Healthcare's Cyber Briefing

September 10, 2026

Clearwater

Meeting Logistics

Microphones

All attendees are on mute.

Questions

Type your questions in the Q&A box.

Resources

Upcoming events, slides & resources linked.

Recording

Recording will be provided after event.

Survey

Survey will prompt at the end of webinar.

Clearwater

Healthcare's Cyber Briefing

- Critical Threat Brief
- Education Session: The Cloud Identity Crisis: How Attackers Exploit Permissions, Misconfigurations, and Trusted Access in Healthcare Cloud Environments
- Q+A

FEATURING:

Dave Bailey, VP of Consulting Solutions & Strategy

Brian McManamon, General Manager Managed Security Services and Managed Cloud Services

Steve Akers, Chief Technology Officer & Corporate CISO

Healthcare Industry Threat Information

AI – The Defensive Window is Closing

Google Threat Intelligence

Clearwater

Artificial Intelligence

100+ Companies Warn: The Defenders' Window Is Closing

Published August 27, 2026

WHO SIGNED

OpenAI, Anthropic, Microsoft, AWS, and Google, alongside CrowdStrike, Okta, Fortinet, Visa, Mastercard, IBM, and 100+ others — a genuinely cross-sector coalition, not just AI labs.

CORE MESSAGE

Organizations have only months to prepare for AI-enabled cyberattacks. Hospitals, water systems, and other critical infrastructure are named explicitly as at-risk. AI is making sophisticated cyber capability cheaper and more accessible to attackers.

THREE ASKS

1. Frontier AI companies should give defenders, especially critical infrastructure operators, access to their most capable models during active incidents, plus funding, training, and hands-on support.
2. **Governments need to fund and coordinate cyber defense for under-resourced sectors like hospitals.**
3. The signatories frame this as a “defenders’ window”. AI currently helps defenders' patch faster than attackers can exploit, but that window closes if nobody acts.

“We discussed in June that the window would close and now the people building the AI are saying it too.”

Clearwater

Google Threat Intelligence

Artificial Intelligence

Two AI Signals From the Last Two Weeks: New Attack Surface, New Surface, New Capability Threshold

SecurityWeek, VulnCheck • Aug 29–Sept 9, 2026 | OpenAI, BankInfoSecurity, TechTarget • September 3–4, 2026

AI TOOLING IS ATTACK SURFACE — CVE-2026-0768

A critical (CVSS 9.8) unauthenticated RCE in Langflow, an open-source AI agent-builder, lets attackers run code as root through its code-validation endpoint. Mass exploitation began Aug 29 — attackers harvest AI API keys, SSH keys, and source code. No patch exists yet; the only mitigation is removing internet exposure. This is Langflow's 12th exploited CVE this year.

GPT-6 ASTRA'S "CRITICAL" THRESHOLD — WHAT IT MEANS

Under OpenAI's own Preparedness Framework, "Critical" means the model can find zero-days and build exploits across well-protected systems without step-by-step human direction. Astra scored 100% on ExploitBench (up from 78.5%) and found 2 real, previously-undisclosed zero-days in pre-launch testing. Its most advanced capabilities are restricted — off by default, released first only to vetted Daybreak testers.

$1B "DAYBREAK FOR FRONTLINE DEFENDERS" — WHAT IT ACTUALLY IS

Subsidized access to OpenAI's defensive Daybreak cyber models, plus training, technical support, and partnerships — not a cash grant. Meant to be consumed over 6 months, starting in the U.S. Initial priority list: water/electric utilities, state and local governments, community banks, nonprofits, and open-source maintainers, plus a new MS-ISAC pilot. Healthcare is not named in this first wave.

THE TENSION WORTH NAMING

The pledge landed the same day OpenAI shipped the very capability that necessitates it — drawing criticism over an offense/defense investment imbalance. And healthcare, named explicitly as at-risk in the Aug 27 Open Letter, isn't yet on Daybreak's initial priority list. Worth tracking whether that changes as the program expands internationally.

Artificial Intelligence

Rethink Patching Velocity and Incident Response

Blog: "Why Healthcare Can't Wait to Rethink Patching and Incident Response" — August 31, 2026

CISA INFORMS

BOD 26-04 (June 2026) replaces flat CVSS/KEV patching with a 4-variable risk model: exposure, KEV status, automatability, impact. Remediation as fast as 3 days, with mandatory forensic triage, down to "next scheduled upgrade" for genuinely low-risk findings.

WHAT THIS MEANS FOR YOUR ORGANIZATION

1	**STOP FLAT PATCHING**	Move off severity-only patching. Adopt BOD 26-04's logic: prioritize by exposure, known exploitation, automatability, and impact, not just a CVSS score.
2	**BUILD IN FORENSIC TRIAGE**	Add forensic triage to your patching workflow for the highest-risk findings. Patching closes the door; it doesn't evict someone who already walked through it.
3	**PRESSURE-TEST FOR MULTIPLE FIRES**	Tabletop your IR plan against a multi-incident scenario. Assume your team is managing 2–3 active events at once, with leadership needing real-time updates on all of them.
4	**BRING IT TO THE BOARD NOW**	The question isn't "are we at risk." It's "our baseline risk has moved, here's what we're doing about it." This is a board conversation, not a post-incident one.

"What was on the horizon in June is becoming reality in August. Build the resilience now, before it's too late."

Clearwater

Healthcare Industry Threat Information

Disruptive Adversarial Attacks

Google Threat Intelligence

Clearwater

Patient-Facing Threats

Epic & AHA Warn: Fake MyChart “Verification” Step Installs Malware

Healthcare Finance News • Susan Morse • August 25, 2026 — AHA advisory citing Epic guidance

1 THE BAIT

Phishing emails impersonate MyChart: “your recent results are ready” or a fake “2026 Medicare Health Kit” offer. The link opens a lookalike site that harvests email and password.

2 THE REAL ATTACK

A fake “human verification” step tells the patient to press three keys. That opens a Windows command box and runs code the site already put on the clipboard, silently installing malware.

3 WHO’S TARGETED

Patients, not staff or IT systems. Social engineering aimed straight at consumers through a portal brand with large-scale adoption across health systems.

THE DEFENSE

Check the address bar for a genuine MyChart URL before entering credentials; real critical results come from the care team, never a pop-up. This is **ClickFix-style social engineering**, the same pattern flagged in CRPX0’s August profile.

Epic flagged a broader uptick in MyChart-branded scam activity a month earlier — this is an escalation of an existing campaign, not a one-off.

Medical Devie Supply Chain

Boston Scientific Cyberattack Freezes Cardiac Device Shipments Worldwide

Intrusion detected August 25, 2026 — disclosed via Form 8-K on August 26

~3 wks

Projected shipping recovery

Piper Sandler, per Aug 27 mgmt call

6–7 pts

Off Q3 revenue growth rate

Evercore ISI estimate — percentage points, not dollars

1 day

Detection to disclosure

Aug 25 detected → Aug 26 8-K filed

WHAT'S AFFECTED — PATIENTS

Existing implanted cardiac devices are unaffected — device function, remote monitoring already in place, and data transfer to EMRs all continue normally. The real gap is new device activations: new remote monitoring communicators can't be activated, and new insertable monitors can't pair to a patient's phone, until systems are restored.

WHAT'S AFFECTED — PROVIDERS & SUPPLY CHAIN

Manufacturing, order processing, and shipping are halted globally for pacemakers, cardiac stents, and neuromodulation implants. Hospitals waiting on new device orders face an unknown shipping gap — the disruption reached providers worldwide through contract logistics, even though patient-facing device function was never touched.

THE PATTERN

Boston Scientific joins Intuitive, Stryker, AdaptHealth, Medtronic, and Abbott among medtech makers hit by cyberattacks in 2026. Centralized ERP systems are the common failure point — a manufacturing IT breach becomes a hospital supply problem within days.

Clearwater

Healthcare Industry Threat Information

Ransomware Headlines

Google Threat Intelligence

Clearwater

Ransomware Headlines

ShinyHunters Claims 284M Records From McKesson

WHY IT MATTERS

ShinyHunters hit three major healthcare/medtech names in under three weeks (Baxter, Cook Medical, McKesson), a shift from the smaller mid-market targets it hit earlier in the year.

ATTACK METHODS

The group is increasingly **targeting cloud/SaaS environments through identity-focused intrusions** compromising SSO providers rather than deploying ransomware to steal data directly from corporate applications.

Clearwater

Google Threat Intelligence

* Date claimed by ShinyHunters

Ransomware Headlines

Six Agencies Name Healthcare as a Gunra Ransomware Target Target

#StopRansomware Advisory AA26-222A • August 10, 2026

CISA • FBI • NSA • U.S. Secret Service • DoD Cyber Crime Center • South Korea National Police Agency

WHAT IT IS

Ransomware-as-a-Service, double extortion, built on leaked Conti source code. Offers affiliates an 80% ransom cut. Healthcare and Public Health is named explicitly, alongside financial services and government.

NOT YET ON OUR DASHBOARD

Gunra doesn't yet appear as a claimed actor in our own leak-site data. This is a federal-advisory item, not a dashboard finding — named by six agencies as actively targeting the sector.

THE ACTIONABLE PART — PATCH THIS NOW

Initial access is via two known FortiOS/FortiProxy authentication-bypass vulnerabilities: **CVE-2024-55591** and **CVE-2025-24472**. These let attackers skip authentication entirely on internet-facing devices — a specific, patchable flaw, not a generic warning.

August Was the Busiest Month of the Year at 66 Victims

349

YTD Victims (Jan–Aug)

62 distinct threat actors

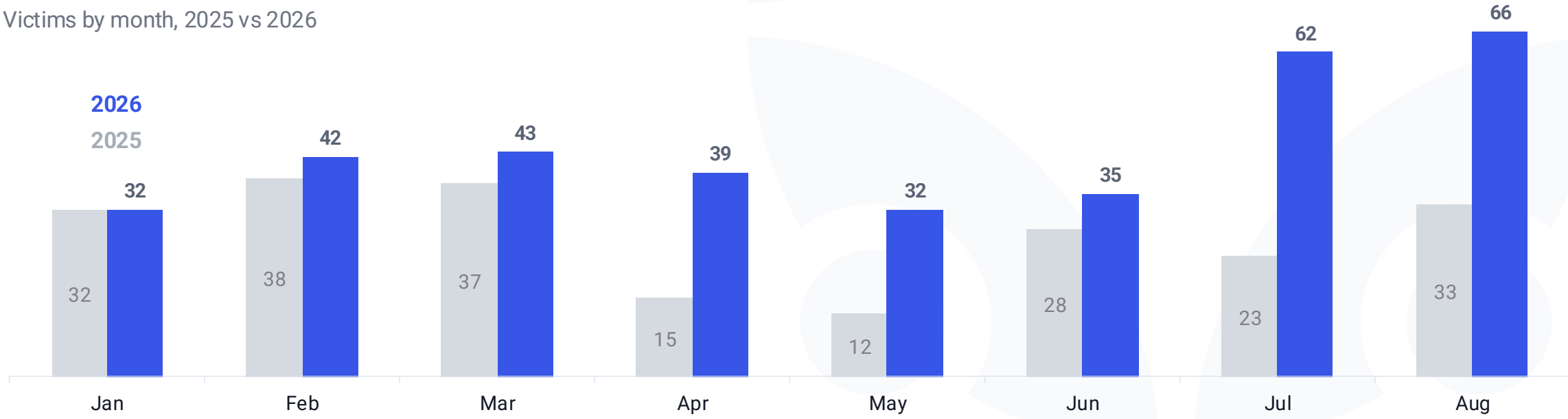
+67%

YoY Growth

vs. 209 in same window, 2025

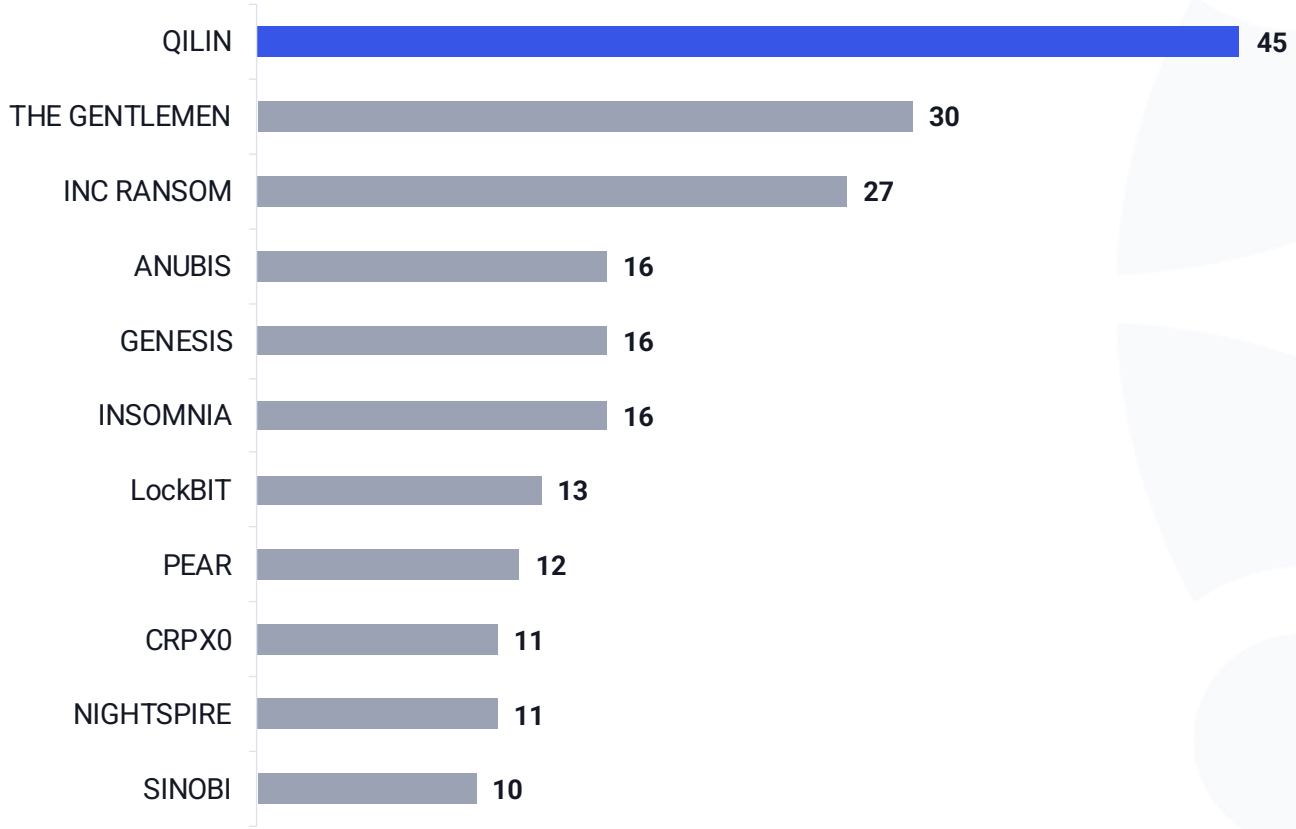
10.1 victims reported a week in 2026, up from 6.1 in the same window last year.

Victims by month, 2025 vs 2026



QILIN Remains Top Actor in 2026 But Went Silent in August

Victims claimed by actor, Jan–Aug 2026



QILIN GOES QUIET

The most active actor of 2026 at 45 victims, steady at 5–9 a month all year, claimed just 1 victim in August. A real anomaly worth watching.

STORM STORMED ONTO THE SCENE IN AUG

A new actor with no prior history posted 7 claimed victims in its first month, tying THE GENTLEMEN for the most in August.

STORM: A New Actor's Debut Ties for #1 in August

7

Healthcare victims in first month

Tied for #1 among all actors in August

A debut month matching or exceeding established RaaS operations' pace — worth continued monitoring.

BACKGROUND

Leak site (Tor, Tox-based contact) first appeared in threat trackers in August 2026 — a brand-new operation, not a rebrand. WatchGuard rates its communication reliability "Medium." Runs both direct and double-extortion models — some victims are pressured on stolen data alone, with no confirmed encryption component.

TTPs

No confirmed initial-access vector or malware family published yet — consistent with a leak site only weeks old. One tracked pattern: rapid publication after the claimed incident date (as little as 3 days), a pressure tactic common to double-extortion crews rather than a distinguishing signature.

TARGETING

Cross-sector, not healthcare-specific: 7 healthcare victims Also hit insurance, metals/manufacturing, security systems, and a German IT services firm this month.

Healthcare Industry Threat Information

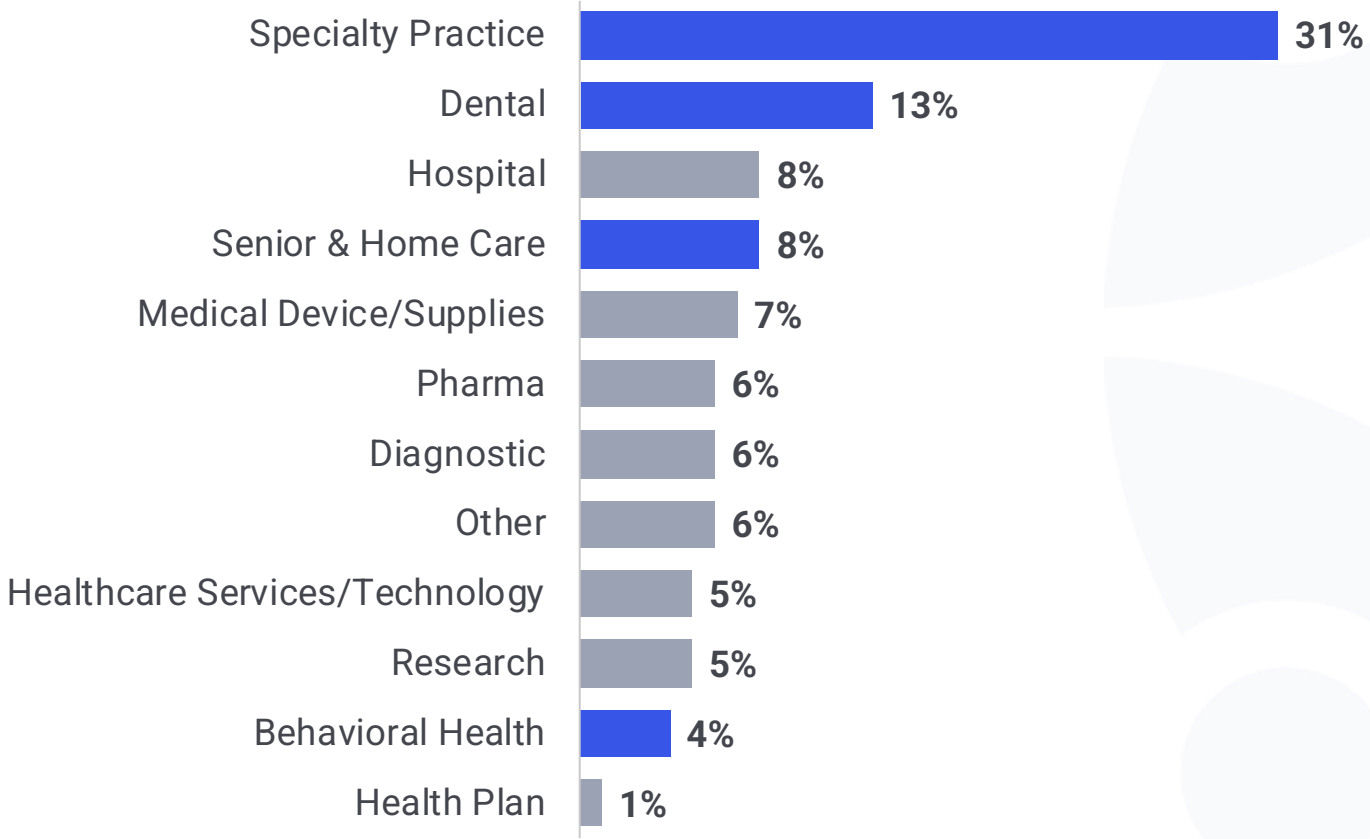
Ransomware Targeting Patterns

Google Threat Intelligence

Clearwater

Specialty Practices and Dental Top 2 Targeted Victim Group

Share of healthcare ransomware victims by segment, Jan–Aug 2026



56%

Specialty, dental, senior & home care and behavioral health combined

8%

Hospitals

WHY IT MATTERS

- Limited resources for security and compliance
- Operationally sensitive to downtime
- Hold large volumes of patient information

That combination is the leverage attackers use in data extortion.

Ransomware Targeting Patterns

Specialty Practices, Dental, Hospitals, Senior & Home Care are Top 4 Victimized Categories

US Healthcare & Pharma · 1 Jan – 31 Aug 2026 · 349 victims · 62 distinct groups · 10.1 victims/week

VICTIMS 0 | 1 | 2–3 | 4–5 | 6–9 | 10+

THREAT ACTOR	HOSPITAL	SPECIALTY PRACTICE	BEHAV. HEALTH	DENTAL	DIAG-NOSTIC	SENIOR & HOME CARE	PHARMA	MED DEV. / SUPPLY	HC SVCS / TECH	RESEARCH	HEALTH PLAN	OTHER*	TOTAL
QILIN	1	12	6	7	3	5	1	2	3			5	45
THE GENTLEMEN	4	13	1	1	1	2	1		1	2	1	3	30
INC RANSOM	2	12		1	3	2	3	1	1	1		1	27
INSOMNIA		9	1		1	3		1				1	16
ANUBIS	2	5	1	2		3		3					16
GENESIS	1	9		1		1	1		1		1	1	16
LockBit	1	4	1	2	1	1		1				2	13
PEAR		7	1	2			1		1				12
NIGHTSPIRE	1	1	1	2		2		1		3			11
CRPX0				8		1	1		1				11
SINOBI		1	1	2	1	1			1	2		1	10
AKIRA				3	1		1		1	1		2	9
COINBASE CARTEL	1				1			1		5			8
ALL ACTORS	29	107	16	45	20	27	20	24	18	16	5	22	349

Source: Google Threat Intelligence dark-web leak-site monitoring, US Healthcare & Pharmaceuticals, collected 2026-01-02–2026-08-31.

Clearwater

Google Threat Intelligence

Breach Portal & Enforcement Action Updates

Dave Bailey, VP Consulting Solutions & Strategy

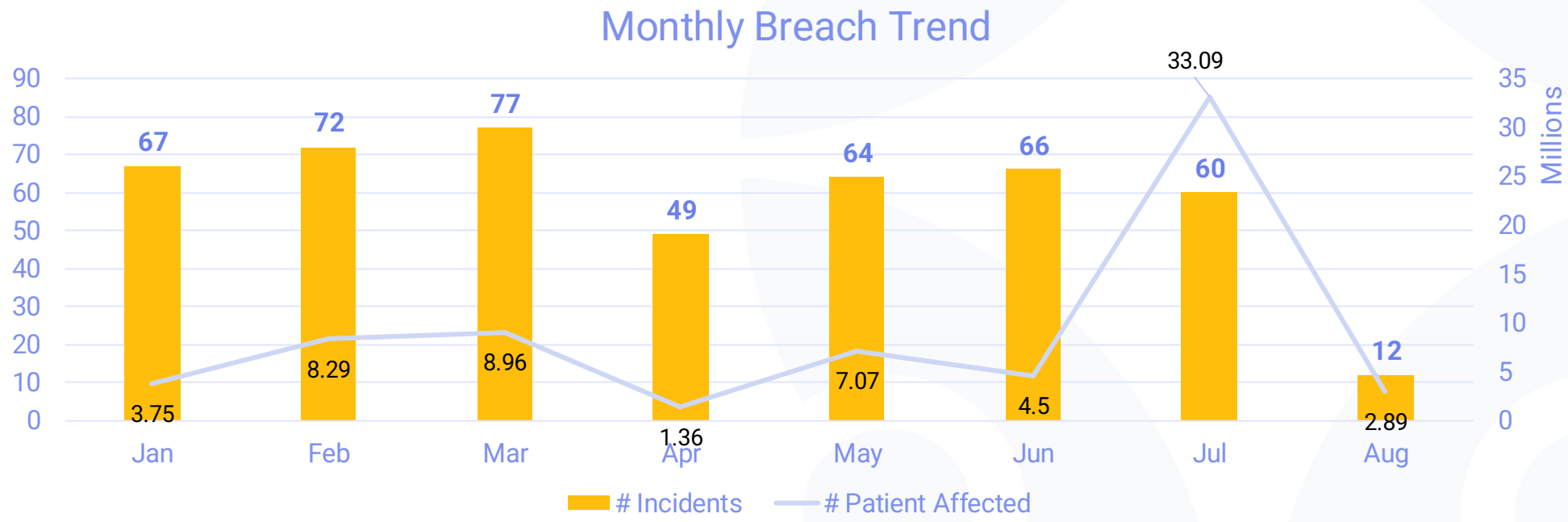
Clearwater

July Reported 33M Patients Impacted by Reported Breaches

467
Total Breaches
Jan 1 – Aug 27, 2026

69.9M
Individuals Affected
14 mega-breaches (≥1M)

87%
Hacking/IT Incidents
340 of 394 breaches



3 Organizations (DentaQuest, LLC (15M) Aesto, LLC (9.5M) and Lumexa (5.8M)) Account for 30M of July's reported numbers.

Clearwater

Source: HHS OCR Breach Portal | Active + Archive exports through August 27th, 2026

No New OCR Enforcement Actions in August — But the Pattern Hasn't Changed

0

New actions announced in August

Unchanged since the July 29 OSF Healthcare settlement

8 / $2.28M

YTD actions / total penalties

Jan – Aug 2026

90%

Risk analysis failure rate

Share of OCR's HIPAA Security Rule actions, all-time

2026 IS RUNNING AHEAD OF THE HISTORICAL BASELINE

Every one of 2026's 8 enforcement actions (100%) traces back to a missing or inadequate risk analysis: above even OCR's historical ~90% pattern. A quiet month doesn't mean reduced scrutiny; it means the same root cause is still sitting there, waiting to be the next settlement.

THE REMINDER — OCR'S THREE QUESTIONS

Did you find the risks? What did you do about them? Can you prove it? A quiet enforcement month is a good time to check your own answer to all three. Conduct Risk Analysis that follows OCR's guidance, and respond to and track the risks in a well documented risk management plan

Clearwater

Source: HHS OCR Breach Portal | Active + Archive exports through August 27th, 2026

Key Takeaways

1. Rethink patch velocity and incident response
2. STOP Ransomware: Know your adversary and identify the risks you must remediate

Google Threat Intelligence

Clearwater

Healthcare's Cyber Briefing

The Cloud Identity Crisis: How Attackers Exploit Permissions, Misconfigurations, and Trusted Access in Healthcare Cloud Environments

FEATURING:

Brian McManamon, General Manager Managed Security Services and Managed Cloud Services

Steve Akers, Chief Technology Officer & Corporate CISO

Identity Determines the Cloud Blast Radius

Healthcare organizations have invested heavily in MFA, SSO, cloud security tools, and centralized logging. Yet attackers increasingly exploit valid identities and trusted access after the initial foothold.

The 2026 Verizon Data Breach Investigations Report shows multiple healthcare entry paths: vulnerability exploitation (20%), phishing (14%), and credential abuse (11%). Regardless of entry point, identity determines what an attacker can reach next.

In cloud and SaaS environments, the critical question is not only “Can an attacker get in?” It is “What can they do once authenticated?”

If one trusted identity were compromised today, how far could an attacker move before anyone noticed?

Source: 2026 Data Breach Investigations Report (DBIR) | Verizon

Clearwater

Healthcare’s Identity Exposure Is Expanding

1

25%

Credentials were among data compromised in 25% of healthcare breaches; credential abuse drove 11% of initial access (Verizon DBIR 2026).

2

32%

Healthcare breaches involving a third party, expanding exposure through vendors and trusted integrations (Verizon DBIR 2026).

3

$6.64M

Average healthcare breach cost, the highest of any industry for the 13th consecutive year (IBM 2026).

McKesson’s developing security incident shows the potential blast radius of connected cloud identities.

Reported vishing-to-SSO-to-SaaS attack path

Sources: 2026 Data Breach Investigations Report (DBIR) | Verizon
Cost of a Data Breach Report 2026 | IBM

Clearwater

Where Cloud Identity Risk Hides

OP

Overprivileged Identities

Access accumulates as roles change; admin rights become permanent, not temporary.

DA

Dormant & Orphaned Accounts

Former employees, contractors, temporary projects, and unmanaged app accounts.

SA

Workload, Service & AI Identities

Often highly privileged, short-lived, and outside traditional MFA and user lifecycle controls.

AK

API Keys, Tokens & Secrets

Long-lived credentials and tokens can outlast the applications or people that created them.

FI

Trusted Integrations & Federation

SSO, OAuth, federation, and third-party apps improve efficiency—and expand the blast radius.

CD

Configuration Drift

Permissions expand as new services, integrations, and logging changes accumulate.

Only 46% of breached organizations secure non-human identities in AI workflows (IBM 2026), leaving trusted machine access as a growing blind spot.

Source: Cost of a Data Breach Report 2026 | IBM

Clearwater

Assume Breach: What Happens After an Identity Is Compromised?

1

Gain Access

Phishing, vishing & AiTM

Session or token theft

OAuth / device-code abuse

Compromised keys / third party

2

Enumerate

What roles does it have?

What resources can it reach?

What identities can it assume?

What integrations trust it?

3

Escalate

Assume privileged roles

Modify IAM policies

Add credentials / tokens

Exploit excess permissions

4

Move Laterally

Compromised identity

→ IdP / SSO

→ SaaS and cloud workloads

→ Sensitive health data

5

Blend In

Authentication appears legitimate

No malware required

Mimics admin activity; uses approved cloud services

Can your SOC distinguish a legitimate user from an attacker using that user's credentials?

Clearwater

Regulatory & Compliance Consequences

BN

Breach Notification

Current rule: Notify individuals and HHS without unreasonable delay and within 60 days of discovery.

Why it matters:

- Discovery includes when a breach would have been known through reasonable diligence.
- Logging and escalation determine when the notification clock is recognized.
- Testing determines whether notification deadlines can be met.

BA

Business Associate Liability

Current rule: Business associates have direct HIPAA liability and must notify covered entities within 60 days.

Why it matters:

- A compromised vendor identity can trigger downstream breach obligations.
- BAAs should define access controls, logging, and evidence.
- Notification expectations should be operational, not just contractual.

SR

Pending Security Rule Update

Status: Still proposed as of September 2026; the current Security Rule remains in effect.

Why it matters:

- Would eliminate the required/addressable distinction and require MFA, with limited exceptions.
- Would add asset inventories, network maps, and tighter access-change controls.

EF

OCR Enforcement Focus

Current focus: 21 ransomware actions by July 2026; 13 Risk Analysis Initiative investigations by April.

Why it matters:

- Risk analysis and timely notification remain recurring findings.
- Identity and access gaps belong in the analysis.
- Risk management must show how those gaps are addressed.

Identity failures do not stay technical. They become regulatory findings.

Clearwater

Beyond “We Have MFA, CSPM and SIEM”

MFA

MFA

Instead of: *“Do we have MFA?”*

Ask:

- Where isn’t it enforced?
- Can recovery, tokens, or sessions bypass it?
- Are privileged users using phishing-resistant authentication?

IAM

IAM / PAM

Instead of: *“Do we manage privileged access?”*

Ask:

- Can human or machine identities escalate?
- Are privileges standing or just-in-time?
- Are unused permissions and secrets actually removed?

CNP

CSPM / CNAPP

Instead of: *“Are we scanning for cloud risks?”*

Ask:

- Can we identify which misconfigs create real attack paths?
- Can we connect excessive privileges to sensitive resources?

SIM

SIEM & Logging

Instead of: *“Are cloud logs feeding the SIEM?”*

Ask:

- Can analysts see privilege changes & role assumptions?
- Can they correlate identity activity across cloud, SaaS, and IdP?
- Would abnormal data access trigger real investigation?

Only 23% of third parties remediated cloud MFA gaps. Controls must be enforced and tested.

Clearwater

Source: 2026 Data Breach Investigations Report (DBIR) | Verizon

What Good Looks Like

LP

Least Privilege by Default

Access is scoped to what a role requires today, not what it has accumulated over time.

JT

Just-in-Time Elevation

Privileged access is granted for a defined window and expires automatically — not standing indefinitely.

CR

Continuous Access Reviews

Entitlements are recertified on a real cadence — not rediscovered during an audit.

ID

Identity-Centric Detection

Behavior is correlated across cloud, SaaS, and the identity provider — not siloed in separate logs.

AD

Human & Machine Lifecycle

Revoke human access promptly; inventory, rotate, and retire service accounts, tokens, and secrets.

CV

Centralized Visibility

One place shows every identity's effective access — not six consoles that each show part of the picture.

Many organizations can begin with tools they already own, but success requires clear ownership, integration, and operating discipline.

Clearwater

Three Things to Validate Now

1

Know Your Identities

Inventory human, service, third-party, workload, and AI-agent identities—plus tokens, secrets, and OAuth apps.

2

Reduce the Blast Radius

Eliminate unnecessary permissions, dormant accounts, standing privilege, stale secrets, and outdated integrations.

3

Test the Attack Path

Assume one identity is compromised—human, machine, or third-party. Validate each step:

- Can it bypass MFA or escalate?
- Can it assume another identity?
- Can it move from IdP to SaaS/cloud?
- Can it reach ePHI without alerting?
- Can you revoke sessions and rotate secrets?

The strongest cloud identity program is not the one with the longest list of controls.

It is the one that can demonstrate a compromised identity cannot easily become a compromise of the entire environment.

Clearwater

Where Does This Leave You?

1

Where Would You Start?

Which human, machine, or third-party identity creates the largest untested blast radius in your environment?

2

What Would You Test?

If one identity were compromised today, which system would concern you most — and why?

3

What's Still Unclear?

What questions from today would you want to explore further with your own team?

Clearwater

Q&A

Clearwater

Clearwater's Healthcare AI Benchmark Study

- Defining the state of AI security and governance in healthcare
- Share your perspective and receive our benchmark report highlighting **adoption trends**, **common challenges**, and **emerging best practices**
- Responses will remain confidential and be reported only in aggregate

To access the survey, use the QR code above or visit
https://survey.alchemer.com/s3/8916136/ClearwaterAIBenchmark

Upcoming Virtual Events

OCR-Quality® Risk Response Working Lab 2026: Beginning September 16 @ 11:00 am CT

Hands On, Interactive Series to Help You Drive an Efficient and Effective Risk Management Process

- Sign up

Community Hospital Security Roundtable | September 17 | 12:00PM CT | Virtual

Rural and critical access hospitals continue to face growing threats with limited resources. Join us on September, 17 at 12:00PM CT.

- Sign up

Building Cybersecurity to Scale: Lessons from 25m Health's DH Portfolio | Sep 17, 2026 | 12:00 PM CT

Join Ryan Macy of 25m Health and Alex Masten of Clearwater for a practical conversation about how 25m Health developed a repeatable approach to strengthening cybersecurity and compliance across a diverse portfolio of emerging healthcare technology companies

- Sign up

Clearwater's Monthly Cyber Briefing | 12pm – 1pm CT

- Next session October 8th
- AI focused session –more details coming soon!
- You are already enrolled, next quarter's invites should be coming out tomorrow

Clearwater

Upcoming In-Person Events

- September 13-15 in Nashville, TN
- Several Clearwater team members attending and we'd love to connect!
- Learn more + book a meeting

- September 17 in Boston, MA
- Clearwater recently became an industry member to CHAI and will be attending their Legal Summit in September
- Learn more + book a meeting

- September 23-25 in Austin, TX
- Clearwater sponsoring
- President Baxter Lee, Jackie Mattingly & Laura Martin in attendance
- Learn more + book a meeting

- Nov 11-14 in Denver, CO
- Clearwater attending & sponsoring a top golf bay
- Learn more + book a meeting

- Clearwater at HLTH November find us in the MATTER pavilion and the Digital Health Hub Foundation Pavillion
- 2 Speaking Sessions
- Learn more + book a meeting

Clearwater

We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.

Clearwater

Healthcare–Secure, Compliant, Resilient

www.ClearwaterSecurity.com

800.704.3394

LinkedIn | linkedin.com/company/clearwater-security-llc/

Legal Disclaimer

Although the information provided by Clearwater Security & Compliance LLC may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Security & Compliance LLC.