



THE VIZIUS GROUP



WHITE PAPER · VERSION 2.0 · OCTOBER 2026

The Ransomware Vaccine

A 7-phase plan to make ransomware much harder to pull off, and recoverable if it lands.

Written for IT managers and MSPs. Readable by business leaders. Includes a 0 to 10 scorecard, a one-page checklist and a glossary.

Glenn Johnson
Principal Engineer and CEO, The Vizio Group

Find the blind spots. Skip the busywork.
vizio.com

Two questions every leader should be able to answer

Ransomware showed up in 48% of breaches in the 2026 Verizon Data Breach Investigations Report, up from 44%.¹ The FBI counts it among the top threats to critical infrastructure.¹⁵

No product guarantees you won't be hit. The realistic goal: make an attack much harder to pull off, and be able to recover without negotiating with criminals. Your IT team or MSP should be able to answer two questions in plain terms:

1. **How likely is a ransomware event?**
2. **How ready are we to recover if it happens?**

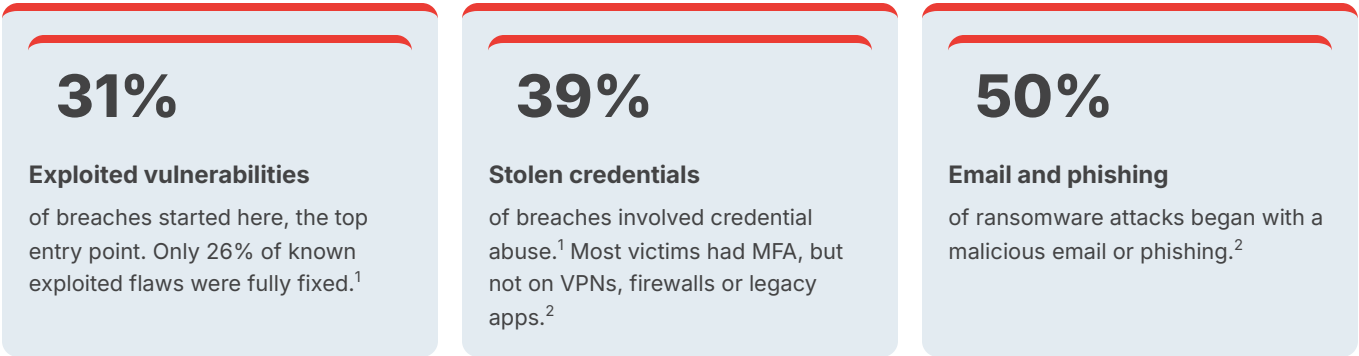
Hand them this paper and say: "Run this playbook, tell me where we stand, and give me a plan to close the gaps." Run it once as a project, then repeat it as a health check. Tools named are examples; adapt them to your environment.

What's new in version 2.0

- **Evidence** from 2025 and 2026 incident data, with sources on page 9.
- **Phishing-resistant MFA**: passkeys and security keys first; SMS and voice codes retired.
- **Patch deadlines by risk**, following CISA's 2026 directive on known exploited flaws.
- **Current password rules** from NIST: length and breach checks, no forced rotation.
- **Backups attackers can't delete**, tested every quarter.
- **New**: help desk checks, infostealer response, scoring anchors, a who-to-call list.
- **Half the length** of version 1.0.

Start with the Big 3

Three ways in drive most ransomware: exploited vulnerabilities, stolen credentials and phishing. The two largest 2026 studies rank them differently, but both put these three on top.



Preparation pays: 66% of organizations whose data was encrypted recovered from backups, up from 54%.²

The seven phases

#	Phase	The question it answers	Page
1	The Big 3: exposure, identity, phishing	Can they get in?	4
2	Email and endpoint protection	Will we stop what gets through?	5
3	Privileged access	Can one stolen account become full control?	5
4	Internal vulnerability management	Are known holes closed on time?	5
5	Backup and recovery	Can we restore without paying?	6
6	Detection and response	Will we notice in time, and know what to do?	6
7	Scorecard and validation	Are we improving, and can we prove it?	7

The order runs outside-in. All seven matter, so work them in order rather than debate priorities. Checklist on page 9; glossary and sources on page 9.

1a External exposure

What's on the internet, and how broken is it? One flaw in a firewall or VPN can open the whole network.

- **Inventory** public IP ranges, domains, firewalls, VPNs, remote access, web apps, admin interfaces and cloud services.
- **Scan from outside** at least monthly and after changes.⁷
- **Patch internet-facing systems first:** 3 days for known exploited flaws (Phase 4).
- **Remove exposure.** Close unused ports. No RDP or admin interface open to the internet, ever. Put remote admin behind a gateway with phishing-resistant MFA.
- **Replace edge devices past end of support.** No patches are coming.⁵

1b Identity and device trust

Make a stolen password useless.

- **MFA on everything reachable from outside:** email, VPN, remote access, firewall and cloud admin consoles, and backup consoles. Attacks land in the gaps.²
- **Phishing-resistant first:** passkeys, Windows Hello for Business or FIDO2 keys, for admins and remote access now, everyone next.³ Where push prompts remain, require number matching. Retire SMS and voice codes; Microsoft stops providing them in Entra ID from February 2027.⁹
- **Passwords, per NIST:** 15+ characters where a password is the only factor; block breached and common passwords; no composition rules or forced periodic changes. Change on evidence of compromise.⁸ Provide a password manager.
- **Watch for leaked credentials and infostealers.** Half of ransomware victims had one in the 95 days before the attack.¹ On a hit, reset the password, revoke sessions and check the device.
- **Conditional Access:** only managed, healthy devices (supported OS, patched, encrypted, EDR running) reach email, files and key apps. Block legacy authentication.

1c Phishing and social engineering

Phishing now arrives by text, voice, QR code and deepfake as well as email.

- **Train short and often** on one habit: verify any unexpected or urgent request through a channel you already know.
- **Simulate and coach.** Track report rates as well as click rates. Show leaders a trend, not a wall of shame.
- **One-click reporting,** and thanks for every report, false alarms included.
- **Harden the help desk.** Verify identity through a known channel before resetting a password or MFA; ransomware crews call posing as employees.¹⁰
- **Verify bank-detail changes** by calling back on a known number.

PHASE 2

2 Email and endpoint protection

You likely own these tools. The question is whether they work and whether anyone is watching.

- **Email filtering** scans links and attachments and quarantines suspicious mail, with a named owner.
- **SPF, DKIM and DMARC** on every domain, with DMARC at quarantine or reject.
- **DNS or web filtering** blocks malicious and newly registered domains.
- **EDR on every supported device**, with tamper protection on. Check coverage monthly against your asset list.
- **Alerts watched 24×7** by your staff, your MSP or a managed detection and response (MDR) service, with a clear escalation path.
- **Isolate** systems that can't run modern tools on their own network segment.

PHASE 3

3 Privileged access

Who can do anything they want here? One compromised account should not mean full control.

- **Inventory and trim** domain, cloud and local admin rights and service accounts. Prefer just-in-time elevation (for example, Entra Privileged Identity Management) to standing rights.
- **Separate admin accounts** for admin tasks only, with phishing-resistant MFA and no email or browsing.
- **Unique, auto-rotated local admin passwords** on every machine. Windows LAPS is built in.¹²
- **Review quarterly** and when people change roles or leave.

PHASE 4

4 Internal vulnerability management

Do inside what you did outside. Patch by risk, using CISA's Known Exploited Vulnerabilities (KEV) catalog.

- **Scan internal systems** at least quarterly, monthly if you can, and track findings to closure.⁷
- **Meet these targets:**

Fix within	When
3 days	A KEV flaw on an internet-facing system, or an internet-facing flaw attackers can exploit automatically for full control. Also check KEV-hit systems for compromise.
14 days	Any other KEV flaw, and other critical flaws on internet-facing systems.
30 days	Everything else, on a monthly patch cycle.

Adapted from CISA BOD 26-04 (June 2026), which sets 3, 14 and 60 days for federal agencies;⁶ the 30-day default follows CIS Controls v8.1.⁷
Can't patch in time? Take the system offline or isolate it.

- **Automate patching** and watch for failures. Change control should schedule fixes, not stall them.

PHASE 5

5 Backup and recovery

Backups decide whether ransomware is an inconvenience or a crisis. They fail when they share the network or credentials with production, or were never tested.

- **One copy attackers can't touch:** three copies, two kinds of storage, one off-site, and at least one immutable or offline. Encrypt them.³
- **Separate identity:** backup systems off the production domain, with their own accounts, phishing-resistant MFA and few admins. Alert on deletions or retention changes.
- **Cover what the business runs on,** including SaaS such as Microsoft 365. Sync and version history are not backups.
- **Set recovery targets** (RTO and RPO) per critical system, agreed with the business.
- **Test quarterly:**⁷ restore files and one full system, confirm the app works, and record time taken against the RTO.
- **Keep golden images** and an offline copy of the recovery plan.³

PHASE 6

6 Detection and response

Ransomware needs time and quiet. Detection and a rehearsed plan take both away.

- **Alert on** mass file changes, disabled security tools and new admin accounts.
- **Centralize logs** from sign-ins, domain controllers, firewalls and VPN, EDR and backups, kept at least 90 days.
- **Write a one-page playbook:** who may isolate systems; first steps (isolate, don't wipe, keep evidence); how to talk if email is down; who to call: your cyber insurer first, legal counsel, your response firm, the FBI (field office or IC3.gov) and CISA.¹¹
- **Set your ransom position in advance** with counsel. Paying doesn't guarantee recovery and can breach US sanctions.¹³
- **Run a tabletop** with leadership at least yearly.⁷

7 Scorecard and validation

Plans die on the shelf. Keep this one alive with a simple score.

- Score each phase 0 to 10, the same way every time:

0

Not started

3

Partly done, ad hoc, no owner

5

Most systems covered, not monitored

8

Complete, monitored, owner named

10

Complete, tested this year, independently checked

- Set a target per phase and note why. Not everyone needs a 10.
- Report to leadership at least yearly, quarterly if you can: scores, targets, changes and the next three actions.
- Validate, don't assume: restore tests, external scans, a tabletop, and an independent assessment every year or two.
- Match your insurance application. A court voided one policy after the insured overstated its MFA.¹⁴
- Need a framework? NIST maps ransomware outcomes to CSF 2.0.⁴

Ransomware preparedness scorecard

Phase	Score (0 to 10)	Target	Owner	Next action
1. The Big 3				
2. Email and endpoint protection				
3. Privileged access				
4. Internal vulnerability management				
5. Backup and recovery				
6. Detection and response				
7. Scorecard and validation				
Overall				

PREPAREDNESS CHECKLIST

One page, one meeting

Review with your IT team or MSP. Mark each line Yes, In progress (IP), No or Not applicable (NA).

Item	Yes	IP	No	NA
IDENTITY AND ACCESS				
MFA covers email, VPN, remote access, admin consoles and backups, with no gaps.	☐	☐	☐	☐
Admins and remote access use phishing-resistant MFA; SMS and voice are retired.	☐	☐	☐	☐
Passwords: length and breach checks, no forced rotation.	☐	☐	☐	☐
Only managed, compliant devices reach company data; legacy sign-in is blocked.	☐	☐	☐	☐
EXTERNAL EXPOSURE				
Internet-facing systems are inventoried and scanned at least monthly.	☐	☐	☐	☐
No RDP or admin interface is open to the internet.	☐	☐	☐	☐
No firewalls, VPNs or routers are past end of support.	☐	☐	☐	☐
EMAIL, ENDPOINTS AND PEOPLE				
Email and DNS filtering are on; DMARC is at quarantine or reject.	☐	☐	☐	☐
EDR runs on every supported device, with alerts watched 24x7.	☐	☐	☐	☐
Staff get short, regular training and can report a phish in one click.	☐	☐	☐	☐
The help desk verifies identity before resets; payment changes get a call-back.	☐	☐	☐	☐
PRIVILEGED ACCESS AND PATCHING				
Admin accounts are few, separate and reviewed quarterly.	☐	☐	☐	☐
Local admin passwords are unique and auto-rotated.	☐	☐	☐	☐
Patch targets are met: 3, 14 and 30 days by risk.	☐	☐	☐	☐
Internal scans run at least quarterly and findings are closed.	☐	☐	☐	☐
BACKUP AND RECOVERY				
Critical systems and SaaS data are backed up, with agreed RTO and RPO.	☐	☐	☐	☐
One copy is immutable or offline, behind separate credentials.	☐	☐	☐	☐
Restores, including one full system, are tested quarterly.	☐	☐	☐	☐
DETECTION, RESPONSE AND GOVERNANCE				
Key logs are centralized and kept at least 90 days.	☐	☐	☐	☐
A one-page ransomware playbook and call list exist, with an offline copy.	☐	☐	☐	☐
Leadership ran a tabletop this year and reviews the scorecard.	☐	☐	☐	☐
Our controls match our cyber insurance application.	☐	☐	☐	☐

Key terms in plain English

Ransomware

Malware that encrypts or steals data, then demands payment.

MFA

Multi-factor authentication: proof beyond a password, such as a passkey or app prompt.

Conditional Access

Rules for who can reach what, from which devices.

KEV

CISA's catalog of Known Exploited Vulnerabilities. Patch these first.

SPF, DKIM, DMARC

Email records that stop others sending as your domain.

RTO and RPO

How fast a system must be back, and how much data you can lose.

SIEM

A system that collects and correlates logs to spot attacks.

Phishing

A fake email, text or call that tricks someone into clicking or sharing credentials.

Passkey, phishing-resistant MFA

Sign-ins (passkeys, Windows Hello, FIDO2 keys) that only work on the real site.

Infostealer

Malware that steals saved passwords and live sign-in sessions.

EDR and MDR

Endpoint detection and response; MDR adds a team watching it 24×7.

Immutable backup

A copy no one, not even an admin, can change or delete for a set time.

LAPS

Windows tool that gives each machine a unique, rotating admin password.

MSP

Managed service provider: outsourced IT for a monthly fee.

Sources

Checked October 2026. Superscript numbers in the text refer to this list.

1. Verizon, 2026 Data Breach Investigations Report. verizon.com/dbir
2. Sophos, The State of Ransomware 2026. sophos.com/en-us/blog/sophos-state-of-ransomware-2026
3. CISA, FBI, NSA and MS-ISAC, #StopRansomware Guide. cisa.gov/stopransomware/ransomware-guide
4. NIST IR 8374r1, Ransomware Risk Management: A CSF 2.0 Community Profile (June 2026). doi.org/10.6028/NIST.IR.8374r1
5. CISA BOD 26-02, Mitigating Risk from End-of-Support Edge Devices. cisa.gov/news-events/directives
6. CISA BOD 26-04, Prioritizing Security Updates Based on Risk (June 2026); KEV catalog. cisa.gov/known-exploited-vulnerabilities-catalog
7. CIS Critical Security Controls v8.1, safeguards 7.5, 7.6, 7.7, 11.5, 17.7. cisecurity.org/controls/v8-1
8. NIST SP 800-63B-4 (2025). doi.org/10.6028/NIST.SP.800-63B-4
9. Microsoft Learn: passkeys by default and SMS and voice retirement in Entra ID; number matching. learn.microsoft.com/entra
10. CISA and FBI advisory AA23-320A, Scattered Spider. cisa.gov/news-events/cybersecurity-advisories/aa23-320a
11. NIST SP 800-61r3 (2025). Report incidents at report.cisa.gov and ic3.gov.
12. Microsoft Learn, Windows LAPS overview. learn.microsoft.com/windows-server/identity/laps
13. US Treasury OFAC, ransomware payment sanctions advisory (Sept. 2021). ofac.treasury.gov
14. Travelers Property Casualty Co. v. International Control Services (C.D. Ill. 2022).
15. FBI IC3, 2025 Internet Crime Report. ic3.gov

Talk to a Principal Engineer

Worked through the checklist, or want an outside view of where you stand? A Principal Engineer will help you decide what to fix first. Thirty minutes, no slide deck.

+1.864.800.0550

vizius.com/contact

We give this plan away so fewer organizations get held hostage.

Suggestions welcome.

Glenn Johnson, Principal Engineer and CEO



THE VIZIUS GROUP

Find the blind spots. Skip the busywork.

141 Traction Street, Greenville, SC · vizius.com

The Ransomware Vaccine · Version 2.0 · October 2026

© 2026 The Vizio Group. Free to share unchanged.

Not legal advice. Adapt to your environment.