THE BLUE LENS

DEFENSIVE SECURITY REPORT

Written by
Brayden Park
Cybersecurity Consultant at
Echelon Risk + Cyber

ECHELON RISK + CYBER

ECHELONCYBER.COM

Table of Contents

Overview

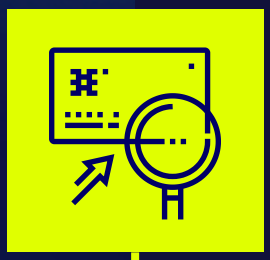
Over the past 18 months, we've seen acceleration on both sides of the battlefields. This was not just for defenders, but for adversaries. From infostealer-driven access markets to zero-day edge device exploits, the attacker ecosystem matured into a scalable, business-like force. Cloud complexity, identity gaps, and third-party dependencies continue to outpace security investment.

This report distills findings from five of the industry's most respected threat and 2024 and 2025 breach reports (Mandiant, CrowdStrike, IBM, Verizon, and the World Economic Forum), overlays frontline experiences from Echelon's client base, and outlines practical strategies security leaders can implement to defend more effectively in 2025.

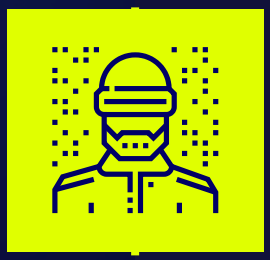
Threat Landscape:

Lessons Learned from 2024

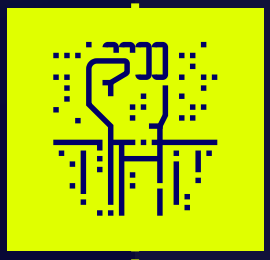
The Adversary Moves Faster – *So Must You*



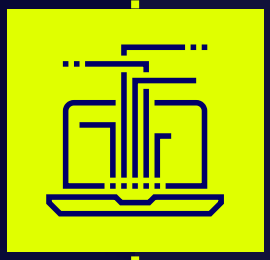
Initial Access Shifts (Mandiant M-Trends 2025): Exploits were the leading vector (33%) for the 5th year in a row. Phishing declined slightly, while stolen credentials surpassed it at 16%. [1]



Infostealer Surge: Credential theft fueled by info-stealers and dark web credential markets.



Edge Device Exploits: Zero-days in PAN-OS, Ivanti, and Fortinet widely abused.



Third-Party Risk (Verizon 2025 Data Breach Investigations Report): 53% of breaches involved third-party assets. [2]

Top Targeted Sectors: Business and Professional services, high-tech, manufacturing, and healthcare sectors led the breach count. [1]

Our Advice to Stay Ahead of Evolving Cyber Threats

Exploit chaining and credential-based attacks remain among the most effective tactics used by adversaries, especially in environments with legacy infrastructure, flat networks, or weak MFA enforcement. Prioritize patching externally exposed services, segmenting legacy systems, and enforcing strong identity controls to reduce exposure.

Credential theft often fueled by infostealers and reused passwords—continues to be a top driver of breach activity. Implement phishing-resistant MFA, harden privileged access, and regularly audit third-party integrations to close these gaps.

Despite growing awareness, many organizations still struggle to visualize how identities, credentials, and integrations expose them to risk. Regularly review identity risks, map attack paths, and create zero-trust access policies to stay ahead of these evolving threats.

ECHELON PERSPECTIVE

Throughout 2024 and into 2025, we worked closely with organizations to remediate risks stemming from zero-day vulnerabilities and credential-based attacks. Our efforts focused on conducting identity risk assessments, improving network segmentation, and addressing over-permissioned accounts and third-party integrations. These initiatives helped reduce access sprawl, strengthen MFA enforcement, and close critical exposure gaps across hybrid environments.

Defensive Controls: What's Breaking and Why

When Security Tools Aren't Enough

01.

Dwell Time[1] Reversal

Global median dwell time rose to 11 days, the first increase since 2010. [1]

02.

Cloud Gaps

Misconfigurations and weak identity protections continue to enable lateral movement.

03.

IAM Gaps

Stolen credentials and MFA fatigue continue to allow attackers to remain undetected in environments.

04.

Shadow Data

35% of breaches involved unmanaged "shadow" data assets. [3]

Client Anecdote

During a recent security review for an education-focused organization, the Echelon team uncovered a familiar but risky pattern. Several global admin accounts had no MFA enabled, and there weren't any conditional access policies in place. These accounts had full control over Microsoft 365 and Entra ID, making them ideal targets for threat actors.

Even more concerning, administrators were using the same accounts for both day-to-day work and privileged tasks. It was a setup that blurred the lines between routine use and high-risk access—amplifying exposure. Our recommendations prioritized enforcing MFA for all privileged roles and creating a clear separation between admin duties and regular user activity. Simple changes, but ones that significantly reduce risk.

[1] *DWELL TIME: THE PERIOD BETWEEN WHEN AN ATTACKER FIRST COMPROMISES A SYSTEM AND WHEN THEY ARE DETECTED AND REMOVED.*

Our Advice to Beef Up Defensive Controls

Over-privileged accounts and weak identity governance continue to present high-risk exposure points especially when MFA is not enforced or conditional access policies are overly permissive.

ORGANIZATIONS SHOULD

1. **Enforce MFA for all admin roles without exception**
2. **Eliminate shared or dual-use accounts by separating day-to-day use from privileged accounts**
3. **Conduct routine reviews of role assignments and group memberships**
4. **Minimize standing privileges through role-based access control (RBAC) and Just-In-Time access models**
5. **Regularly audit conditional access exclusions and phase out legacy authentication wherever possible**

The Adversary Evolves – and So Should Defense

Sophisticated, Scalable, and AI-Enabled

- **Social Engineering Surges**
  A 442% increase in vishing attacks targeting internal support desks, alongside rising smishing and deepfake-driven scams aimed at impersonating executives and tricking employees. [4]

- **GenAI in the Attacker's Toolkit**
  The proliferation of AI tools enables attackers to launch deceptive campaigns more cheaply, quickly, and effectively — from phishing and job scams to election disinformation and impersonation. [5]

- **Access Brokers on the Rise**
  52% of observed activity to initial access as a service. [4]

- **Cloud Native Exploitation**
  Attackers increasingly target misconfigured SaaS and identity platforms.

Client Anecdote

A phishing email impersonating a trusted vendor bypassed email security layers and was acted upon by a user with access to financial workflows. Despite awareness training, the attack succeeded, highlighting the real-world limits of technical controls and end-user vigilance.

Echelon was engaged to assist with investigation, response coordination, and post-incident analysis. Our team helped identify control gaps, documented findings, and provided practical steps to harden defenses and reduce future risk.

Echelon's Advice on Incident Response

Recovery shouldn't end at containment. The period after an incident offers a critical opportunity to strengthen future resilience.

Organizations should:

- Conduct open, judgement-free after-action reviews (AARs) to identify not only what failed, but why
- Re-evaluate and fine-tune security tooling, alerting thresholds, and incident response workflows based on lessons learned.
- Document playbooks for common incident types and integrate them into regular testing cycles.
- Treat each incident as a catalyst for long-term maturity emphasizing repeatable processes, cross-team alignment, and measurable improvement over time.

The Business of Breaches

It's Not Just IT – it's Financial, Operational, and Regulatory

Echelon's Advice on Reducing Long-Term Risks (and Cost):

The true cost of a breach often extends far beyond technical remediation. Legal exposure, reputational damage, and business continuity gaps can significantly amplify impact.

To reduce long-term risk and recovery costs, organizations should:

- Develop and routinely test an incident response plan with input from legal, IT, and executive leadership
- Conduct tabletop exercises to identify coordination challenges and decision-making gaps before a real incident
- Establish a clear internal and external communications strategy, including breach notification protocols
- Integrate post-incident reviews into governance processes to drive continuous improvement across security, compliance, and business operations

$4.88M

Breaches cost an average of $4.88M

Up 10% year-over-year, driven by operational downtime, loss of business, and remediation. [3]

292 Days

Stolen Credential Breaches Take 292 Days to Detect

The longest of any attack vector [3]. Because attackers use valid credentials, their activity often blends in with normal user behavior, allowing them to remain undetected, escalate access, and cause greater damage over time. This highlights the urgent need for stronger identity controls and monitoring.

$4.99M

Insider Risk is the Costliest

Malicious insiders drove an average breach cost of $4.99M, making them the most expensive threat category due to their trusted access and deep organizational knowledge. [3]

$830K

Industrial Sector Breaches Saw the Highest Cost Increases

+$830K due to downtime sensitivity. [3]

How Security Leaders Can Stay a Step Ahead in 2025

A Practical Guide to Defense, Rooted in Reality

Fortify Identity as the New Perimeter

- Deploy phishing-resistant MFA (FIDO2, hardware keys), particularly for administrator access.
- Enforce credential vaulting and service account lifecycle management.
- Integrate Identity Protection telemetry into threat detection (e.g., CrowdStrike Falcon IDP, Microsoft Entra Identity Protection).

Elevate Threat Detection and Hunting

- Use intelligence driven threat hunting across cloud and identity.
- Tune SIEM/SOAR platforms for callback phishing and RMM tool abuse.
- Hunt for signals of initial access brokers and beaconing.

Cloud Hardening

- IaaS: Review virtual networks, security group configurations, and storage permissions in platforms like AWS, Azure, and GCP to reduce lateral movement and overexposure.
- PaaS: Assess identity integrations, logging configurations, and access to managed services such as databases, containers, and serverless functions.
- SaaS: Continuously review OAuth scopes, third-party app access, and validate least-privilege role use in tools like Microsoft 365, Okta, and Salesforce.

De-risk Your Digital Supply Chain

- Enforce vendor patch cadence and firmware management.
- Require attestations for access to sensitive environments.
- Architect identity segmentation for third parties.

Strengthen Human Resilience

- Train help desk and execs on callback and deepfake scams.
- Build runbooks for social engineering escalation.
- Offboard users with full audit logging, automated access revocation, and validation reporting to ensure complete deprovisioning across systems.

Conclusion:
Security as a Business Imperative

In a world of enterprising adversaries and widening attack surfaces, reactive defense is no longer enough. Executives must shift from "protecting everything" to "defending what matters most, faster."

Organizations should focus on maturing their defensive posture through practical, continuous process improvement — not just in technology, but in people and operations. By strengthening workflows, upskilling teams, and embedding security into daily practices, companies can build resilience where it matters most: at the intersection of humans, processes, and technology.

Ready to Strengthen Your Defense?

At Echelon, we've guided clients across these exact initiatives with tangible outcomes. From designing phishing-resistant IAM architectures to operationalizing security tools and hardening multi-cloud environments, our work spans both strategy and implementation: building security roadmaps, tuning detection systems, closing identity gaps, and helping teams operationalize Zero Trust principles. Whether you're starting from a baseline or optimizing existing controls, we help turn security goals into action.

Echelon Can Help You

- Harden Identity and Access Management
- Assess and Enhance Defensive Security Controls
- Review Cloud and SaaS Security Configurations
- De-risk Your Digital Supply Chain
- Conduct Threat Hunting and Exposure Mapping
- Prepare for Breaches with Real-World Playbooks
- Engage in Managed NG-SIEM or Advisory Support

Our approach is rooted in defense-in-depth and Zero Trust principles. It's reinforced by clear reporting and measurable progress that align security with business outcomes.

LET'S TALK

If these challenges resonate, our team is ready to help, whether it's a one-time review or ongoing strategic support.

References

[1] Mandiant. M-Trends 2025 Threat Intelligence Report. Google Cloud, 2025.

[2] Verizon. 2025 Data Breach Investigations Report.

[3] IBM Security. Cost of a Data Breach Report 2024.

[4] CrowdStrike. 2025 Global Threat Report.

[5] WEF Global Cybersecurity Outlook 2025