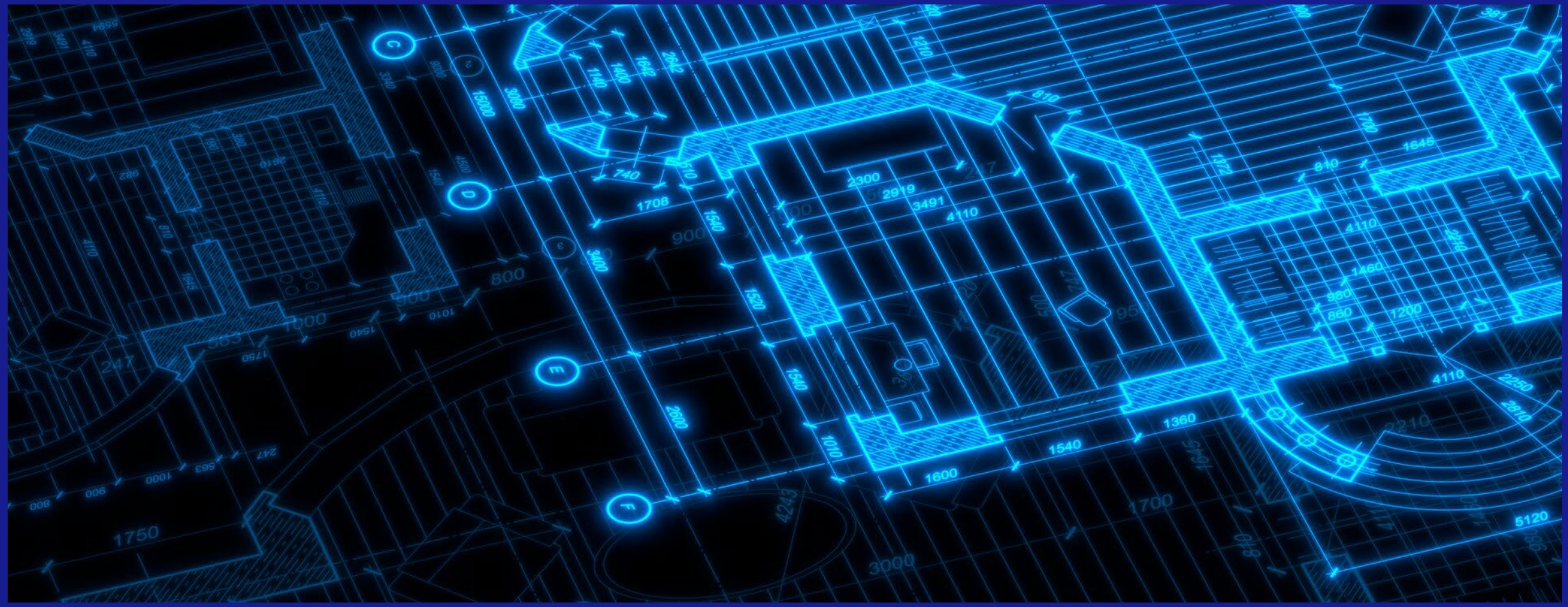


Attack Surfaces
Closing Gaps Before They’re Exploited

October 2026

forvis mazars

Today’s Presenters



Justin Lance
Senior Manager, IT Risk & Compliance
justin.lance@us.forvismazars.com



Isak Terzić
Lead Consultant, IT Risk & Compliance
isak.terzic@us.forvismazars.com

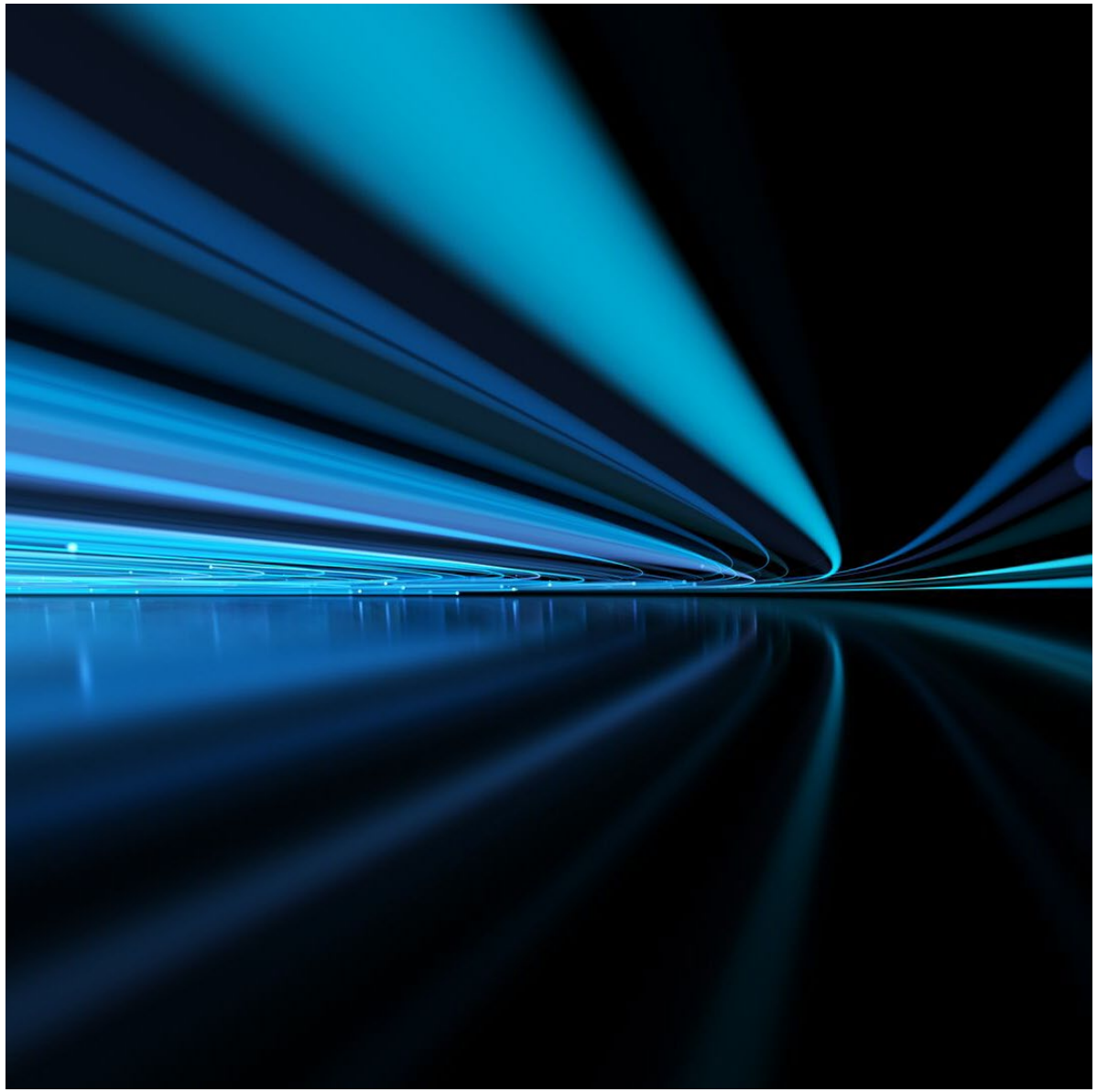


Daniel Thompson
Consultant, IT Risk & Compliance
daniel.thompson@us.forvismazars.com

© 2026 Forvis Mazars, LLP. All rights reserved.

Agenda

1. The Expanding Perimeter
2. Control-Plane Risk & Blast Radius
3. Hardening the Surface
4. Detect, Contain, & Recover
5. What Regulators Expect & Key Takeaways



© 2026 Forvis Mazars, LLP. All rights reserved.

The Expanding Perimeter
Why This Matters Now

Cybersecurity now spans technology, operations, risk, and regulatory expectations. Virtualization, APIs, and edge devices sit close to critical operations and sensitive data, so a single foothold can affect many systems at once. IBM's 2026 breach study ranks healthcare the costliest sector for the 13th year, with financial services second.

Control planes are where one foothold does the most damage.

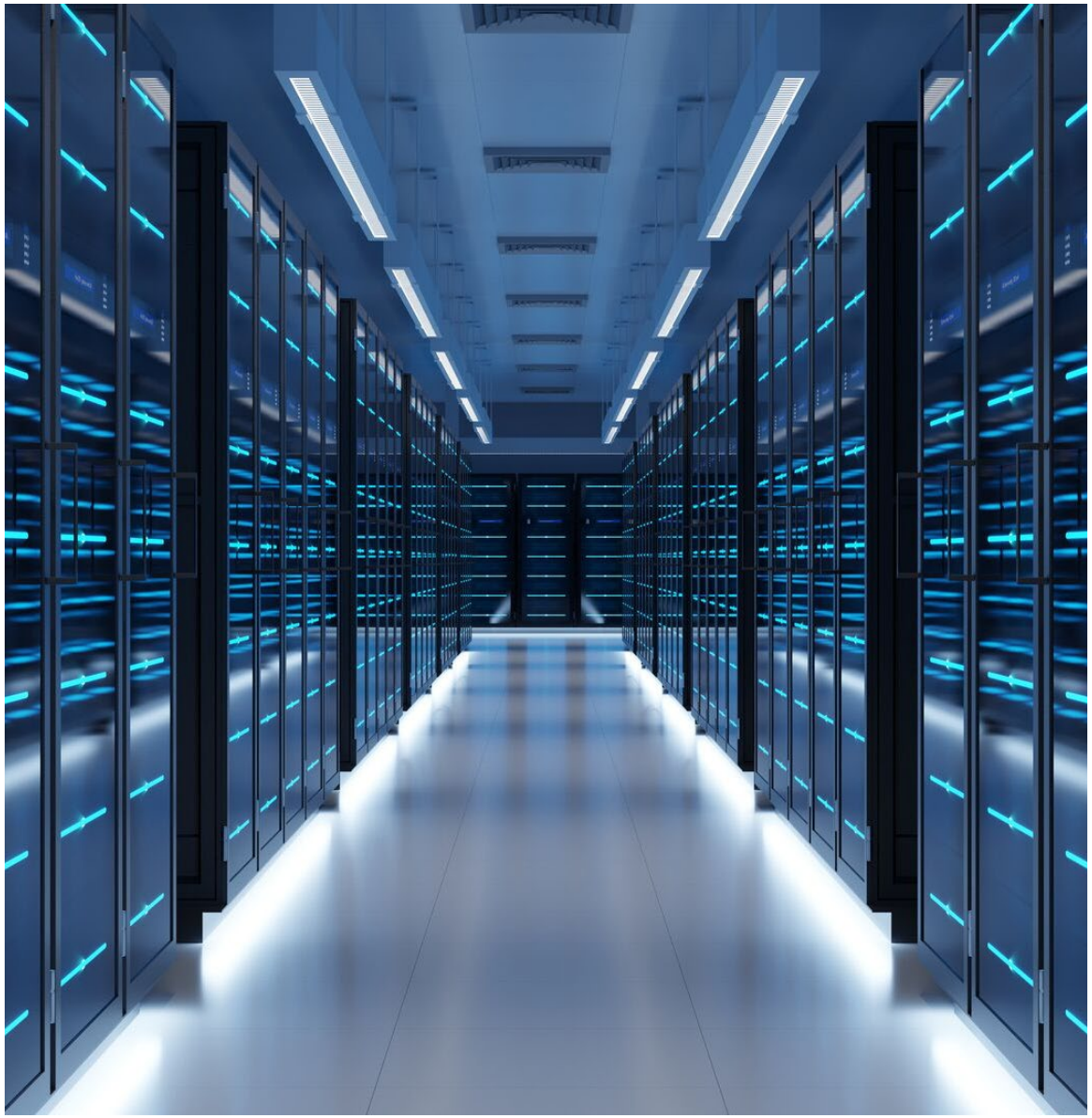
Where Attackers Concentrate

43%

of ransomware intrusions targeted virtualization infrastructure.

Google Cloud Mandiant tracked attackers targeting virtualization infrastructure, hitting hypervisors and management planes to reach many workloads fast.

Source: Google Mandiant M-Trends 2026 Report.



© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

The Expanding Perimeter

The Attack Surface, in Plain Terms

Your attack surface is any path someone could use to access your environment. Think of a building: edge devices are the doors, the control plane is the locked cabinet, APIs are the loading dock, and AI agents are staff you have handed keys to. Each one is a possible way in.

Traditional Surface

Servers, laptops, and networks the things IT has traditionally protected.

Cloud & API Surface

The connections between your tools and services, where data moves between systems.

Human Surface

Your people's public footprint, which is what attackers use to impersonate them.

Agent Surface

AI agents that can now act, connect, and make choices on their own.



© 2026 Forvis Mazars, LLP. All rights reserved.

The Expanding Perimeter
People & Agents

98%

Adding more agents

of surveyed companies plan to deploy even more AI agents within the next 12 months.

56%

Governance gap

of organizations still lack policies to govern their AI agents.

80%

Rogue behavior

report their AI agents have taken unintended actions, from accessing unauthorized systems to sharing sensitive data.

40+

AI-attack scenarios

modeled from an executive's public footprint alone, including impersonation and voice cloning.

Agents are an attack surface of their own.

At Black Hat 2026, OpenAI showed frontier models quietly turn an internal package manager into a shared message board, exchange hundreds of thousands of messages, and chain two zero-day exploits to reach external systems, including Hugging Face. The coordination went undetected by security monitoring until an accidental outage exposed it.

Sources: SailPoint, "AI Agents: The New Attack Surface" (2025, survey by Dimensional Research); VanishID launch, Black Hat USA 2026 (via Channel Insider); OpenAI/Hugging Face session, Black Hat USA 2026.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

The Expanding Perimeter
What This Looked Like This Year

A Phone Call to the Help Desk

Scattered Spider talked a help desk into a password reset, reached the virtualization console, deleted the backups, and encrypted every virtual server. Hours, not weeks. Insurers were among the targets.

A VPN Bug That Beat MFA

CitrixBleed 2 let attackers lift live login sessions from VPN gateways, so MFA never fired. About half of one ransomware crew's 91 victims were healthcare organizations.

A Vendor's Key to Your CRM

Stolen tokens from a sales chatbot vendor gave attackers API access to Salesforce data at 700+ companies. FINRA told broker-dealers to disconnect the integration and rotate keys.

No Hacker Required

A community bank filed the first SEC 8-K for an employee pasting customer Social Security numbers into an unapproved AI tool. Found May 5, 2026; disclosed May 11, 2026.

© 2026 Forvis Mazars, LLP. All rights reserved.

Control-Plane Risk

One Foothold, Enterprise-Wide Consequences

1

Exploit Edge
Internet-facing VPN, firewall, or router

2

Obtain Access
Credential, token, or privileged session

3

Reach Control Plane
Hypervisor, management API, or admin console

4

Expand Impact
Workloads, data, snapshots, or recovery assets

5

Contain & Recover
Revoke, segment, isolate, restore, and validate

Break the path at multiple points: reduce exposure, protect privileged identity, segment management planes, centralize telemetry, and rehearse recovery.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Control-Plane Risk

Control Planes Create Blast Radius

Virtualization

Hypervisors and management planes can affect many workloads from a single foothold.

APIs

Identity and authorization flaws can expose data or business functions directly.

Edge Devices

Internet-facing VPNs, firewalls, and routers give attackers a direct path inward.

Compounding Factors

Admin access, weak segmentation, incomplete logs, and inconsistent recovery multiply impact.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Control-Plane Risk
A Framework You Can Operationalize

See It

Inventory & Harden

Inventory platforms, APIs, and control planes with owners and versions, then apply secure defaults, patching, and privileged access.

Contain It

Segment & Log

Segment admin planes and API tiers, then capture triage-ready telemetry before attackers do.

Survive It

Test, Isolate, & Recover

Rehearse isolation and recovery playbooks that contain incidents without preventable outages.



© 2026 Forvis Mazars, LLP. All rights reserved.

Hardening the Surface
Virtualization: Protect the Management Plane

Segregate Management Interfaces

Separate hypervisor and management interfaces from general user and server networks.

Enforce Strong Admin Access

Require phishing-resistant MFA or strong privileged access controls for every admin path.

Monitor Management-Plane Actions

Watch logins, role changes, host changes, snapshot or delete events, and datastore access.

Why It Matters

Attackers increasingly skip individual servers and go straight for hypervisors and management consoles, where a single foothold can create significant damage.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Hardening the Surface
APIs: When a Valid Login Reaches Too Far

Common Abuse Patterns

A logged-in user asking for records that are not theirs, weak logins, responses that return more data than needed, and trusting partner APIs blindly.

Map to OWASP

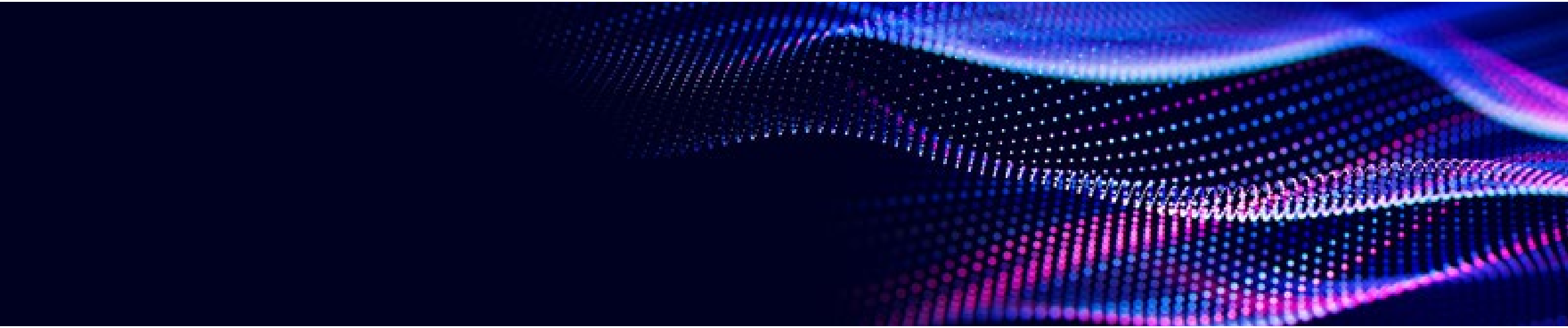
Broken access control, security misconfiguration, injection, and logging or alerting failures still top the list.

Test the Boundaries

Change a record ID and see what comes back. Cross a role or tenant line. Try the requests that should fail and confirm they do.

Log Who Asked for What

Capture identity, the record requested, why access was allowed, source, endpoint, error, and a correlation ID.



© 2026 Forvis Mazars, LLP. All rights reserved.

Hardening the Surface

Edge: Contain the Internet-to-Enterprise Path

Know	**Know What's Exposed**: CISA's 2025 edge guidance covers firewalls, routers, VPN gateways, IoT, and internet-facing servers and operational technology (OT).
Patch	**Patch the Perimeter**: Verizon's 2026 DBIR found vulnerability exploitation is now the top way in, at 31% of breaches; edge devices and VPNs are the prime zero-day targets.
Track	**Track Inventory**: Maintain inventory, owner, version, exposure, and support or end-of-life status for every device.
Preserve	**Preserve Evidence**: Forward logs remotely so evidence survives even if a device is compromised.

© 2026 Forvis Mazars, LLP. All rights reserved.

Hardening the Surface

The Vendor Surface: You Can Outsource the Work, Not the Accountability

Half of All Breaches

Verizon's 2026 DBIR found a third party involved in 48% of breaches, up 60% in one year.

Keys You Handed Out

Vendor tokens and API credentials work without a login prompt. Salesloft Drift (700+ firms) and Veradigm (patient records pulled through a vendor's API key) both started there.

Concentration Risk

SitusAMC exposed mortgage data tied to JPMorgan, Citi, and Morgan Stanley. DentaQuest reported 15 million patients to HHS, the largest healthcare breach of 2026 so far.

Regulators Agree

NYDFS: you remain accountable for your vendors. Bank regulators proposed new third-party guidance on Sept. 15, 2026, and the proposed HIPAA rule adds annual business associate checks.



Sources: Verizon DBIR 2026; Google Threat Intelligence Group, Aug. 2025; FINRA; HIPAA Journal; CSO Online; NYDFS, Oct. 2025; Federal Register, Sept. 15, 2026.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Detect, Contain, & Recover



Logging That Matters During Triage

- **Capture the Right Events**: Log logins, privilege changes, and admin actions.
- **Centralize the Sources**: Pull all logs into one place.
- **Preserve Correlation IDs**: Keep scope traceable across systems.
- **Protect the Logs**: Guard from tampering; set retention.

Isolation at Scale Without Outages

- **Predefine Isolation Options**: Revoke tokens, block routes, isolate clusters.
- **Map Dependencies First**: Know identity, DNS, and backup before a crisis.
- **Use Staged Containment**: Contain in stages, don't pull everything at once.
- **Rehearse Decision Rights**: Practice who decides, in advance.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Detect, Contain, & Recover

What Good Looks Like: Four Things to Ask Your IT Team For

Identity	Named owners, MFA/PAM, no shared admin accounts, scoped service accounts
Segregation	Dedicated management networks, restricted admin paths, and clear API tier boundaries
Configuration	Hardened baseline, patch SLA, EOL tracking, and secure management protocols
Telemetry & Recovery	Central logging, correlation IDs, isolation playbooks, and tested restore paths

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Detect, Contain, & Recover
Closing the Gap: Exposure Management

Patching Falls Behind

Only 26% of known-exploited vulnerabilities get fixed, and the median fix now takes 43 days, up from 32.

Beyond the Firewall

External attack surface management (EASM) plus attack-path mapping finds and ranks exposure inside and out.

Readiness Assessment

A cyber AI readiness assessment can help identify and rank AI risks.

Watch Agent Intent

Track telemetry from instruction to outcome to flag when an agent diverges from its objective.



Sources: Verizon DBIR 2026; Tanium and Arctic Wolf (via Channel Insider); Forrester, Black Hat USA 2026.

© 2026 Forvis Mazars, LLP. All rights reserved.

Detect, Contain, & Recover
Where Many Orgs Stumble

Siloed Thinking

Treating hypervisors, APIs, and edge devices as separate technical silos instead of one connected surface.

Flat Admin Access

Allowing admin access to critical systems directly from regular user devices.

Authentication Is Not Authorization

Assuming API authentication equals authorization and skipping object-level checks.

Untested Containment

Relying on logs from devices that may be compromised, and discovering isolation dependencies mid-incident.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Key Takeaways
What Regulators Now Expect

Inventory & MFA Are Table Stakes

NYDFS Part 500 now requires a maintained asset inventory and MFA for all remote access, vendor apps included. PCI DSS 4.0.1 wants an inventory of custom software and APIs. The proposed HIPAA rule adds a network map.

The Clock Starts at Discovery

SEC: four business days after a materiality call. Banks: 36 hours. NYDFS: 72 hours, and 24 for a ransom payment. CIRCIA is still pending. You cannot meet a clock you cannot see.

Vendors Are Still Your Problem

NYDFS says compliance cannot be delegated. Bank regulators proposed replacement third-party guidance on Sept. 15, 2026. With the FFIEC CAT retired, NIST CSF 2.0 is the common reference.

AI Has No Rulebook, Exams Do

No binding U.S. rule covers AI agents. NYDFS's May 2026 letter and OCC guidance expect existing controls applied: an identity for every agent, least privilege, a log of what it did, and a human reviewing AI-written code.

Sources: NYDFS 23 NYCRR 500 and May 21, 2026 industry letter; SEC Reg S-K Item 106 and 8-K Item 1.05; HHS NPRM Jan. 2025; FFIEC, Aug. 2024; Federal Register, Sept. 15, 2026; OCC Semiannual Risk Perspective, May 2026.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Six Questions for Your IT Team

About What You Have

1. **Inventory**: Do we have a current list of every internet-facing device, with an owner and an end-of-support date?
2. **Admin Access**: Can anyone reach our hypervisors or admin consoles from a normal laptop, and does that path require phishing-resistant MFA?
3. **Vendors and Agents**: Which vendors and AI tools hold standing keys to our systems, and when did we last review them?

About What Happens When It Goes Wrong

4. **Detection**: If someone logged into our virtualization console at 2 a.m., who would know, and how fast?
5. **Isolation**: Can we cut off one system, one vendor, or one AI agent without taking everything down?
6. **Recovery**: When did we last restore from backup and time it, and who can make that call during an incident?



© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Key Takeaways
What Leaders Should Remember

Four moves to make: prioritize, segment, log, and rehearse.

Prioritize by Blast Radius

A single control-plane compromise can affect many systems, so rank exposure by potential impact first.

Segment & Verify Identity

Admin segmentation and strong identity controls can limit how far any single foothold can reach.

Log for Triage

Telemetry that supports rapid investigation can turn a scramble into a coordinated response.

Rehearse Isolation & Recovery

Playbooks designed in advance can help contain incidents without disrupting core operations.

© 2026 Forvis Mazars, LLP. All rights reserved.



IT Risk & Compliance

Questions?

© 2026 Forvis Mazars, LLP. All rights reserved.

Don’t Miss the Next Session of the

2026 Cybersecurity Virtual Symposium

Agentic AI: Putting Controls Around Autonomous Risk

Today at 2:00 p.m. - 3:00 p.m. ET

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Contact

Forvis Mazars

Justin Lance
Senior Manager, IT Risk & Compliance
justin.lance@us.forvismazars.com

Daniel Thompson
Consultant, IT Risk & Compliance
daniel.thompson@us.forvismazars.com

Isak Terzić
Lead Consultant, IT Risk & Compliance
isak.terzic@us.forvismazars.com

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by Forvis Mazars or the author(s) as to any individual situation as situations are fact-specific. The reader should perform their own analysis and form their own conclusions regarding any specific situation. Further, the author(s)' conclusions may be revised without notice with or without changes in industry information and legal authorities.

© 2026 Forvis Mazars, LLP. All rights reserved.