spread to other systems.

2026-07-29
12:00

Monthly patch push completed INFO

MAINTENANCE Scheduled security updates deployed across all 38 endpoints and 5 servers.

ACTION TAKEN Completed with zero failures. Patch report filed.

04 Response metrics

METRIC	VALUE
Average time from alert to triage	4 minutes
Average time from alert to resolved	22 minutes
Alerts that required human review	14
False positives (investigated, no action needed)	11
Alerts escalated to the practice	2

FROM THE ANALYST

This was a quiet month for Brightwell Dental Group, which is exactly what a monitoring report should look like: most threats are stopped automatically before anyone notices. The two events worth knowing about (the VPN brute-force attempt and the ransomware-style behavior on one workstation) were both blocked, investigated, and confirmed contained. If you have questions about any event in this report, or want to adjust what we watch, just reply. This is a summary of the full event log, which is available any time.