TRUSTED PARTNER NETWORK

STAR 2026 REPORT

POWERED BY MOTION PICTURE ASSOCIATION

SECURITY TRENDS ANALYTICS READINESS

Letter from the Chairman & CEO, Motion Picture Association (MPA)

Storytelling bridges cultures, crosses borders, fuels economies, connects communities, and carries common values across the globe. To sustain this enduring force in our society, we must do more than support it. We must act to protect it.

The Motion Picture Association, the Trusted Partner Network, and our entire content protection operation know that, in today's digital marketplace, security is no longer a technical afterthought. It's an urgent priority. A nonnegotiable investment in the creative community's success. An essential pillar of trust in the creative ecosystem worldwide.

We also recognize that the rapid development of AI and emerging technologies require our sector to do everything possible to keep pace with ever-evolving challenges of this moment in history.

Through the MPA's 360 Strong strategy – which includes close collaboration between TPN and the Alliance for Creativity and Entertainment – we are working to ensure creators and content partners everywhere have the protections they need across the content lifecycle.

The TPN STAR Report is a vital step forward in that collective effort. It establishes a clear, industrywide baseline for content security maturity. It brings greater transparency, consistency, and accountability to an increasingly complex landscape. It highlights the progress we have already made while recognizing the critical work still ahead: helping to strengthen the foundation of trust on which creators depend.

Charles Rivkin
Chairman & CEO
Motion Picture Association (MPA)

TPN President's Perspective

Dear Colleagues,

The Trusted Partner Network was relaunched in 2023 to strengthen content security through deeper collaboration across the global content supply chain. This inaugural TPN STAR Report presents assessor-validated data at scale, based on three years of real-world security assessments across the content supply chain. The result is a clear, objective view of how security controls perform in practice, and where execution breaks down.

The STAR dataset highlights areas of concentrated and pressing risk. Despite growing industry commitment, security performance in practice remains inconsistent - particularly in technically intensive controls and remediation, where execution gaps and slow remediation timelines continue to introduce material risk.

This is not a theoretical gap. It is an operational one.

Recent months have seen an increase in security alerts related to active threats, reinforcing the urgent need for security controls to operate consistently and reliably in day-to-day operations. Addressing this requires stronger control execution, clearer ownership, improved oversight of third-party execution, and more timely remediation of known risks.

The STAR Report is designed to reinforce effective execution through greater visibility and insight, as it establishes a baseline for measuring security performance and identifies where collective action is needed to strengthen resilience across the global content supply chain.

Future editions of the STAR Report will continue to build on this foundation as the program evolves. The 2027 STAR Report will incorporate MPA Best Practices v5.3.1 and Additional Recommendations, alongside results from the new four-tier TPN Shield framework. Early indicators show these enhancements are already driving meaningful improvements in full compliance, reinforcing the value of a clearer pathway for the service provider community, stronger incentives, and greater alignment across the ecosystem.

Despite this, progress to date is not sufficient - especially in the context of heightened threat activity. Accelerating improvement where risk remains highest requires decisive, coordinated action. Securing the global content supply chain is a shared responsibility, and sustained progress will depend on continued commitment and collective action across the industry.

Terri Davies

Terri Davies
President, Trusted Partner Network

Table of Contents items are clickable

EXECUTIVE SUMMARY

A Clear Warning to the Industry

TPN works with Content Owner members to keep the MPA Content Security Best Practices current and relevant. As part of the MPA 360 Strong strategy, TPN also collaborates with the Alliance for Creativity in Entertainment (ACE) to issue security alerts broadly across the industry, promoting shared awareness and preparedness.

Recent alert activity signals a material increase in threat exposure. In the first quarter of 2026 alone, TPN issued more security alerts than in all of 2025 combined, with recurring warnings tied to compromised credentials, gaps in multi-factor authentication, insecure configurations, and weaknesses in vulnerability management.

TPN Data Aligns with Incident Root Causes

The STAR dataset reinforces these signals, showing that non-compliance is most pronounced in technically complex security layers, including Vulnerability Management, Cryptography, Endpoint Hardening, and Access Management. These areas also exhibit the largest gaps between perceived and validated performance, alongside higher rates of remediation refusal rates and longer remediation timelines.

Notably, these same weaknesses repeatedly appear in real-world security incidents. Taken together, the findings show that many of the vulnerabilities realized during incidents are also identifiable through assessments, underscoring the importance of improved and consistent operational execution and timely remediation once a weakness has been identified.

The Core Insight: An Execution Gap

Across the dataset, execution is inconsistent: technical controls may be documented but are not always implemented, monitored, or maintained in practice, resulting in delayed remediation and known vulnerabilities remaining unresolved over time.

An Urgent Call to Action

Closing this gap requires stronger follow-through beyond assessment, with sustained execution of the highly non-compliant technical controls. Organizations must strengthen ownership, accelerate remediation, and reinforce operational security controls including identity and access protections.

As production workflows span cloud environments, distributed teams, and third-party partners, security must operate continuously across the global content supply chain. Addressing these execution gaps is essential to reducing systemic risk.

The Biggest Security Gaps Are In Day-to-Day Execution

Security gaps and non-compliance are most pronounced in technically complex areas where day-to-day execution is inconsistent, particularly Vulnerability Management, Cryptography, and Endpoint Hardening.

In many cases, organizations overestimate how effectively controls are operating (perception gap), and even when gaps are identified, remediation is delayed or refused, leaving known risks unaddressed.

As attacks increasingly target identities, weak access controls continue to heighten exposure, with one in four organizations demonstrating non-compliant Access Management. At the same time, adoption of more advanced security capabilities at the Strategic Layer - including Zero Trust and AI-driven capabilities - remains limited.

Reducing risk will require more consistent execution, faster remediation, and more decisive adoption of updated security practices.

FIVE SECURITY ACTIONS
THE INDUSTRY MUST PRIORITIZE NOW

1

Treat Security as a Daily Responsibility

Security cannot only live in policies or annual assessments. Controls must be actively monitored, tested, and maintained continuously.

2

Fix High-Risk Technical Gaps Early

Focus on closing the most critical weaknesses, especially vulnerability management, endpoint hardening, and cryptography, where non-compliance remains highest.

3

Lock Down Identity and Access

Most attacks begin with compromised credentials. Enforce multi-factor authentication, manage and review accounts regularly and monitor privileged access continuously.

4

Hold Vendors and Partners Accountable

Security gaps in the supply chain create real exposure. Establish clear responsibilities and individually require partners to remediate identified issues.

5

Respond Faster When Security Gaps Are Found

Delayed remediation increases risk. Prioritize fixing the vulnerabilities that matter most, not just the ones that are easiest to close.

INDUSTRY CONTEXT & REPORT SCOPE

Industry Context

The global media and entertainment production ecosystem has become increasingly distributed. Content creation, post-production, and distribution workflows now operate across cloud platforms, remote teams, and specialized third-party partners. As the supply chain expands, maintaining consistent security practices across organizations of different sizes, geographies, and operational maturity has become both more complex and critical.

The Role of TPN

The Trusted Partner Network (TPN), wholly owned by the Motion Picture Association, provides the industry with a unified framework for evaluating and strengthening content security throughout the production lifecycle. Through the MPA Content Security Best Practices and independent security assessments conducted through the TPN+ platform, organizations can measure their security posture against a consistent set of expectations designed to protect sensitive creative assets.

About the STAR Report

The TPN STAR Report analyzes aggregated and anonymized data from these assessments to provide an industry-wide view of security maturity. Unlike many industry studies that rely on surveys or self-reported indicators, the STAR Report is based on independently validated assessment findings, enabling objective analysis of security control implementation, remediation activity, and operational security trends across the global production ecosystem.

DATA ANALYTICS & INSIGHTS

Data Analytics & Insights

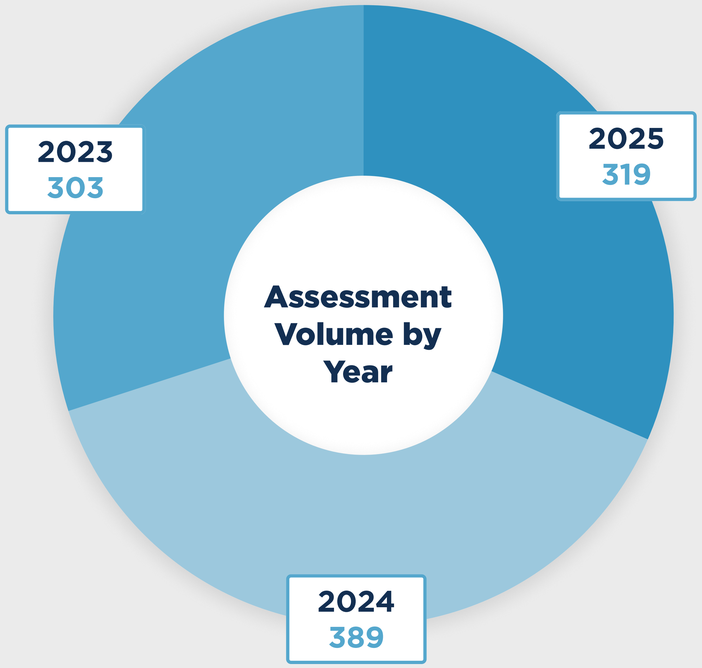
OVERALL SECURITY MATURITY

What does the dataset reveal about overall security maturity across the industry?

Consistent Assessment Activity, Flat Security Outcomes

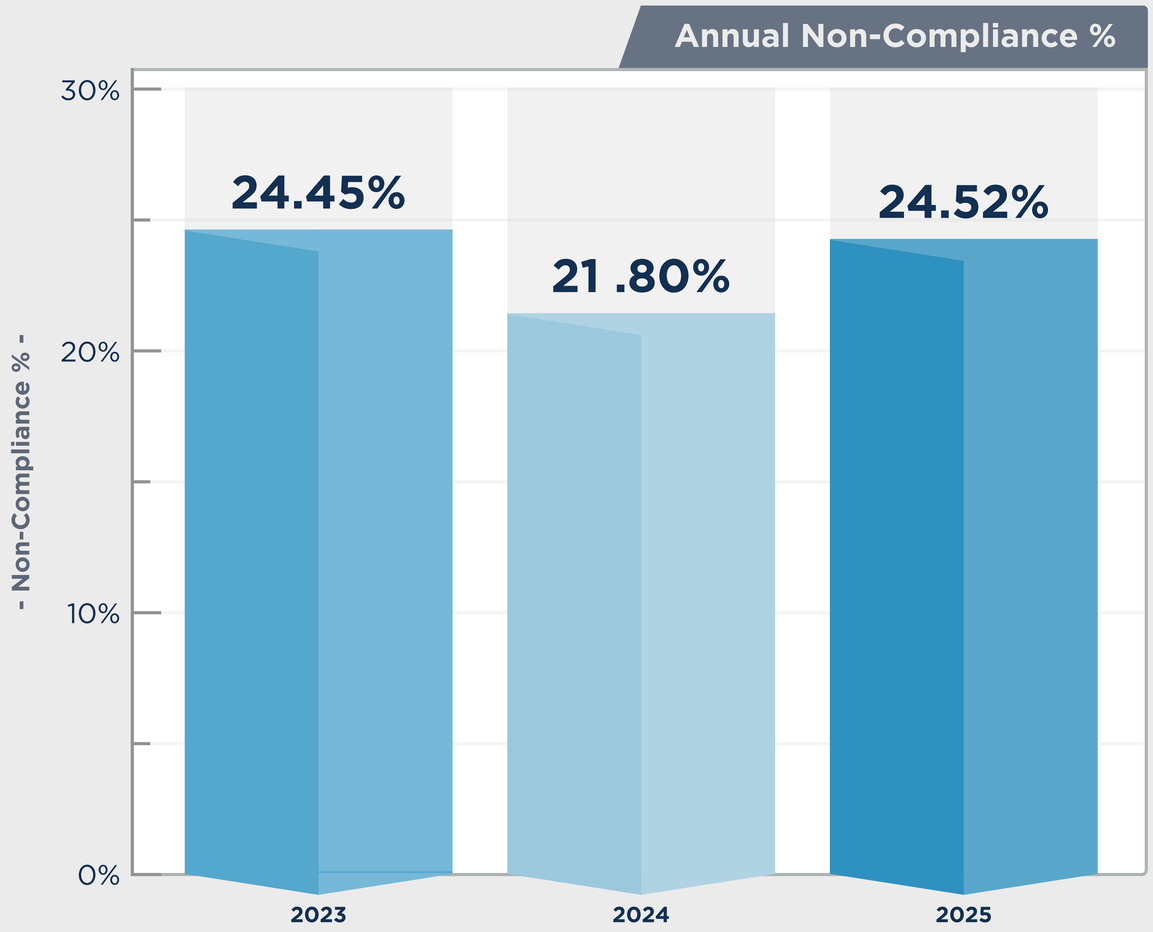
Assessment volume activity remains consistent across cycles, yet non-compliance remains flat, indicating execution, not awareness, is the systemic barrier

Assessment Activity Reflects Reassessment Cycles



TPN assessments occur on a two-year cycle; annual volume reflects timing, not linear growth

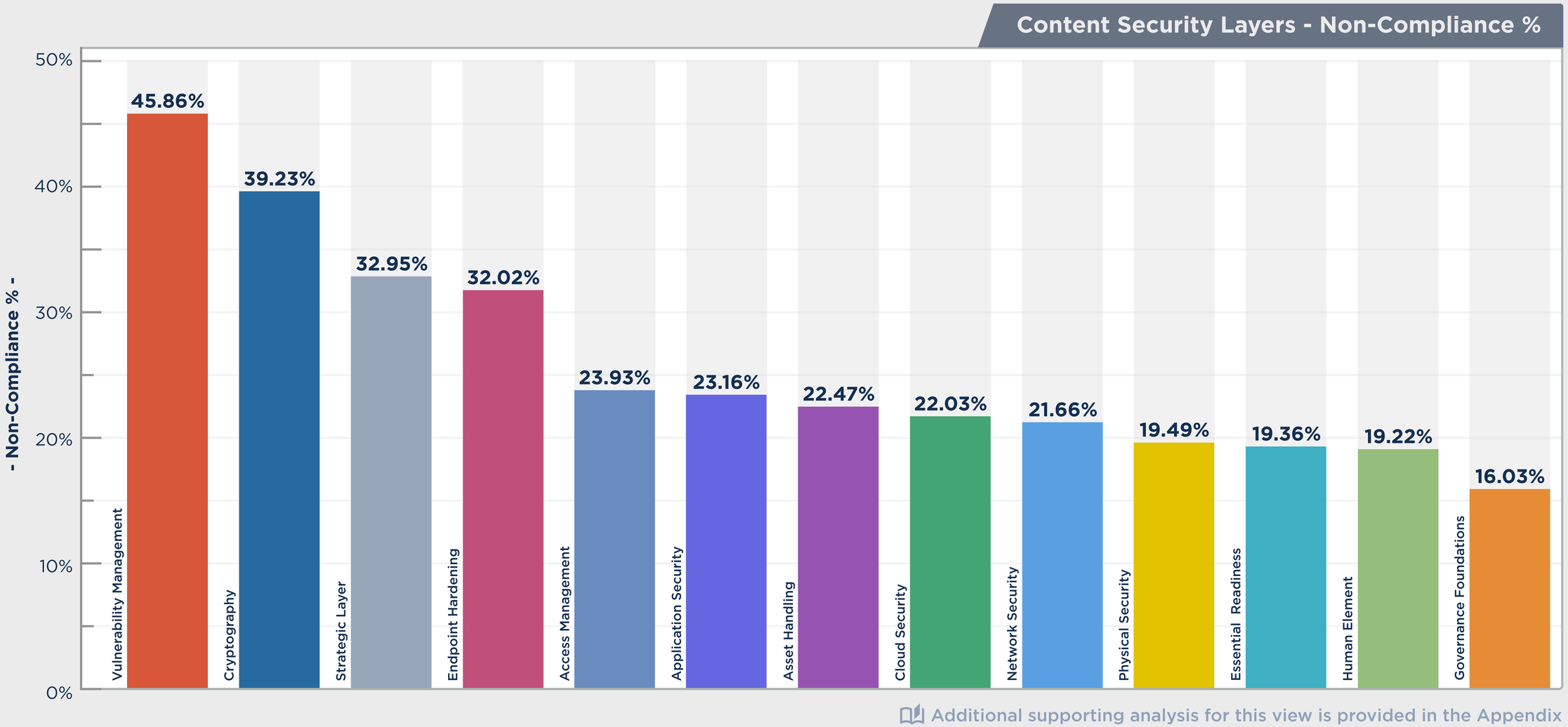
23.45%
Overall Non-Compliance



Data Context: Annual non-compliance reflects results by assessment year; overall non-compliance reflects aggregated findings across multiple assessment cycles

Root Cause: Security maturity is constrained by operational execution, not policy adoption

- The largest security gaps sit in operational technical controls
- Vulnerability Management, Cryptography, and Endpoint Hardening show the highest non-compliance
- Sustaining continuously managed controls, not defining policies, is the primary challenge



Additional supporting analysis for this view is provided in the Appendix

For public reporting, MPA Content Security Best Practices were mapped to Content Security Layers to provide aggregated and comparable maturity insights while avoiding disclosure of control-level vulnerabilities

Data Context: Strategic Layer results (ZTA and AI/ML) are based on a smaller assessment sample and should be interpreted directionally rather than as representative of industry-wide maturity

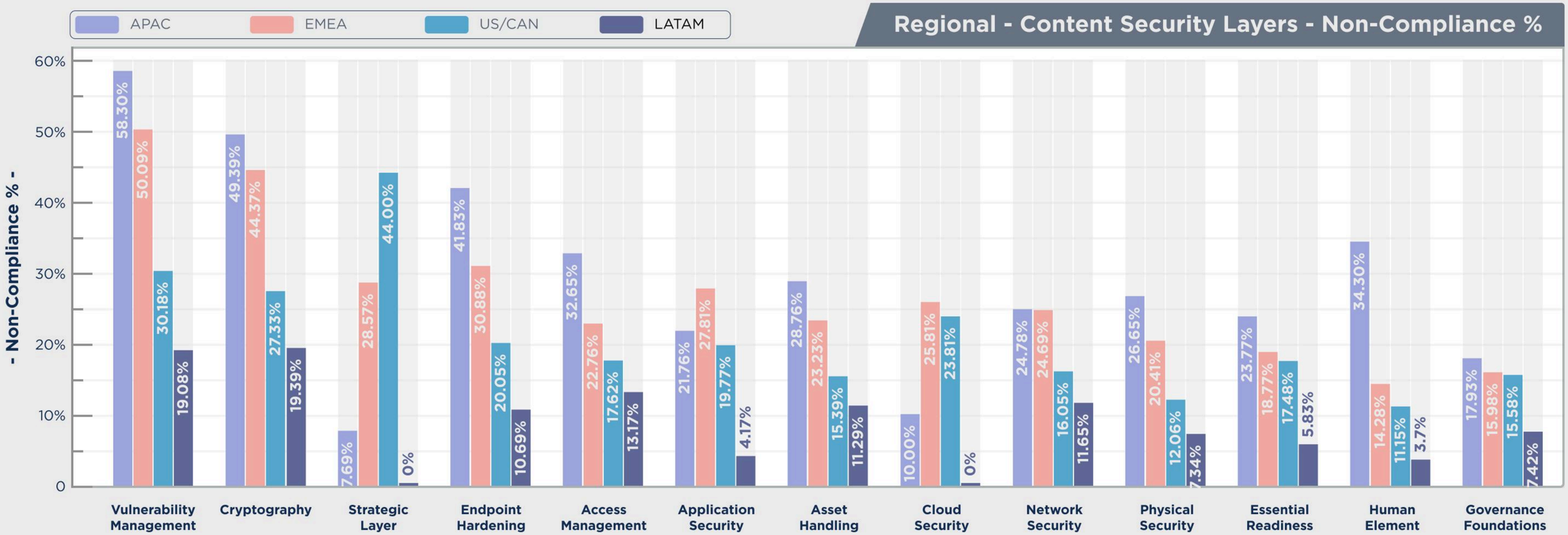
Data Analytics & Insights

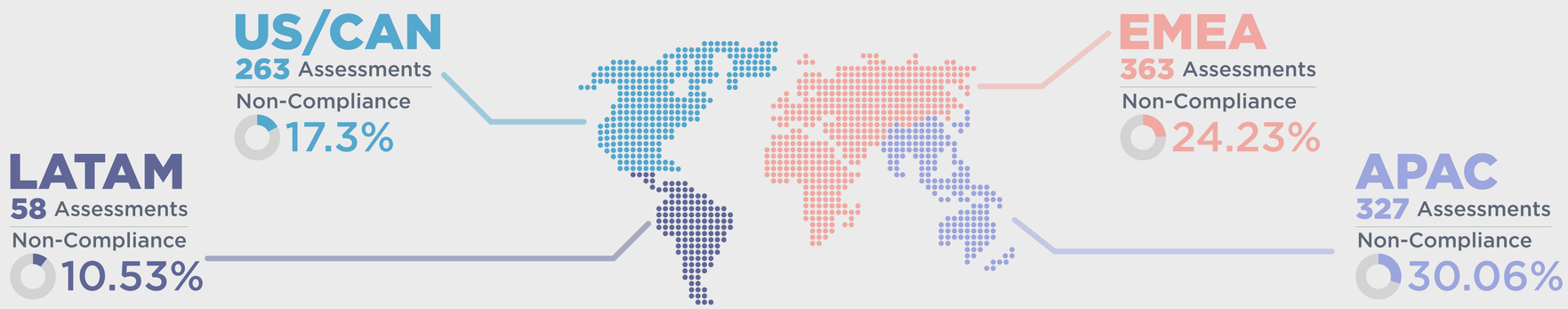
ORGANIZATIONAL DIMENSIONS

How does security maturity vary across regions, annual gross revenue and organizational size?

Vulnerability Management and Cryptography Lead Non-Compliance Across All Regions

- APAC (30.06%) and EMEA (24.23%) show the highest assessment volume and security gaps
- Vulnerability Management is the most persistent global risk (up to 58.30%)
- US/CAN Strategic Layer non-compliance peaks at 44%, reflecting early technology adoption

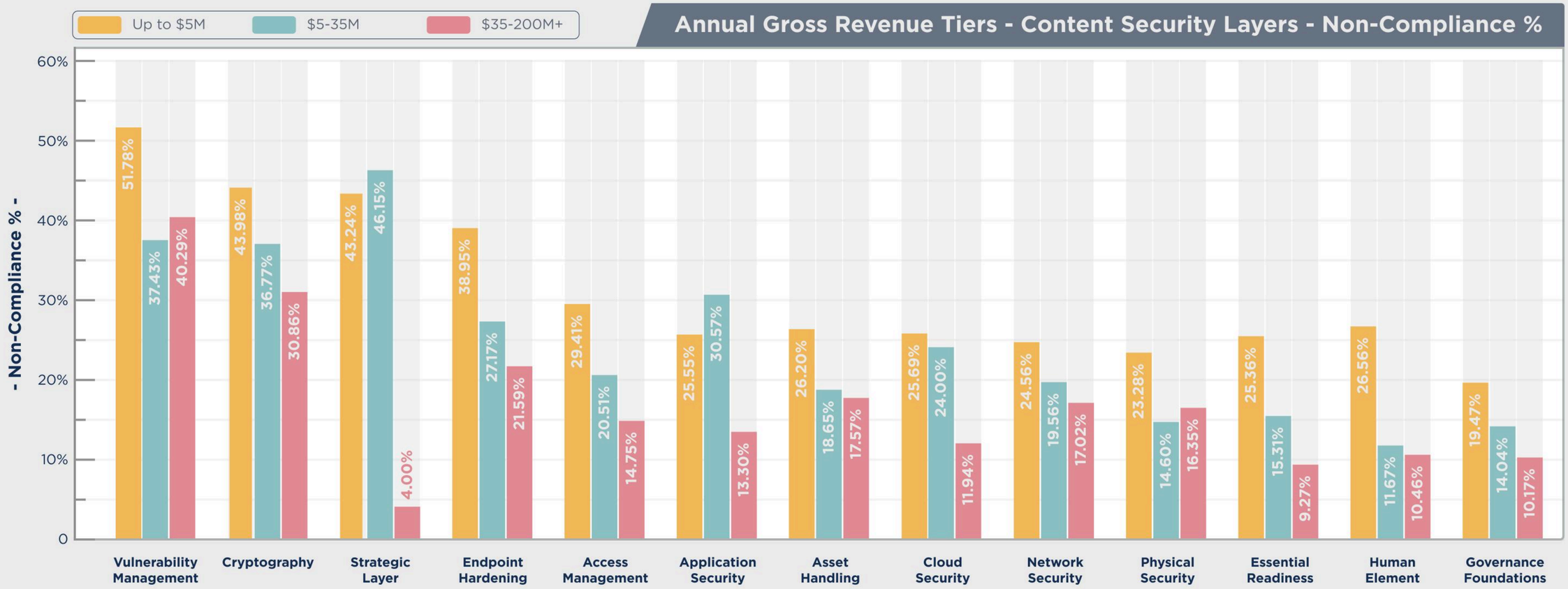




Data Context: LATAM results are based on a smaller assessment sample and should be interpreted directionally rather than as representative of region-wide maturity

Revenue Scale Improves Maturity, But Core Gaps Persist

- Security maturity improves with revenue scale, with overall non-compliance declining from 26.14% (up to $5M) to 16.84% ($35M+)
- Operational technical controls, especially Vulnerability Management and Cryptography remain the highest security gaps across all revenue tiers
- Increased resources strengthen baseline security, but do not resolve the industry's core challenge of sustaining continuously managed controls



Assessed Organization Annual Gross Revenue (AGR)

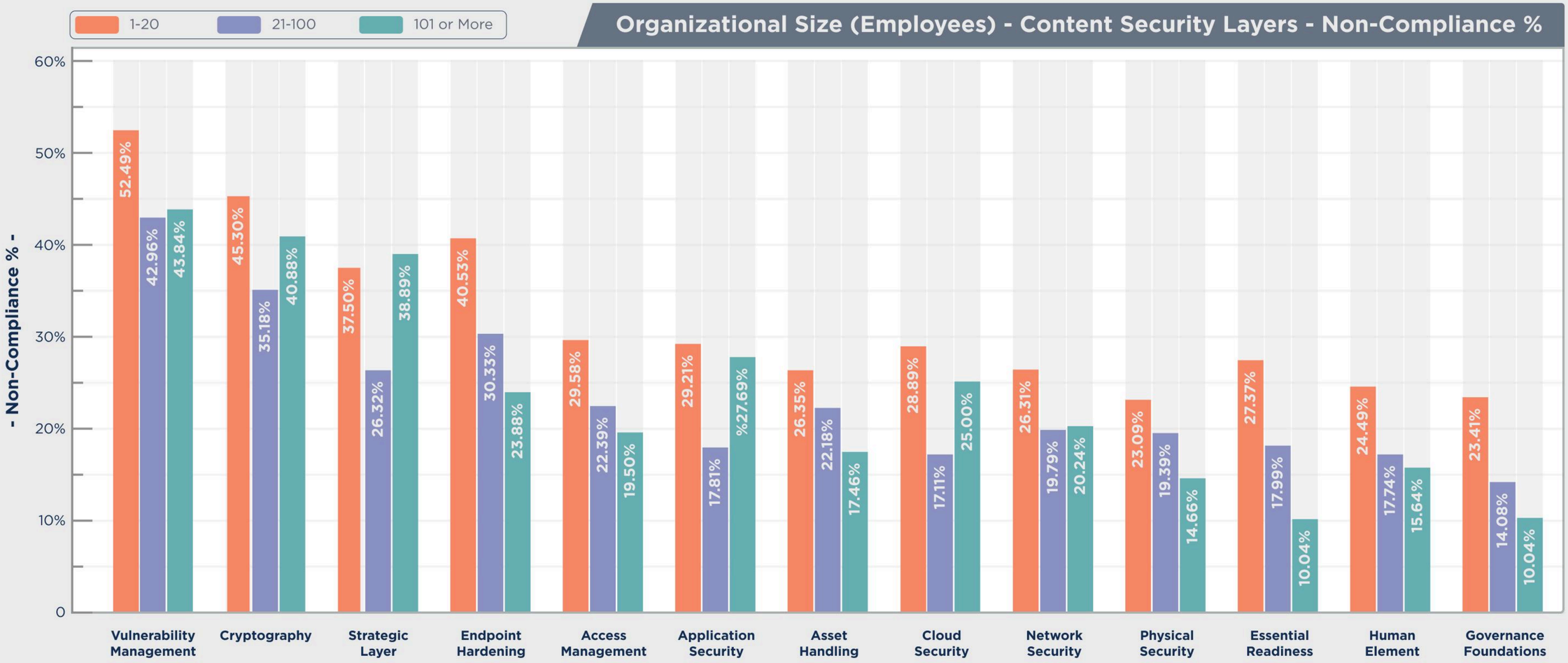
Up to $5M
Assessments **549**
Non-Compliance 26.14%

$5-35M
Assessments **223**
Non-Compliance 19.67%

$35-200M+
Assessments **229**
Non-Compliance 16.84%

Improvements Vary by Organization Size, With Diminishing Gains at Scale

- Overall non-compliance declines from 29.16% (1-20 employees) to 19.46% (101+ employees)
- Vulnerability Management and Cryptography remain persistent challenges across all tiers
- The lowest non-compliance occurs in mid-sized organizations, with diminishing returns at scale



Organizational Size (Employees)

1-20
Assessments **293**
Non-Compliance 29.16%

21-100
Assessments **538**
Non-Compliance 21.86%

101 or More
Assessments **180**
Non-Compliance 19.46%

Data Analytics & Insights

OPERATIONAL EXECUTION GAP

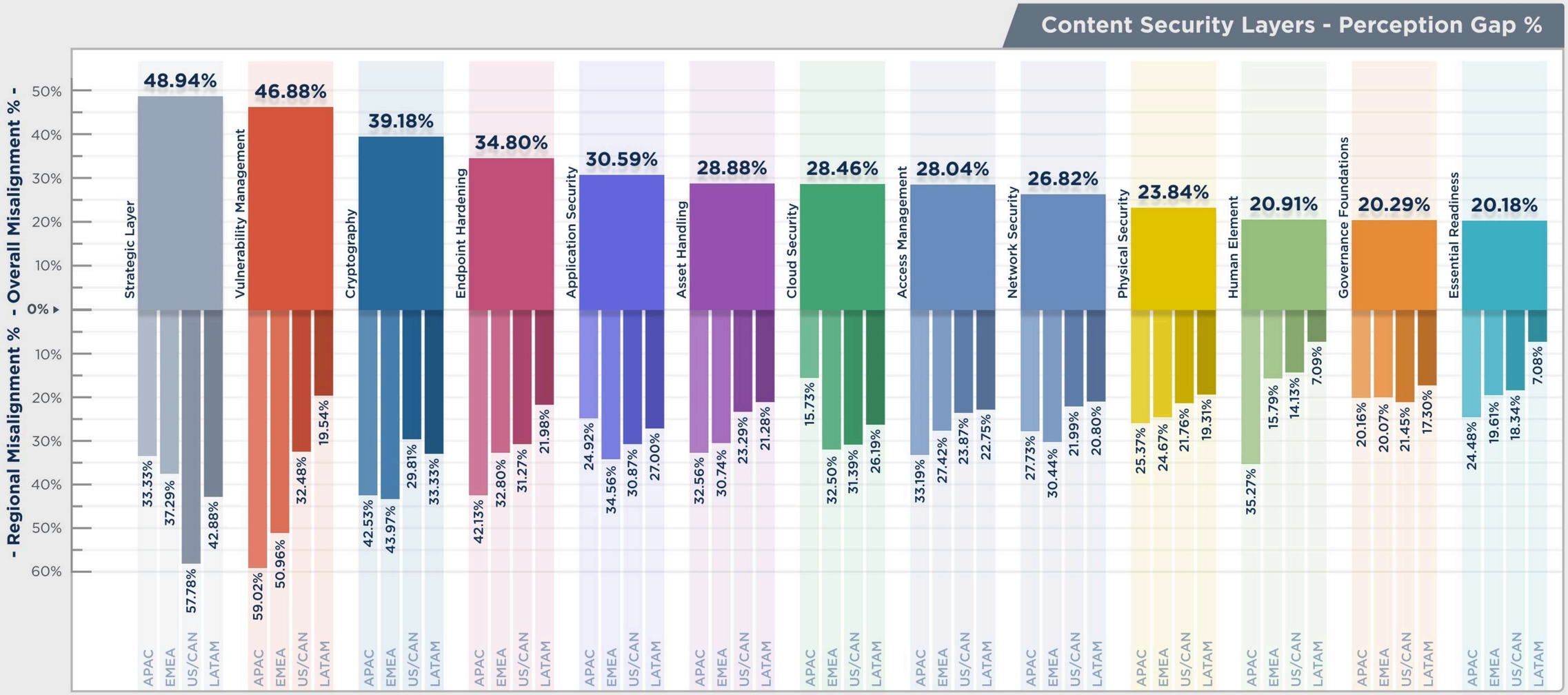
Where do gaps persist between perceived maturity, validated performance, and remediation outcomes?

> The data is showing a clear shift: The challenge is no longer in implementing policies; it's in maintaining operational discipline. Closing the execution gap will define the next phase of security maturity.
>
> ***Crystal Pham - Trusted Partner Network***
> ***Vice President Operations & Program Management***

Organizations Overestimate Their Security Maturity

A significant gap exists between perceived and assessor-validated effectiveness, particularly in operational technical domains:

- The largest perception gaps appear in Strategic Layer, Vulnerability Management, Cryptography and Endpoint Hardening
- Overestimation is most pronounced in emerging capabilities with US/CAN showing the highest Strategic Layer misalignment, indicating faster adoption without corresponding maturity
- Misalignment between self-attested responses and assessor findings is consistent across regions, revenue tiers and organizational sizes



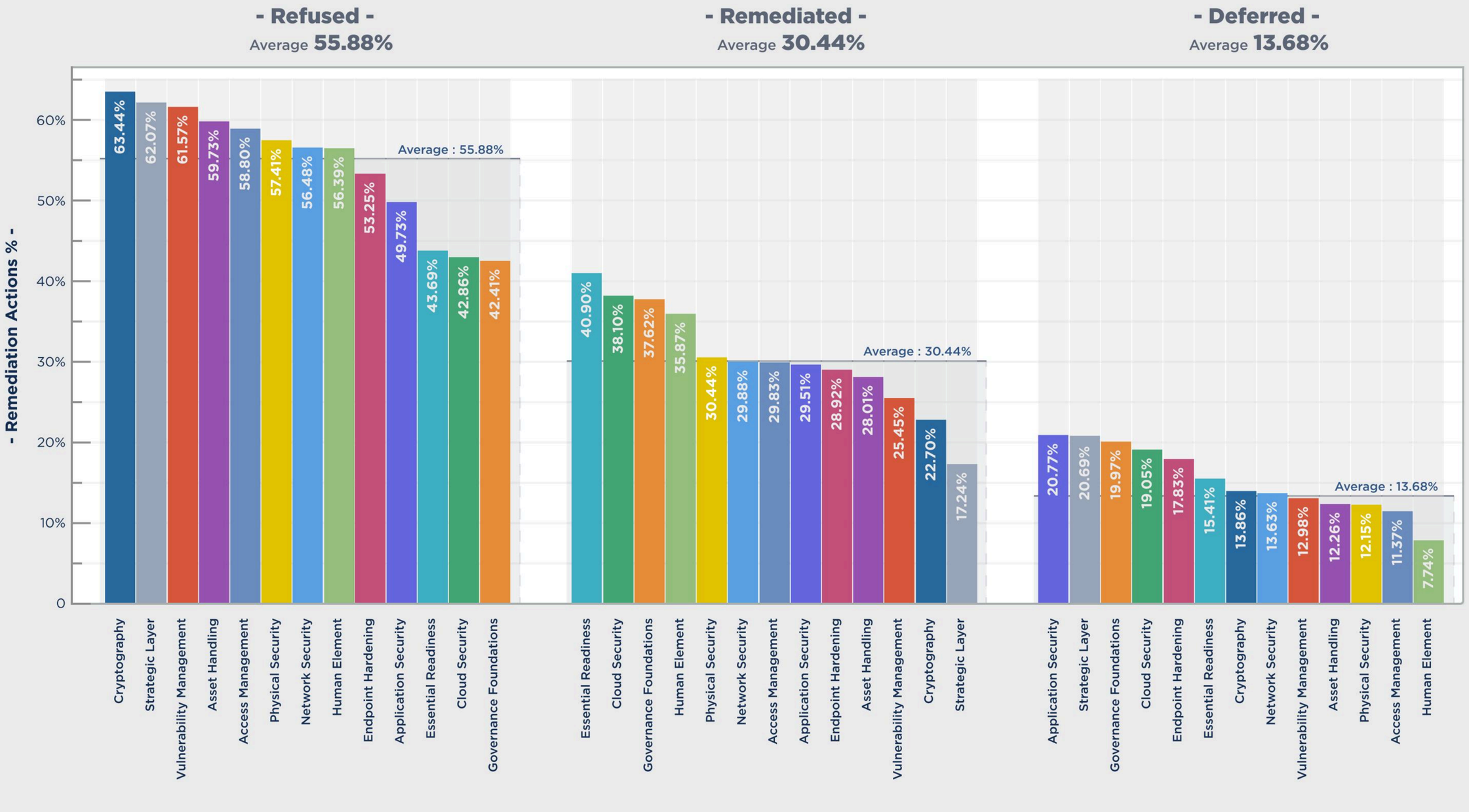
Additional supporting analysis for this view is provided in the Appendix

This analysis compares self-attested responses with independent assessor-validated findings. Any divergence between the two is treated as a perception gap, highlighting differences between perceived control effectiveness and verified operational performance

70% of Security Gaps Remain Unresolved

- Highest remediated rates occur in policy-driven layers (Essential Readiness and Governance Foundations) reflecting preference for lower cost/effort remediation - while Cloud Security similarly achieves stronger remediation despite greater technical complexity
- Majority of technically intensive layers (Cryptography, Strategic Layer, Vulnerability Management) show the lowest remediation correlating to higher cost and complexity

Remediation Outcomes by Content Security Layers



Larger Organizations Take 3x Longer To Remediate Than Mid-Sized Peers

- Refusal rates exceed 50% across all regions and organizational dimensions
- Larger organizations take the longest to remediate (230+ days)
- Mid-sized organizations resolve findings fastest (73-82 days)
- APAC shows the fastest turnaround, but also the highest refusal rate alongside the US/CAN (~60%)

Remediation Outcomes by Organizational Dimensions

Regions	Remediated (%)	Deferred (%)	Refused (%)	Avg Days to Remediate
APAC	29.42%	10.60%	**59.98%**	**76**
EMEA	31.22%	18.69%	50.08%	145
LATAM	37.04%	10.80%	52.16%	156
US/CAN	30.15%	10.61%	**59.23%**	110
Annual Gross Revenue (AGR) Tiers				
Up to $5M	29.27%	14.30%	56.42%	82
$5-35M	32.33%	16.03%	51.64%	**73**
$35-200M+	32.57%	8.60%	58.83%	**256**
Organizational Size (Employees)				
1-20 Employees	28.52%	14.97%	56.51%	91
21-100 Employees	30.01%	14.96%	55.30%	**82**
101+ Employees	36.20%	7.46%	56.34%	**233**

Larger organizations require significantly more time to remediate, while faster timelines do not consistently correspond to higher remediation rates

Data Analytics & Insights

OPERATIONAL RISKS

How prepared are organizations to detect, respond, and manage operational security risk?

> In today's distributed production environment, security gaps across the supply chain create real points of exploitation. Weak operational controls don't just increase risk; they create pathways for intellectual property theft, digital piracy, and organized criminal activity. Closing these gaps is essential to protecting creators, safeguarding consumers, and disrupting the criminal networks that profit from security gaps.
>
> ***Larissa Knapp - Motion Picture Association***
> ***Executive Vice President and Chief Content Protection Officer***

Essential Readiness Strengthens with Organizational Scale, but Training Gaps Persist

- Operational readiness improves with scale, reflecting stronger capabilities in response and recovery
- Regional variation is most pronounced in Training & Awareness; APAC has the highest non-compliance

Essential Readiness - Best Practice Non-Compliance %

Across regions, revenue tiers, and organization sizes, Training & Awareness consistently shows the highest non-compliance among Essential Readiness Best Practices

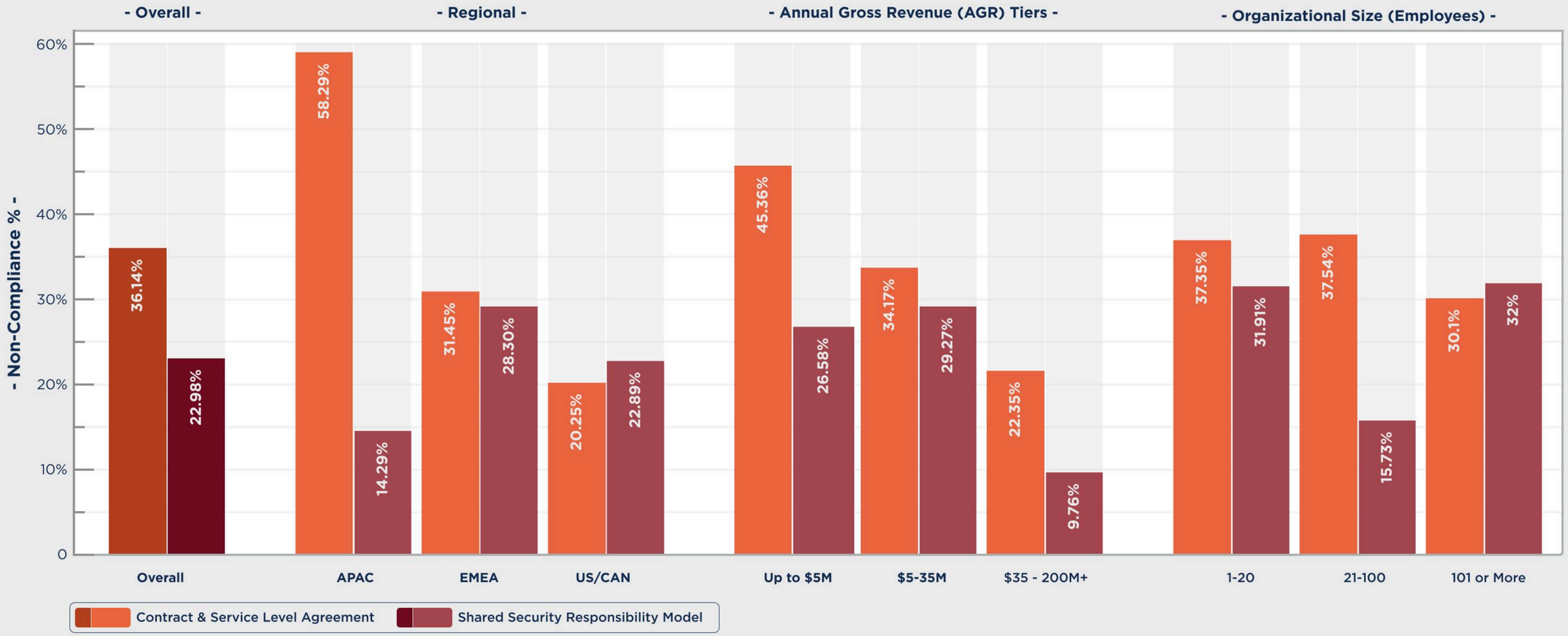
Essential Readiness reflects an organization's ability to detect, respond and recover from security incidents

Data Context: BC & DR Plan = Business Continuity Plan & Disaster Recovery

Third-Party Risk Remains Material Across Models, Regions, and Organizational Tiers

Although Contract Service Level Agreement non-compliance is higher, the persistence of security gaps across both contract-led and shared responsibility models confirms Third-Party Risk Management as an ongoing execution challenge, not a one-time contractual or structural issue

- Security gaps vary widely by region, but no region demonstrates consistently low third-party non-compliance
- Higher revenue and larger organizational size show improvement, yet non-compliance remains meaningful even at scale



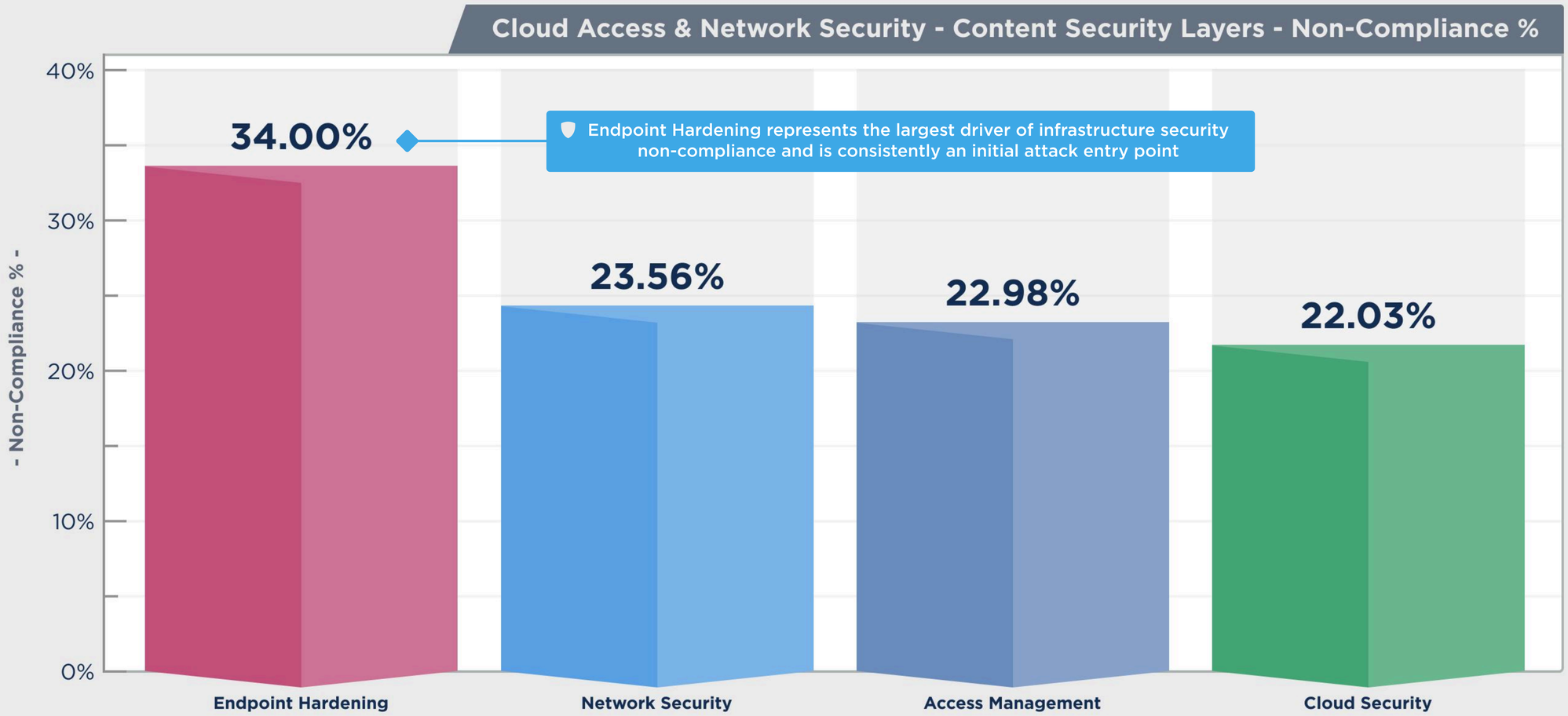
Third-Party Risk Management (TPRM) manages security risks introduced by vendors and partners across production workflows and the supply chain

Data Context: LATAM excluded due to insufficient sample size

Endpoint Hardening Drives Infrastructure Security Risk Across Production Environments

Cloud Access & Network Security risk is driven by execution gaps, with Endpoint Hardening as the leading weakness with variation emerging by organization size and region

- Endpoint Hardening has the highest non-compliance overall, while improvements in general scale with revenue
- APAC risk is concentrated in Endpoint Hardening and Network Security, whereas EMEA and US/CAN show higher non-compliance in Access Management and Cloud Security, indicating region-specific execution gaps across identity and cloud controls



Additional supporting analysis for this view is provided in the Appendix

Cloud Access & Network Security protects connectivity, identity interaction, and data flow across on-premise, cloud, and hybrid environments

DATA ANALYTICS

Data Analytics & Insights

TIMELINES

What drives time from risk identification to remediation across the assessment lifecycle?

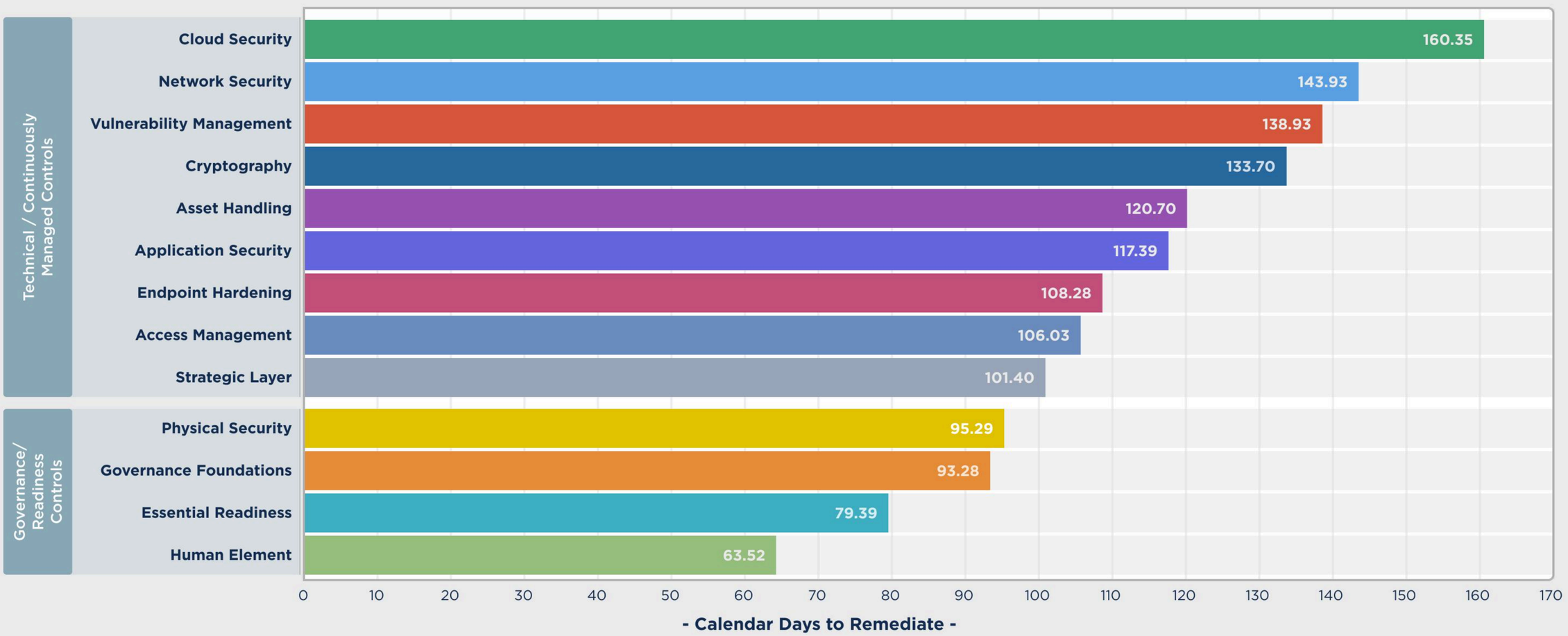
Technically Intensive Controls Drive the Longest Remediation Timelines

- Cloud and Network Security, Vulnerability Management and Cryptography have the longest remediation timelines (130-160 days)
- Governance and readiness controls resolve more quickly (64-95 days)

112.34

Overall Average Days to Remediate

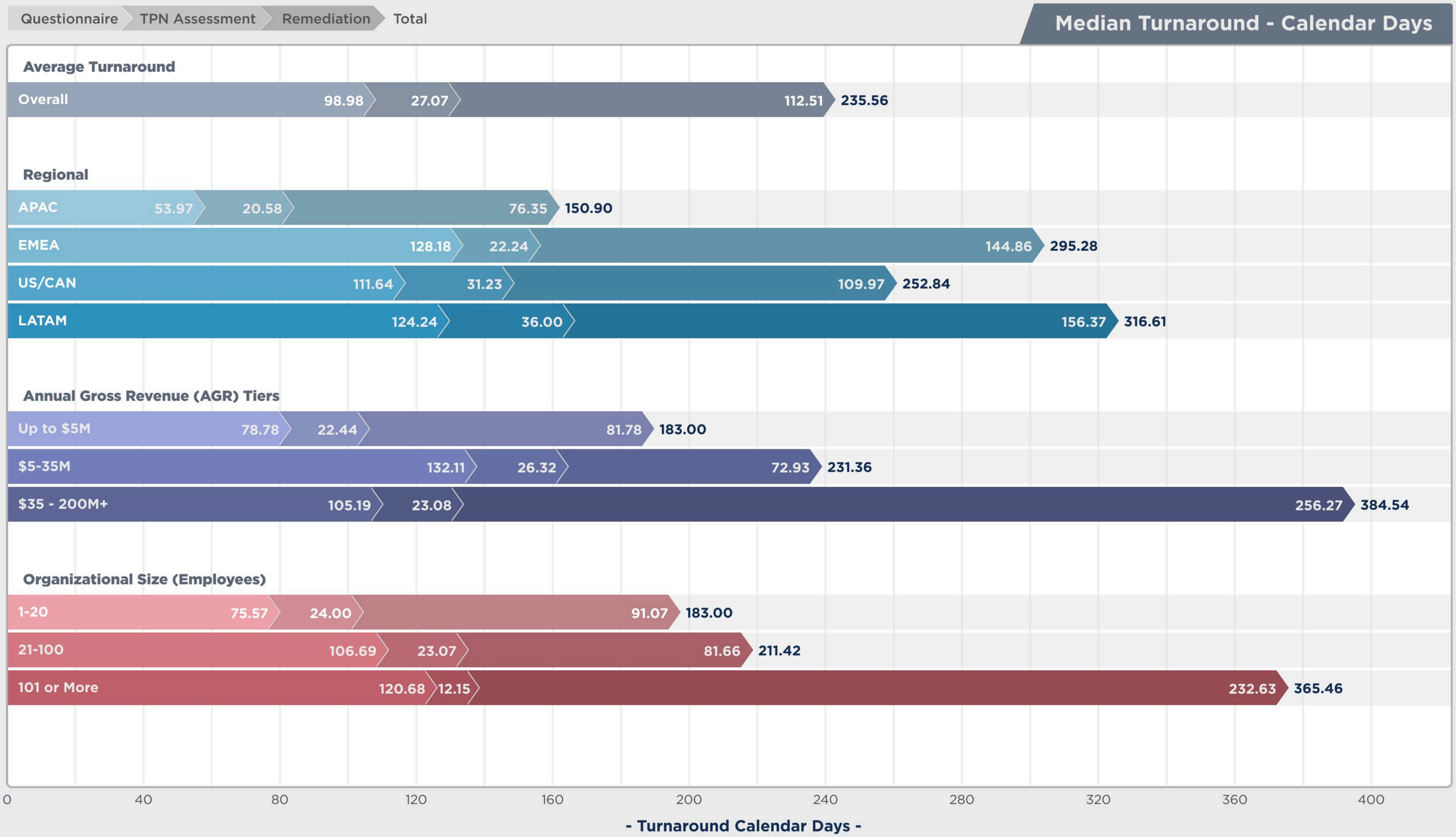
Remediation in technical domains takes up to 2.5x longer than in governance and readiness controls



Time to Identify and Resolve Risk is Driven by Internal Execution

Improving internal execution is the fastest way to accelerate risk identification and remediation

- Self-attested questionnaire completion introduces long timeline delays for risk identification
- TPN assessment timelines are comparatively consistent and short within established SLA
- Remediation extends the overall timeline significantly, delaying time to risk resolution



Data Analytics & Insights

PROGRAM IMPACT

How does continued participation in a security program influence security maturity over time?

> The MPA 360 Strong strategy brings preparedness and enforcement together - TPN strengthening readiness, and the Alliance for Creativity and Entertainment (ACE) advancing content protection. Meaningful reductions in non-compliance are critical because enforcement is only effective when the ecosystem is fundamentally prepared. Raising baseline security rigor across the supply chain strengthens deterrence, reduces incident risk, and ensures the industry can respond from a position of strength.

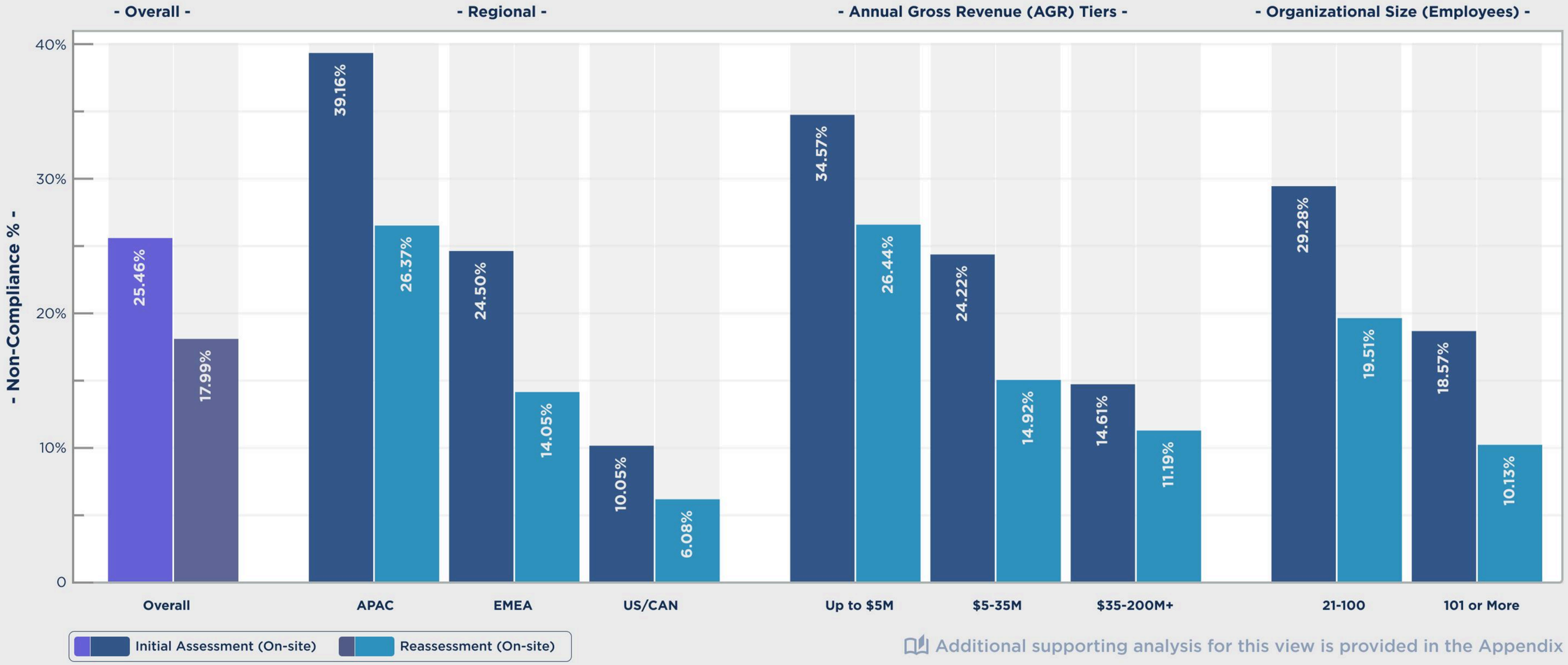
Karyn Temple - Motion Picture Association
Senior Executive Vice President and Global General Counsel

Reassessment Reduces Risk by 29%, But Fewer than Half of Organizations Reassess

Among organizations active in TPN for two years, only 34.41% complete a reassessment, even though reassessment clearly reduces risk over time; over half have annual gross revenue under $5M:

- Non-compliance declines by ~29% between initial assessment and reassessment (25.46% → 17.99%)
- Greatest technical control improvements in reassessments are seen in Cryptography, Endpoint Hardening, and Network Security
- Reduction in non-compliance is consistent across regions, revenue tiers, and organizational size

Reassessment Improvements



Additional supporting analysis for this view is provided in the Appendix

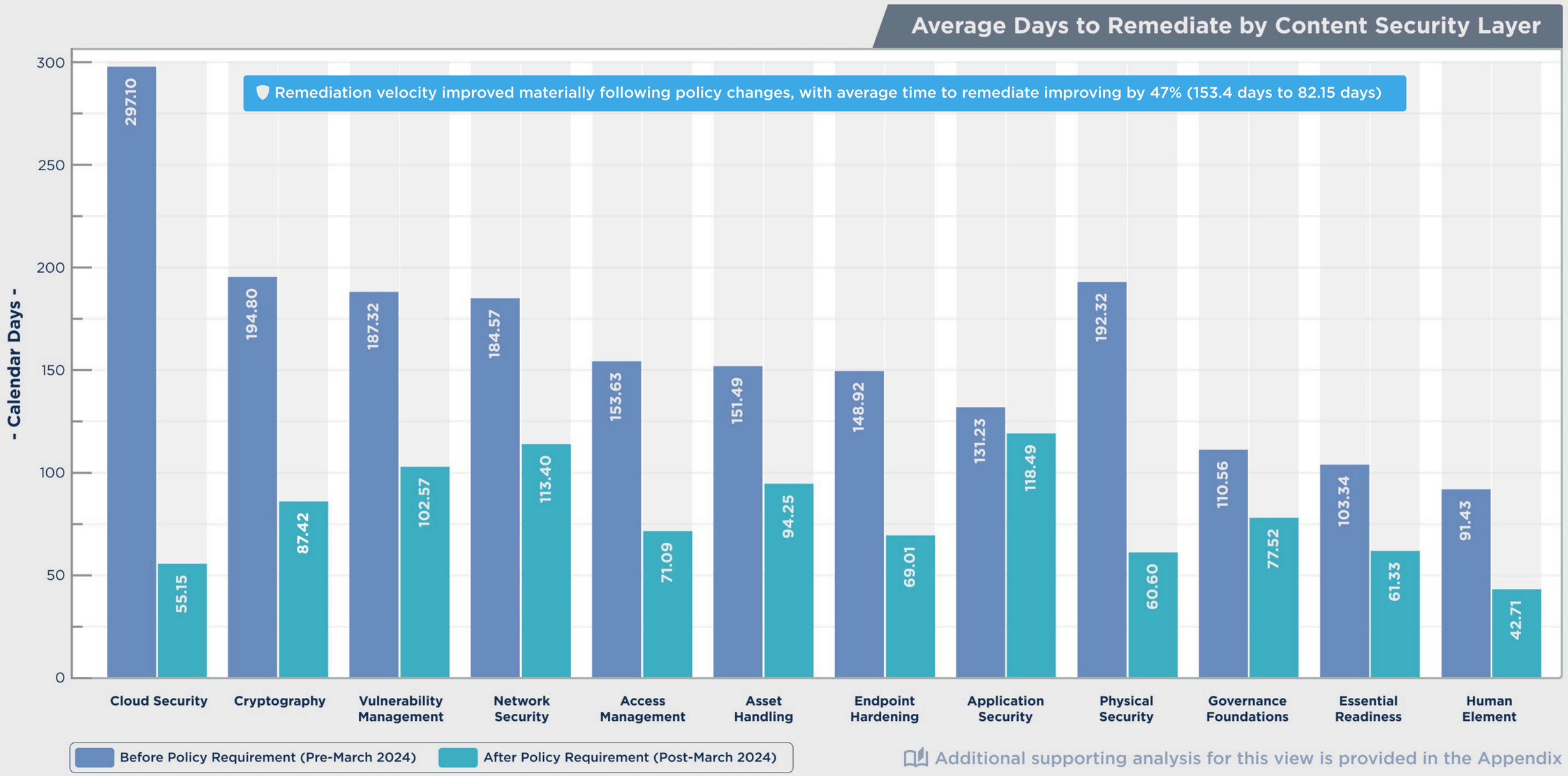
Data Context: Reassessment analysis included on-site assessments only; LATAM and Organizational Size 1-20 excluded due to insufficient sample size

In March 2024, TPN introduced a policy linking TPN Shield issuance to submission of a formal remediation plan, fundamentally changing remediation behavior

Shield-Linked Incentives Cut Remediation Time Nearly In Half

Average days to remediate improved by 47%, and remediation behaviors also improved after the policy introduction:

- Remediation volume improved (30.81% → 37.69%)
- Refusal rates declined materially (62.66% → 43.87%), indicating greater engagement with remediation
- Deferred remediation increased (6.53% → 18.44%), reflecting a shift toward remediation planning



Additional supporting analysis for this view is provided in the Appendix

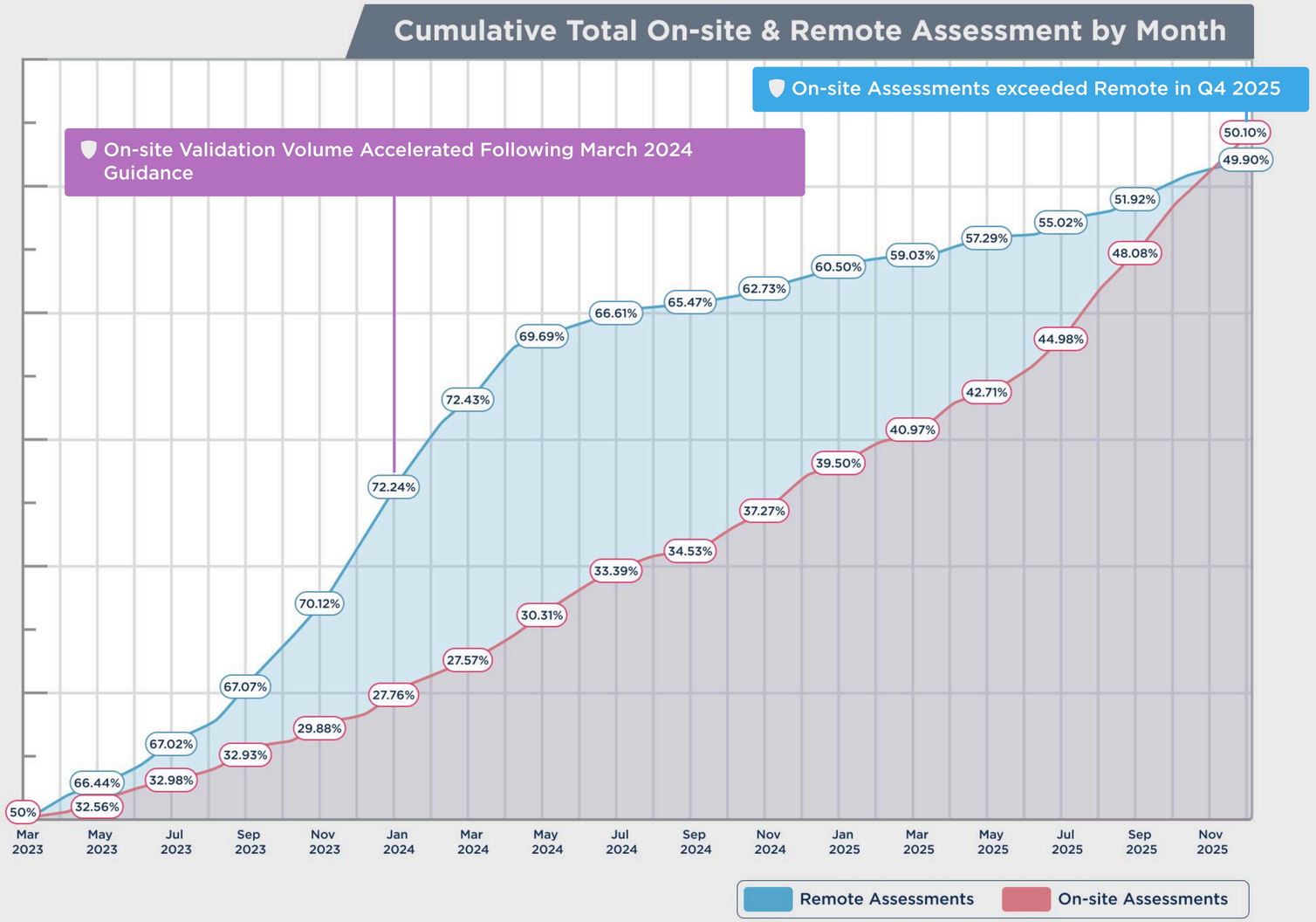
Following COVID-era reliance on remote assessments, TPN guidance in March 2024 re-prioritized on-site evaluations to strengthen assessment rigor

TPN Guidance Drives Shift to On-site Validation to Strengthen Assessment Rigor

Following March 2024 guidance, on-site assessments increased steadily and overtook remote assessments by Q4 2025, reversing prior assessment patterns, and achieving the following:

- Direct assessor validation of controls within live operational environments
- Reduced reliance on documentation as primary assessment evidence
- Greater confidence that controls operate effectively in practice, not just by design

On-site validation became the dominant assessment method by Q4 2025



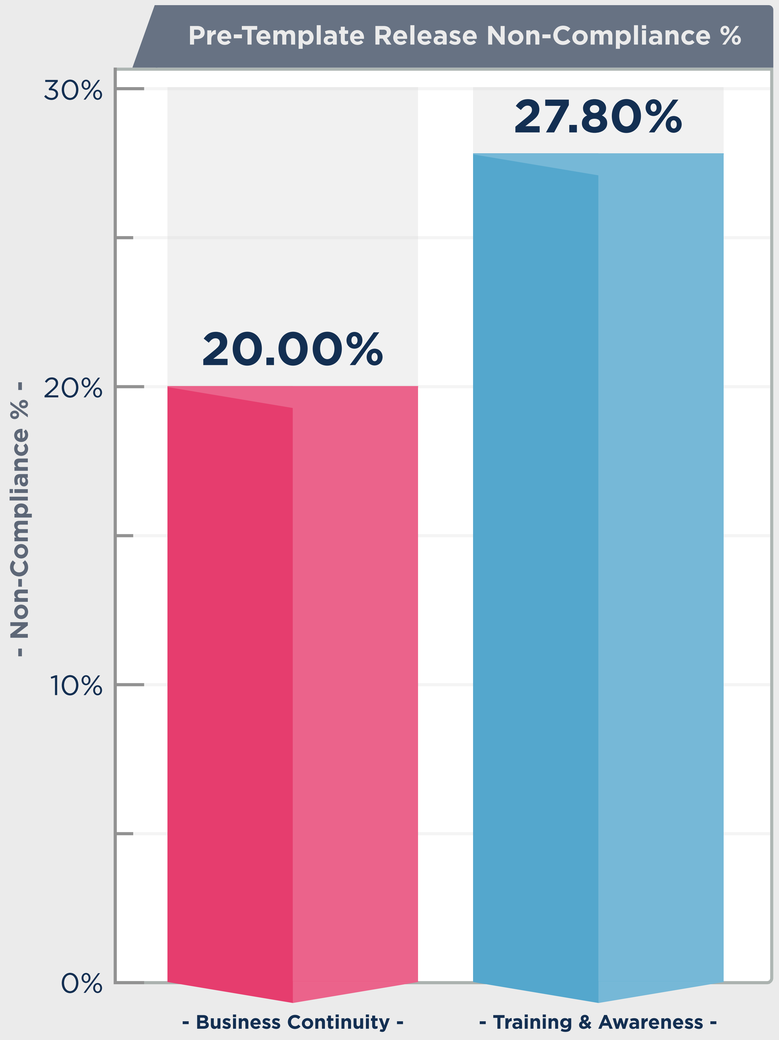
In January 2025, TPN launched free policy templates to support foundational security practices across the industry

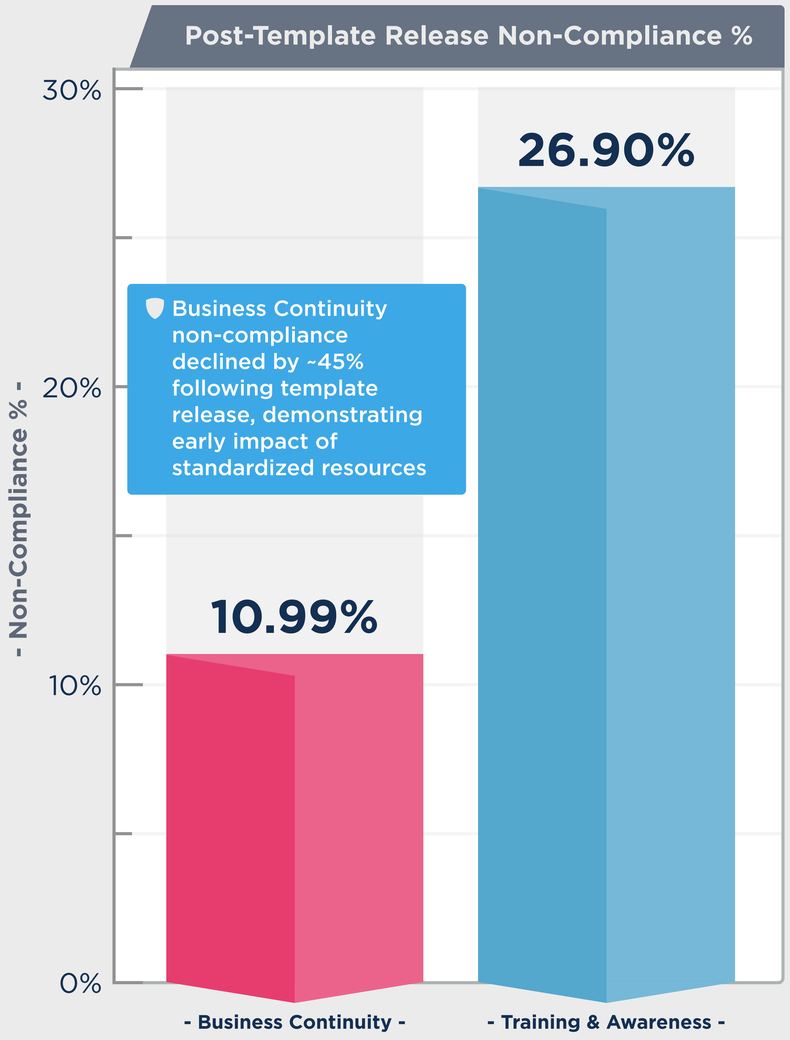
Free Security Resources Drive Measurable Improvements in Foundational Controls

Accessible, policy-driven resources deliver measurable improvements in both compliance and remediation speed

- Remediation timelines improved by ~36%, accelerating issue resolution
- Training & Awareness shows early improvement, indicating growing adoption of standardized practices

Reducing friction through standardized resources directly improves security outcomes



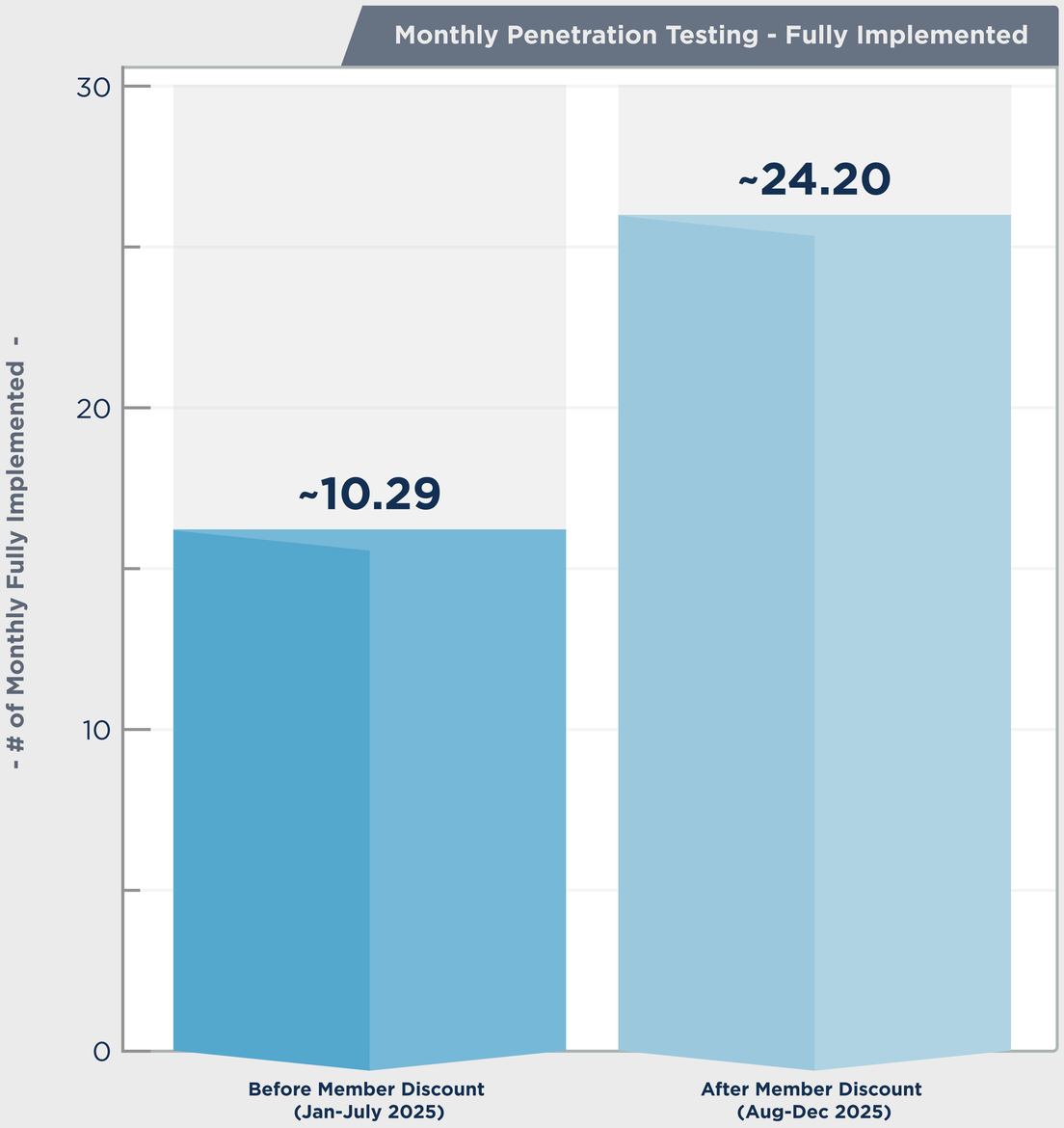


Additional supporting analysis for this view is provided in the Appendix

In August 2025, TPN introduced member discounts for penetration testing through approved partners to expand access to independent testing services

Member Discounts Drove a 135% Increase in Penetration Testing Adoption

- Reducing cost barriers led to a sustained increase in fully implemented annual penetration testing



+ 135% Increase in Monthly Adoption

- Fully Implemented responses rose from 72 (Jan-July) to 121 (Aug-Dec)
- Monthly fully implemented adoption increased from ~10 to ~24 organizations

Data Context: Adoption rates reflect v5.3 only and are normalized to account for different reporting periods

Data Analytics & Insights

OPPORTUNITIES

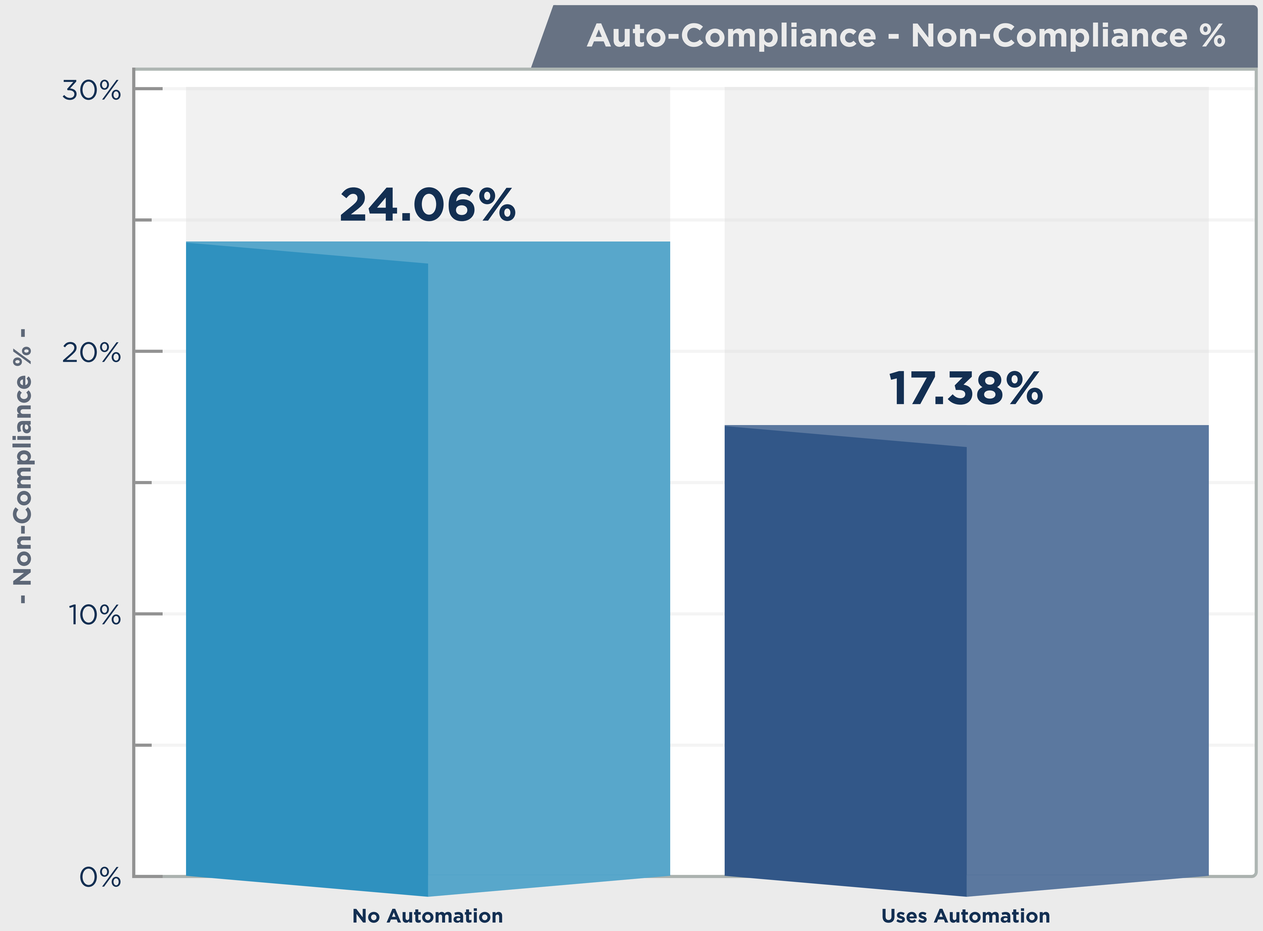
Where do adoption gaps limit execution and where can closing them drive measurable improvement?

Low Adoption Limits the Industry-Wide Impact of Automated Compliance Tools

When adopted, automated compliance extends security assessments by enabling continuous visibility into control performance and earlier detection and remediation

- Organizations using automated compliance tools report materially lower non-compliance, with the strongest improvements observed across Access Management, Application and Cloud Security, Cryptography, Endpoint Hardening, and Vulnerability Management
- Despite these gains, adoption remains below 10%, limiting industry-wide impact even as automation demonstrates clear benefits in technically measurable security layers

Non-compliance improves ~28% with adoption of Automated Compliance Tools



Additional supporting analysis for this view is provided in the Appendix

Data Context: Automation refers to automated compliance tooling used for continuous control monitoring

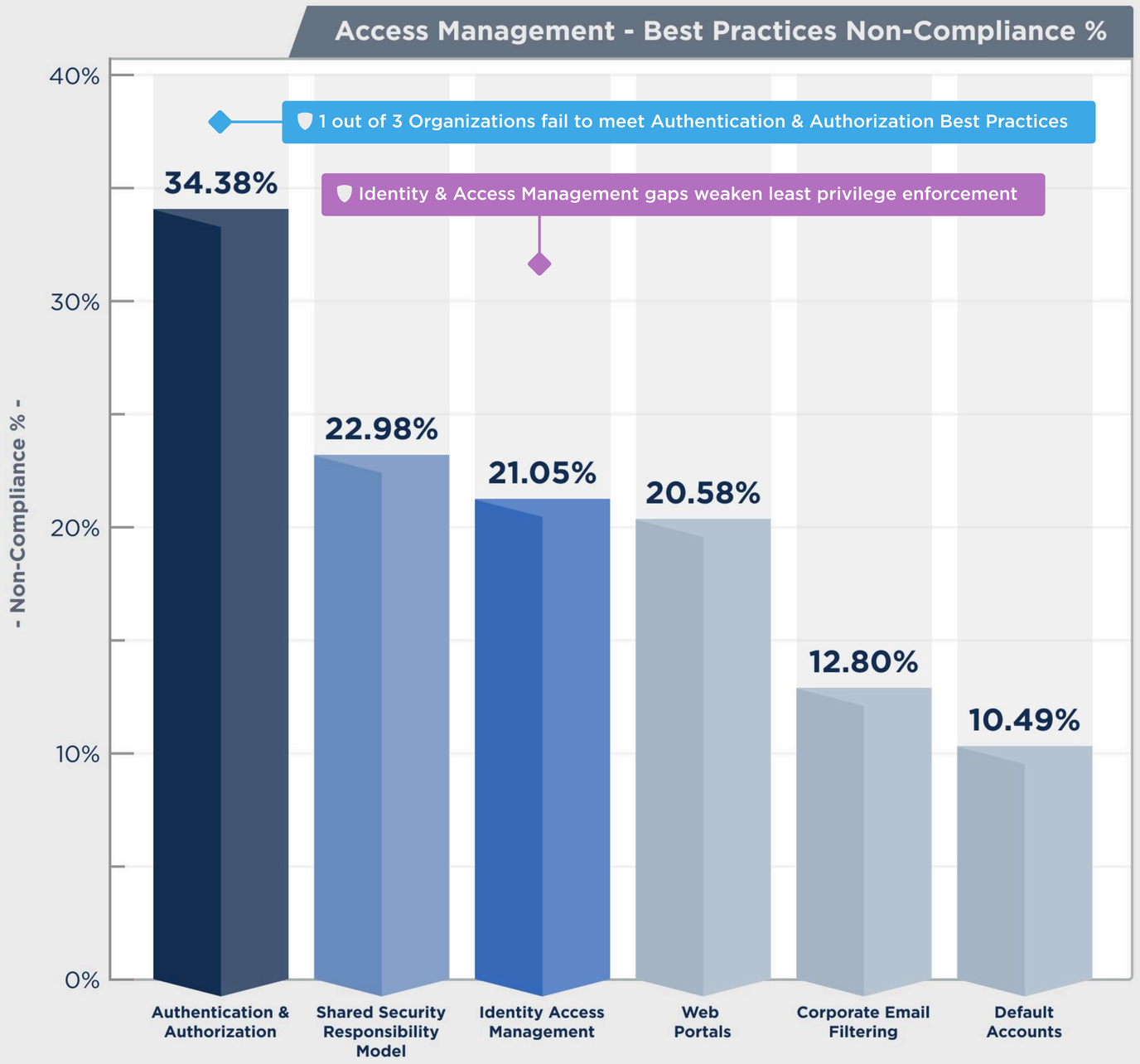
Zero Trust and Identity Security Remains a High-Impact Opportunity for Risk Reduction

- Weak authentication and access controls continue to expose organizations to credential-based attacks
- Only 13% of organizations report Zero Trust adoption - a very low level overall - yet 69% of those claims were deemed "Not Applicable" during assessor validation, indicating widespread industry confusion between true Zero Trust principles and more limited or traditional security implementations

Access Management
Overall Non-Compliance

23.93%

Identity remains a primary attack vector - yet control gaps persist



CLOSING THE EXECUTION GAP

What Immediate actions are required to drive real security improvement?

Operationalizing the industry's five urgent security priorities

	Industry Priority	Who Should Act	Recommended Actions
1	**Treat Security as a Daily Responsibility**	Service Providers	• Regularly scan, test and patch to remediate known vulnerabilities quickly • Continuously monitor devices for security issues, not just during assessments • Encrypt all content in motion and at rest, including drives, files and backups
		TPN	• Explore program enhancements and member discounts that support continuous assurance capabilities, including AI detection and monitoring
2	**Fix High-Risk Technical Gaps First**	Service Providers	• Focus first on fixing the most serious technical weaknesses, especially software vulnerabilities and the technical weaknesses most frequently linked to incidents
3	**Lock Down Identity & Access**	Service Providers & Organizations Sourcing Services	• Require multi-factor authentication (MFA) so accounts are protected even if passwords are compromised • Regularly review who has access to systems and remove access that is no longer needed
4	**Hold Vendors and Partners Accountable**	Organizations Sourcing Services	• Clearly define security expectations in contracts and SSRM with vendors • Ask vendors to provide evidence that they are meeting security requirements • Coordinate vendor oversight across procurement, security, and operational teams • Use the Trusted Partner Exchange to securely share security reports
5	**Respond Faster When Security Gaps are Found**	Service Providers	• Treat security findings as issues to act on - not just document • Schedule regular reviews to track progress and close gaps
		TPN	• Continue publishing year-over-year performance metrics in the STAR Report • Integrate MPA Best Practices and Add'l Recommendations v5.3.1 to STAR in 2027 • Track remediation improvements under the next-gen four tier Shield structure • Continue expanding free resources through the TPN+ Partner Resource Center • Launch and amplify an industry call to action for urgent awareness and action

LOOKING AHEAD

The 2026 STAR dataset establishes a baseline for how security controls perform across the global content supply chain.

Beginning in 2027, expanded coverage of Additional Recommendations and MPA Best Practices v5.3.1, combined with enhanced remediation tracking and the four-tier TPN Shield framework, will provide deeper visibility into how organizations improve over time.

The next phase of maturity will be defined by how consistently security controls operate in practice. This will require greater adoption of continuous monitoring, automation, and clearer ownership of security control performance across organizations.

Over the next 12 months, the accelerating use of AI across creative, operational, and security workflows is expected to further test these controls - amplifying identity, access, data handling, and third-party risk challenges while increasing the consequences of control gaps.

Resilience is also emerging as a critical differentiator. Capabilities such as incident response, business continuity, and disaster recovery will increasingly determine how effectively organizations manage real-world threats in a distributed and rapidly evolving production environment.

As the ecosystem continues to expand across cloud platforms, third-party partners, and identity-driven access models, sustained progress will depend on coordinated action across the industry.

APPENDIX

METHODOLOGY

This report analyzes aggregated, anonymized data derived from security assessments conducted through the Trusted Partner Network (TPN+) platform. The dataset includes questionnaire responses, assessor-validated findings, and remediation outcomes collected during the reporting period. Unlike many industry studies that rely on surveys or self-reported maturity indicators, the analysis is grounded in independently validated assessment results, enabling consistent evaluation of security control implementation across organizations participating in the TPN ecosystem.

A
DATA OVERVIEW

Reporting Period	**Feb 2023 - Dec 2025**
Data Source	**TPN+ Platform**
Regions Represented	**APAC, EMEA, LATAM, US/CAN**
Organizational Dimensions Analyzed	**Region, Annual Gross Revenue, Organizational Size**
MPA Best Practice Versions Included	**Best Practices v5.1, v5.2, v5.3**
# TPN Assessments Analyzed	**1,000+**
Turnaround Times	**Calendar Days**

B
DATASET SCOPE

In-Scope Organizations

- Service providers participating in TPN program during reporting period
- Completed at least one TPN security questionnaire and assessment

In-Scope Security Questionnaires and Assessments

- MPA Best Practices v5.1, v5.2, v5.3

Out-of-Scope Questions & Assessments

- MPA Additional Recommendations v5.1, v5.2, v5.3, v5.3.1
- MPA Best Practices v5.3.1

METHODOLOGY

C
DATASET SOURCES

Data sources include:

- TPN+ platform as system of record
  - Assessor-validated security findings
  - Questionnaire responses
  - Remediation plans

D
DATASET INCLUSION & NORMALIZATION

Dataset Inclusion Criteria

- Paid TPN members
- Completed questionnaires
- Published assessments
- Published remediation plans
- Company-level address, Membership AGR tier, Organizational Size (Employees)
- Site-level address

Framework Version Normalization

Because the MPA Content Security Best Practices evolve over time, controls from versions v5.1, v5.2, and v5.3 were normalized into a common set. When controls were expanded or restructured between versions, responses were mapped so results could be compared consistently across reporting periods.

For example, Business Continuity Plan and Disaster Recovery were combined in versions 5.1 and 5.2 but separated in v5.3. For consistent analysis across versions, responses to these controls are combined into a single normalized BCP/DR control.

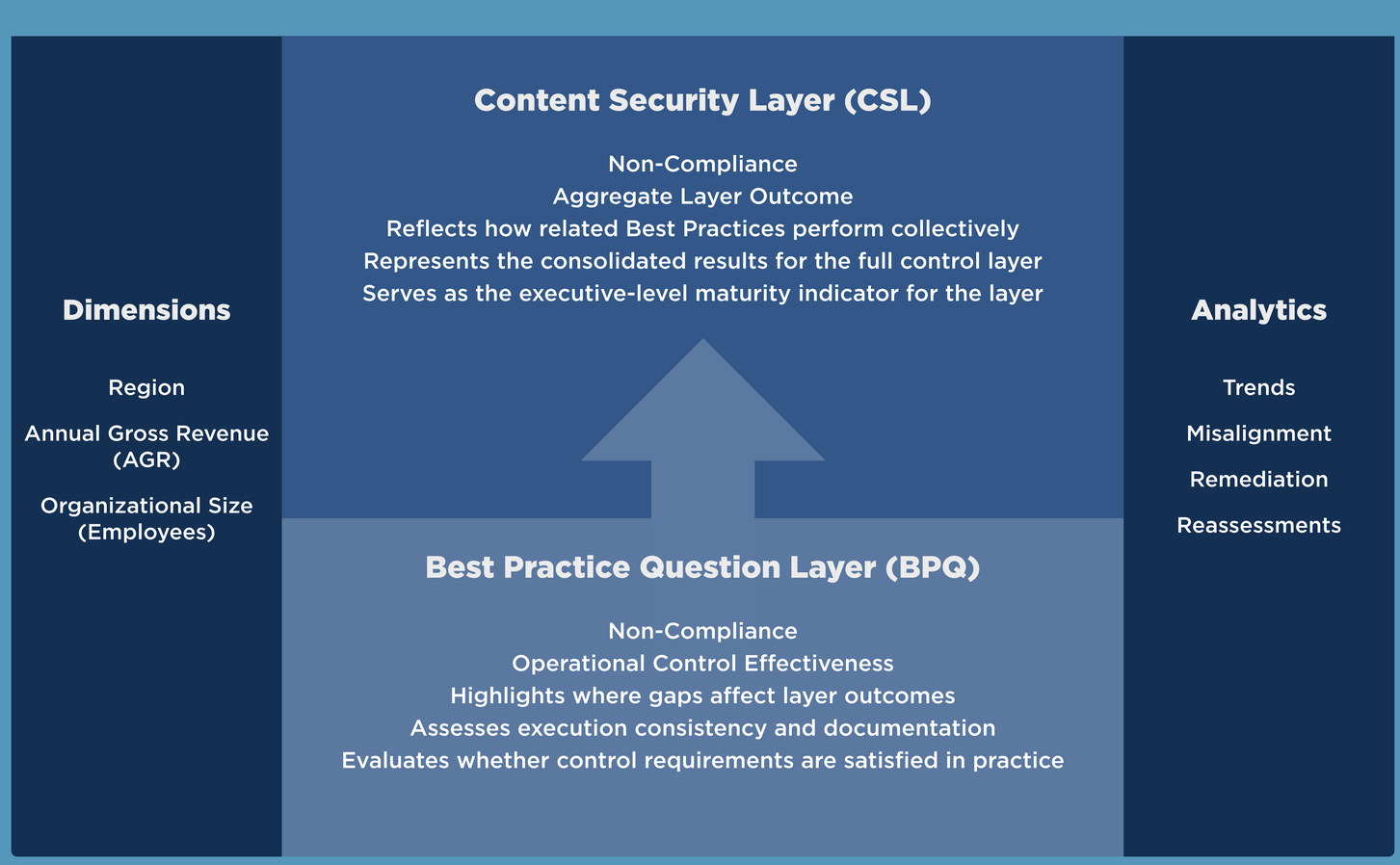
METHODOLOGY

E
ANALYTICAL FRAMEWORK

The 2026 STAR Report measured non-compliance for MPA Best Practice v5.1, v5.2 and v5.3 at both the Best Practice Question level and the aggregated Content Security Layer. This two-tier model provided a consistent and reliable view of operational effectiveness and aggregate layer outcomes.

TPN 2026 STAR Report - Hierarchical Data Model (MPA BP v5.1, v5.2 & 5.3)

The 2026 STAR reporting model measures non-compliance across two tiers: Best Practice Questions v5.1, v5.2 and v5.3 (operational effectiveness), and the Content Security Layer (aggregate outcome). Best Practice Questions collectively determine the overall layer results, providing a structured view of implementation and coordinated control performance. The hierarchy distinguishes between operational coordination and aggregate control performance.



METHODOLOGY

F CONTENT SECURITY LAYERS

For public reporting, MPA Content Security Best Practices were mapped to the following Content Security Layers to provide aggregated and comparable maturity insights while avoiding disclosure of control-level vulnerabilities.

Content Security Layers	Definitions	Best Practices (v5.3.1)
Strategic Layer	**Strategic Layer** represents long term planning and architectural direction that guides the organization's overall security approach and future posture.	OR-5.0, TS-6.0, TS-6.1, TS-6.2, TS-7.0, TS-7.1
Governance Foundations	**Governance Foundations** consist of the overarching policies, oversight structures, and organizational guidelines that shape how security expectations and responsibilities are defined and managed.	OR 1.0, OR 1.1, OR 1.4, OR 3.4 TS 5.0
Essential Readiness	**Essential Readiness** represents the foundational organizational capabilities required to maintain continuity, stability, and effective response during disruptions.	OR-1.2, OR-1.3, OR-2.0, OR-3.3, OR-4.0
Human Element	**Human Element** encompasses the responsibilities, behaviors, and interactions of individuals that influence how an organization operates and maintains its standards.	OR-3.0, OR-3.1, OR-3.2, OP-2.0, PS-1.1
Physical Security	**Physical Security** involves protecting organizational spaces, equipment, and materials through measures that safeguard the built environment and its access points.	OP-1.0, OP-1.1, OP-1.2, OP-1.3, OP-2.1, PS-1.0, PS-1.2, PS-1.3, PS-1.4, PS-1.5, PS-2.0, PS-3.0, PS-3.1, PS-3.2
Network Security	**Network Security** focuses on maintaining the integrity and controlled operation of the organization's interconnected systems and communication pathways.	TS-2.0, TS-2.2, TS-2.3, TS-2.4, TS-2.5, TS-2.6, TS-2.7, TS-2.8, TS-2.9, TS-2.10, TS-2.11, TS-2.13
Cloud Security	**Cloud Security** refers to the protections and governance applied to organizational information and operations hosted within externally provided or cloud-based platforms.	PS-3.3, TS-1.12, TS-2.12
Access Management	**Access Management** ensures that individuals, systems, and services are permitted to interact with organizational resources only in alignment with defined roles and responsibilities.	TS-1.2, TS-1.6, TS-1.7, TS-1.8, TS-1.9, TS-1.10, TS-1.11
Endpoint Hardening	**Endpoint Hardening** strengthens the configuration and operation of devices used within the organization to ensure they function securely and consistently.	TS-1.1, TS-1.3, TS-1.4, TS-1.5
Application Security	**Application Security** ensures that applications are designed, built, and maintained in a manner that upholds organizational expectations for secure and reliable operation.	TS-1.13, TS-1.14, TS-1.15, TS-1.17, TS-1.18, TS-8.0, TS-8.1, TS-8.2, TS-8.3
Vulnerability Management	**Vulnerability Management** involves the structured identification, evaluation, and resolution of weaknesses across organizational systems and processes.	TS-4.0, TS-4.1, TS-4.2
Cryptography	**Cryptography** encompasses the methods and practices used to protect information through controlled transformation and management of encoded data.	TS-3.0, TS-3.1, TS-3.2
Asset Handling	**Asset Handling** includes the structured processes for receiving, storing, managing, transferring, and disposing of organizational content and materials throughout their lifecycle.	OP-3.0, OP-3.1, OP-3.2, TS-1.0, TS-1.16, TS-2.1

Referenced for contextual alignment only - several technical weakness areas observed across the STAR dataset (e.g.: Access Management, Cryptography, Endpoint Hardening and Vulnerability Management) are consistent with cross-industry application security risk categories identified in the 2025 OWASP Top 10.

METHODOLOGY

G
MEASUREMENT DEFINITIONS

For the STAR report, non-compliance refers to any Best Practice an Assessor has determined as **Partially Implemented or Not Implemented** during a TPN assessment. This was measured through Assessor Findings at the **Best Practice Question** level.

For analytical consistency, Best Practice Questions de-scoped during the Baseline Questionnaire process or were determined as Not Applicable (NA) through the Assessor Findings were **excluded** from non-compliance calculations, as these items were not required to be implemented.

- **Fully Implemented** - Status of assessment Best Practice or Additional Recommendation if ALL components of a Best Practice or Additional Recommendations are met.
- **Partially Implemented** - Status of assessment Best Practice or Additional Recommendation if SOME, but not all, components of a Best Practice or Additional Recommendation are met.
- **Not Implemented** - Status of assessment Best Practice or Additional Recommendation if NONE of the components of a Best Practice or Additional Recommendation are met.
- **Not Applicable** - Status of assessment Best Practice or Additional Recommendation if the Best Practice or Additional Recommendation does not need to be met for this Service Provider.

H
PERCEPTION GAP

The Self-Attestation Perception Gap measures the difference between organizations' questionnaire responses and assessor-validated findings. A perception gap occurs when a control reported in the questionnaire by the Service Provider is identified by the Assessor as a different implementation during the assessment.

METHODOLOGY

I REMEDIATION STATUS

Assessed organizations provide a remediation plan that includes the following options which were used to analyze remediation data.

- **Remediated**: The non-compliant item was implemented in accordance with the Best Practice.
- **Will Remediate Later ("Deferred")**: The non-compliant item was acknowledged, and the Service Provider agreed to remediate it, but at a future date.
- **Will not Remediate ("Refused")**: The Service Provider does not plan to address the non-compliant item.
    - **No Remediation Plan**: The Service Provider did not enter a remediation plan for the non-compliant item. For data analytics purposes, all "No Plan" items are included within the "Refused" category.

METHODOLOGY

J ORGANIZATIONAL DIMENSIONS

Regions

Region was captured using self-reported site and/or primary company addresses for applications. Each country was consolidated into four geographical regions for aggregated and anonymized reporting.

- APAC – East Asia, Southeast Asia, South Asia, and Oceania
- EMEA – UK, Russia, Europe, Middle East, and Africa
- LATAM – Mexico, Central America, South America, and Caribbean
- US/CAN – United States and Canada

Assessment participation varied by region. LATAM reflects lower assessment volume and a narrower distribution across AGR and employee ranges; findings should therefore be interpreted directionally rather than as fully representative of the broader market.

Annual Gross Revenue (AGR) Tiers

TPN membership level AGR ranges were consolidated into three tiers for aggregated and anonymized reporting:

- Levels 1-3: Up to $5M AGR
- Levels 4-7: $5-35M AGR
- Levels 8-10: $35-200M+ AGR

Service Provider Membership level	Annual Gross Revenue (AGR)	Annual TPN Membership
1	Self-Employed	$250
2	Up to $2M	$1k
3	$2-5M	$3k
4	$5-10M	$5k
5	$10-15M	$7.5k
6	$15-25M	$10k
7	$25-35M	$15k
8	$35-50M	$30k
9	$50-200M	$50k
10	$200M+	$85k

Organizational Size (Employees)

Employee range was captured using self-reported number of employees at a company level which included full or part-time, consultant, contractor, intern, freelancer, or temporary workers. All tiers were consolidated into three groups for aggregated and anonymized reporting.

1 person only with no other employees 2 to 20 employees	**1 - 20**
21 to 50 employees 51 to 100 employees	**21 - 100**
101 to 200 employees 201 to 300 employees More than 300 employees	**101 or More**

METHODOLOGY

K
NON-COMPLIANCE CALCULATION

Definitions & Abbreviations:

Q	Best Practice Question
FI	Fully Implemented
PI	Partially Implemented
NI	Not Implemented
NC	Non-Compliance
PG	Perception Gap
SP	Service Provider Answer
AF	Assessor Finding

Best Practice Question Level

Non-Compliance % was calculated as the number of Best Practice Questions with Assessor Findings marked as Partially Implemented or Not Implemented divided by the count of all Applicable Best Practice Questions during the reporting period.

$$NC\ \% = \frac{(Q_{PI \neq NI})}{(Q_{FI+PI+NI})} \times 100$$

Perception Gap

Perception Gap % was calculated as the number of Best Practice Questions with Service Provider answers different from Assessor Findings divided by the count of all Best Practice Questions during the reporting period.

$$PG\ \% = \frac{(Q_{SP \neq AF})}{(Q_{Total})} \times 100$$

METHODOLOGY

L
DATA QUALITY AND VALIDATION

Data quality checks were applied to ensure the dataset was accurate and consistent before analysis

- All results were reviewed for outliers and anomalous data points
- Two independent analytical models were developed and crosschecked to validate findings and conclusions

M
CONFIDENTIALITY PROTECTIONS

To protect confidentiality, all analysis was performed using aggregated, anonymized data, ensuring no individual organization could be identified.

For public reporting, analytics are presented at one or more aggregated layers to safeguard confidentiality and prevent disclosure of control level vulnerabilities.

N
LIMITATIONS

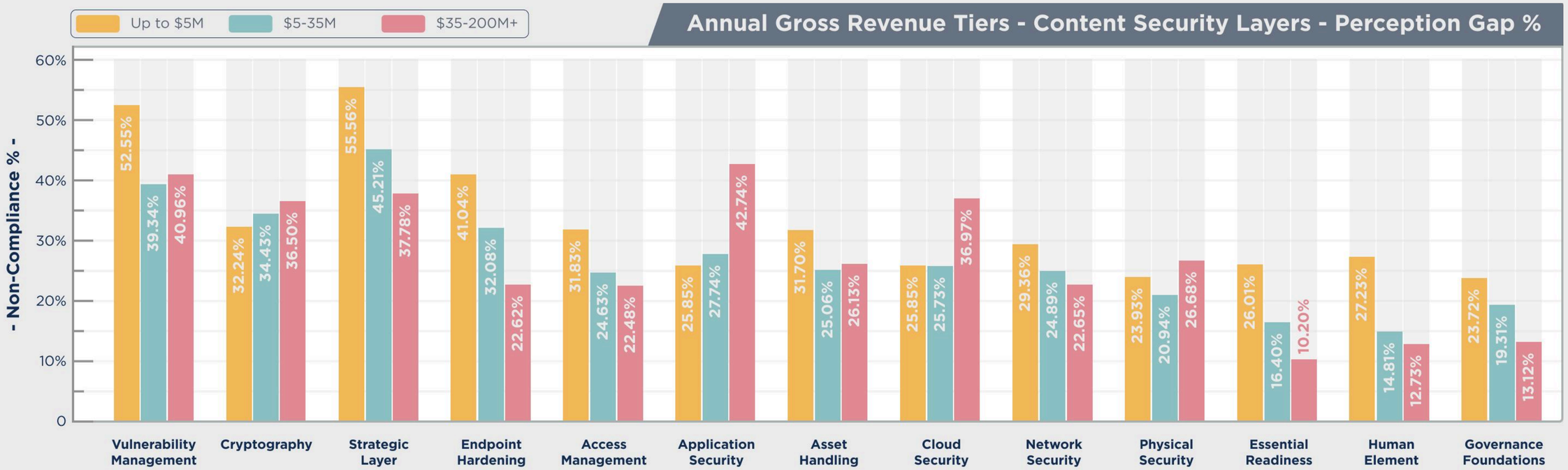
This analysis reflects a point-in-time view based on self-reported and independently assessed data. Results may be influenced by:

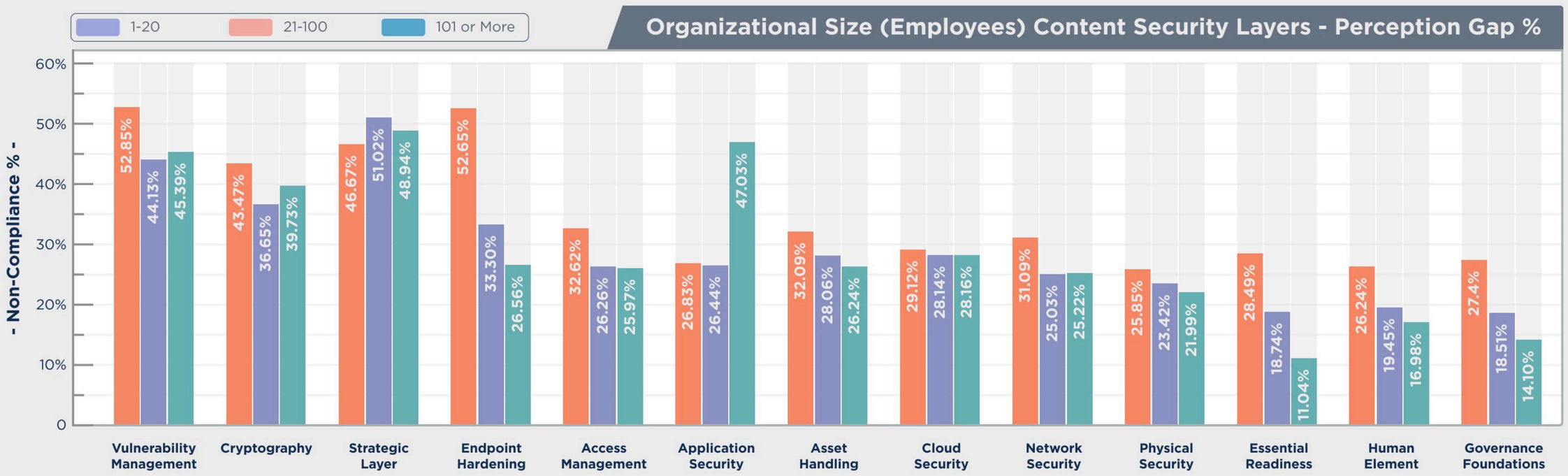
- Variability in assessment timing
- Differences in organizational maturity and resource availability
- Evolving threat landscapes and control interpretations

Accordingly, findings should be interpreted as directional indicators, not absolute measures of security effectiveness.

PERCEPTION GAP

- Misalignment between self-attested responses and assessor findings is consistent across regions, revenue tiers and organizational sizes

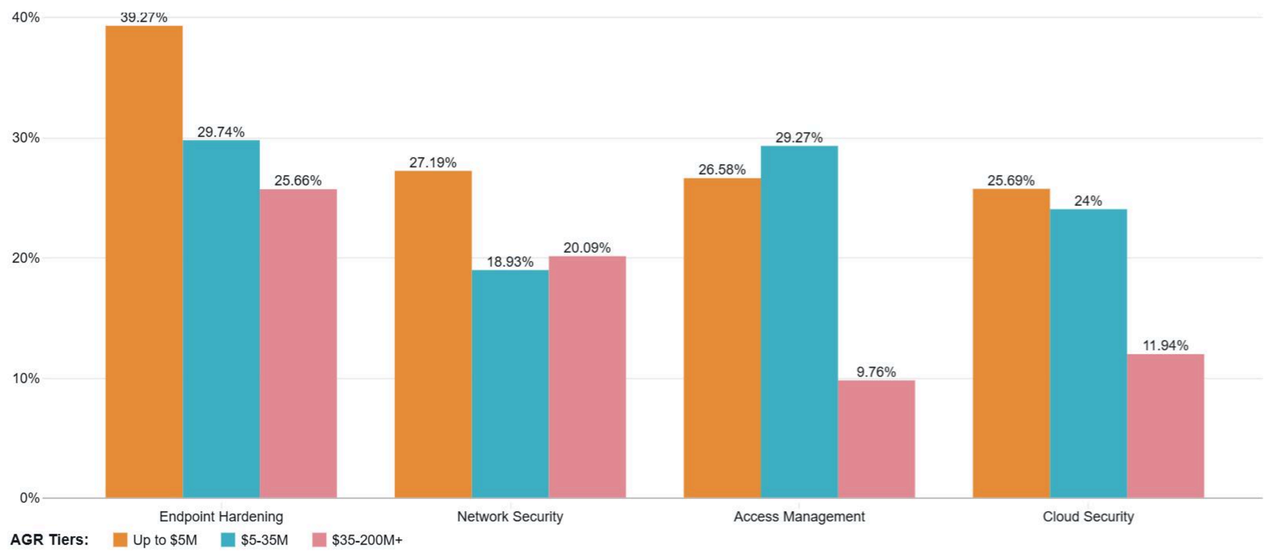




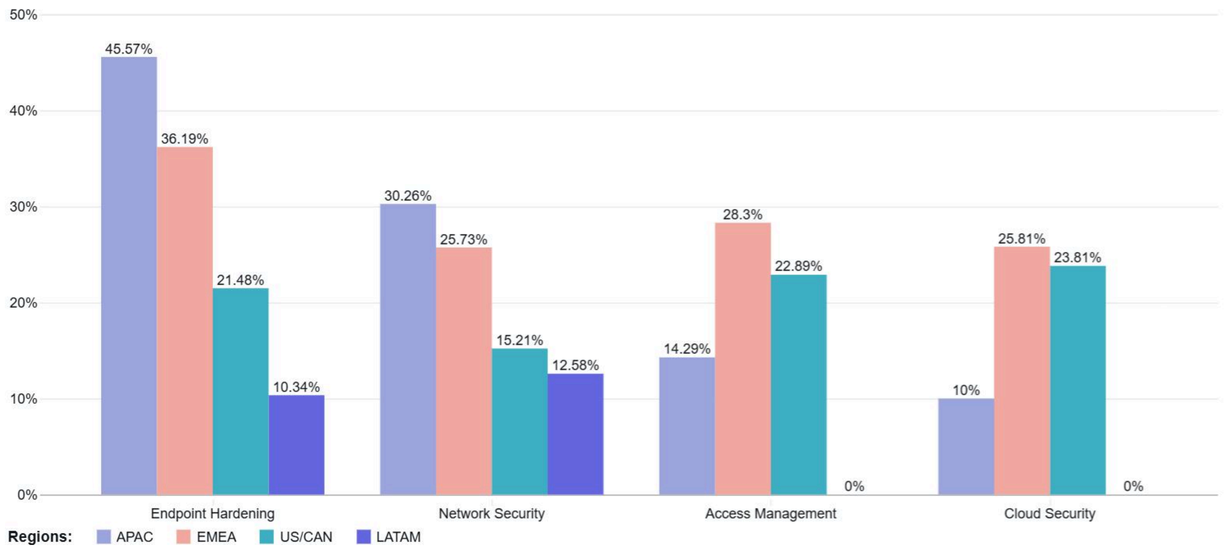
CLOUD ACCESS & NETWORK SECURITY

Endpoint Hardening has the highest non-compliance overall; in general, improvements scale with revenue

Annual Gross Revenue Tiers (AGR)
Cloud Access & Network Security - Non-Compliance %



Regional
Cloud Access & Network Security - Non-Compliance %



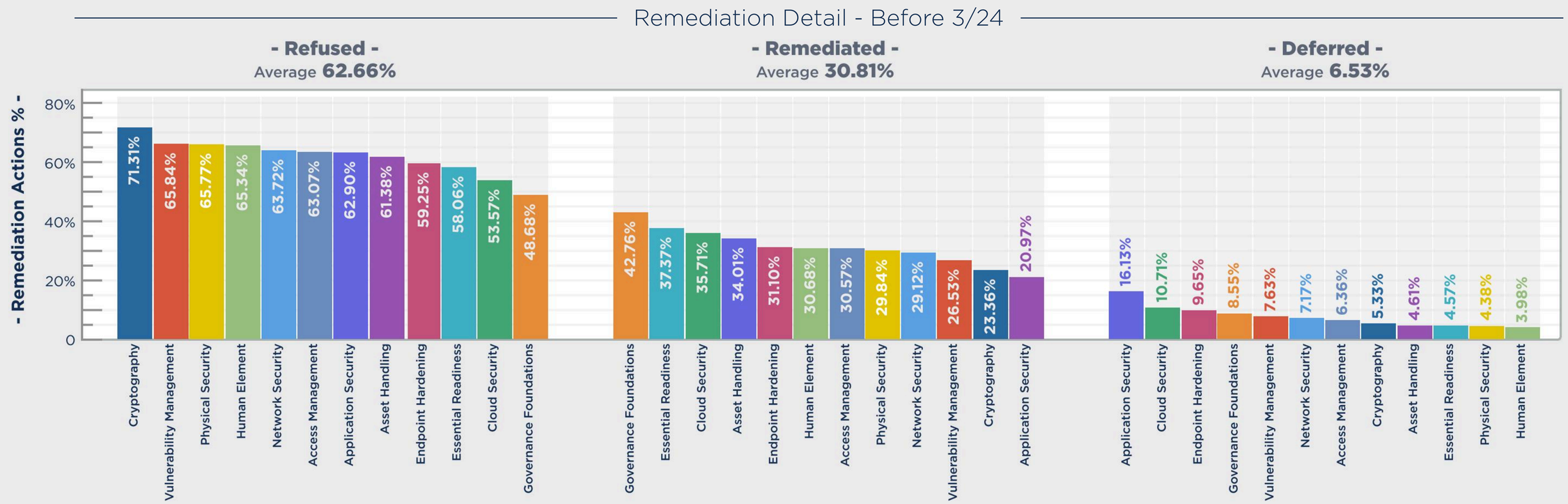
APAC risk is concentrated in Endpoint Hardening and Network Security, whereas EMEA and US/CAN show higher non-compliance in Access Management and Cloud Security, indicating region-specific execution gaps across identity and cloud controls

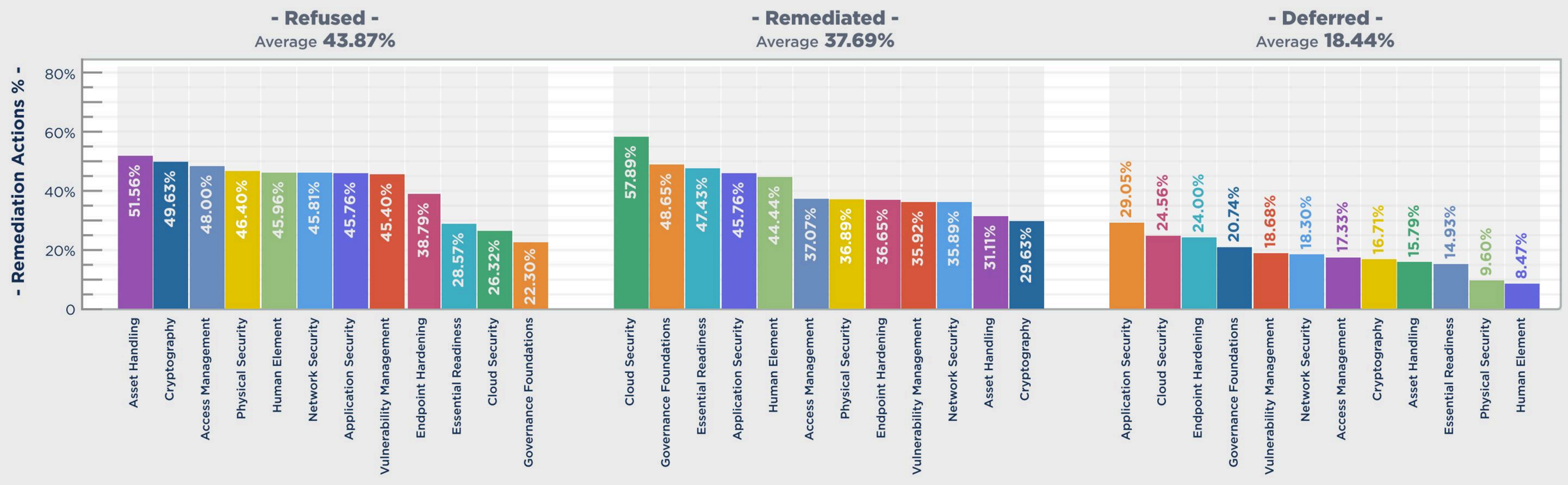
Data Context: LATAM excluded in Access Management and Cloud Security due to insufficient sample size

DATA ANALYSIS

Remediation behaviors also improved after the Shield issuance policy introduction:

- Remediation improved (30.81% → 37.69%)
- Refusal rates declined materially (62.66% → 43.87%), indicating greater engagement with remediation
- Deferred remediation increased (6.53% → 18.44%), reflecting a shift toward remediation planning

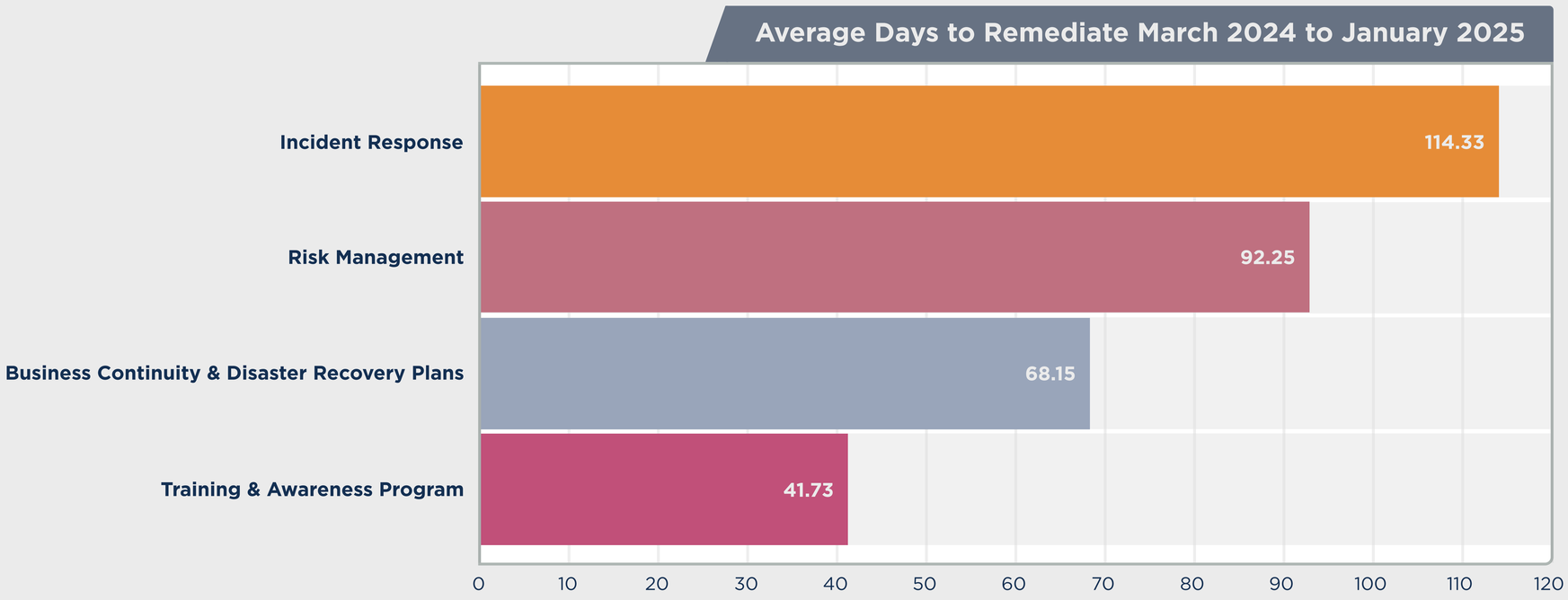




DATA ANALYSIS

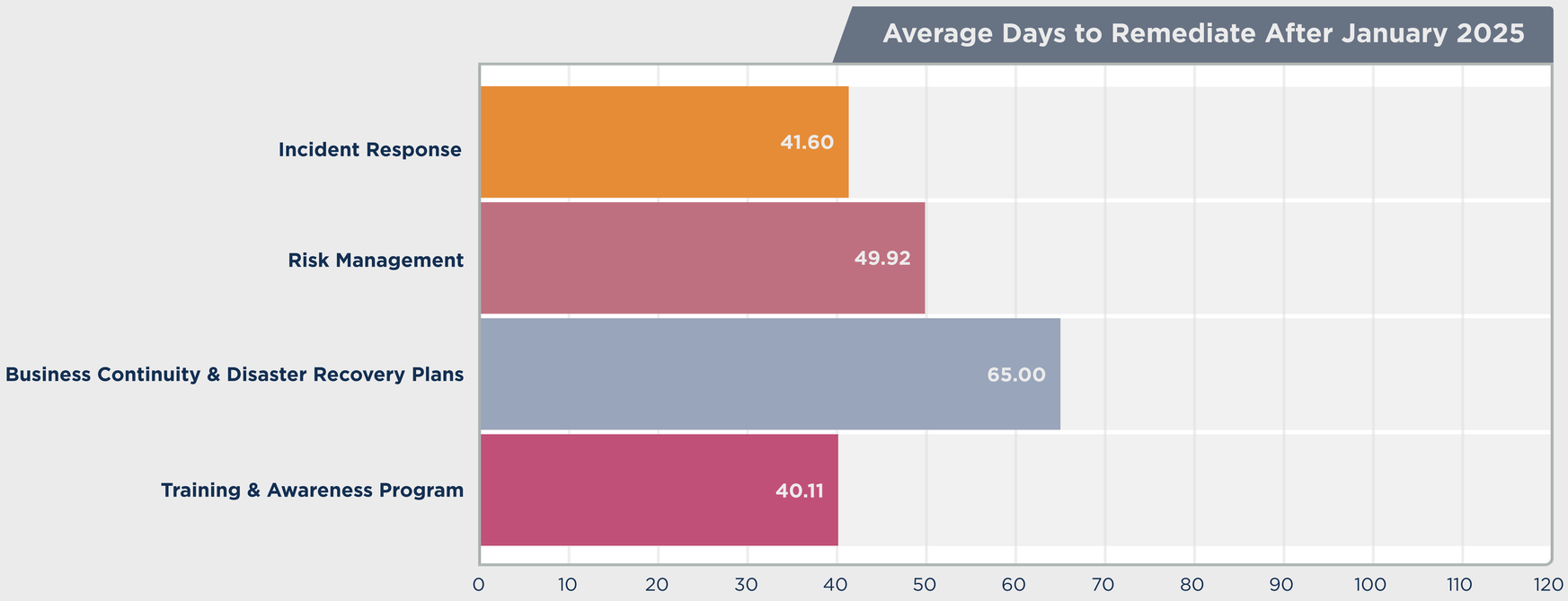
EARLY IMPACT OF FREE SECURITY RESOURCES - REMEDIATION TIMELINES

Accessible, policy-driven resources deliver measurable improvements in both compliance and remediation speed - remediation timelines improved by ~36%, accelerating issue resolution



Average Days to Remediate March 2024 to January 2025

74.17



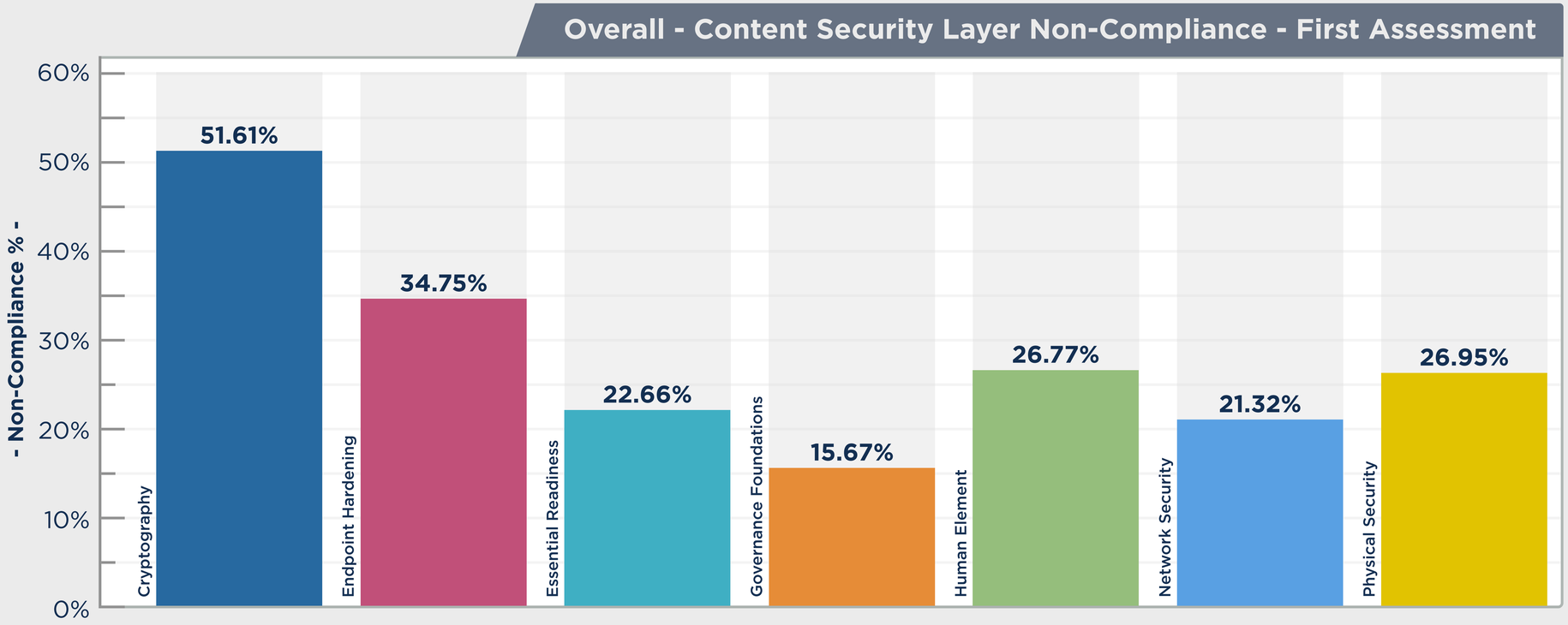
Average Days to Remediate After January 2025

48.46

DATA ANALYSIS

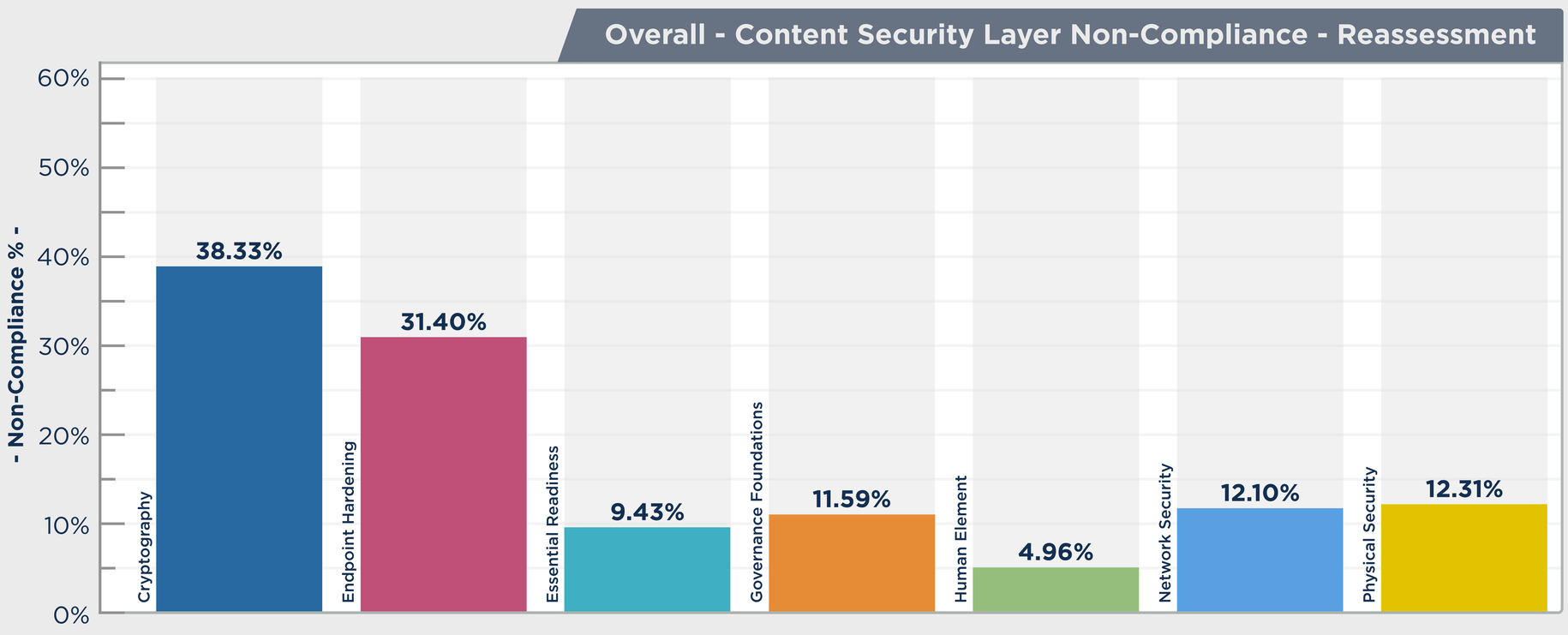
CONTENT SECURITY LAYER REASSESSMENT - NON-COMPLIANCE %

In a reassessment, the greatest technical control improvements are seen in Cryptography, Endpoint Hardening, and Network Security



First Assessment
Overall Non-Compliance

25.46%

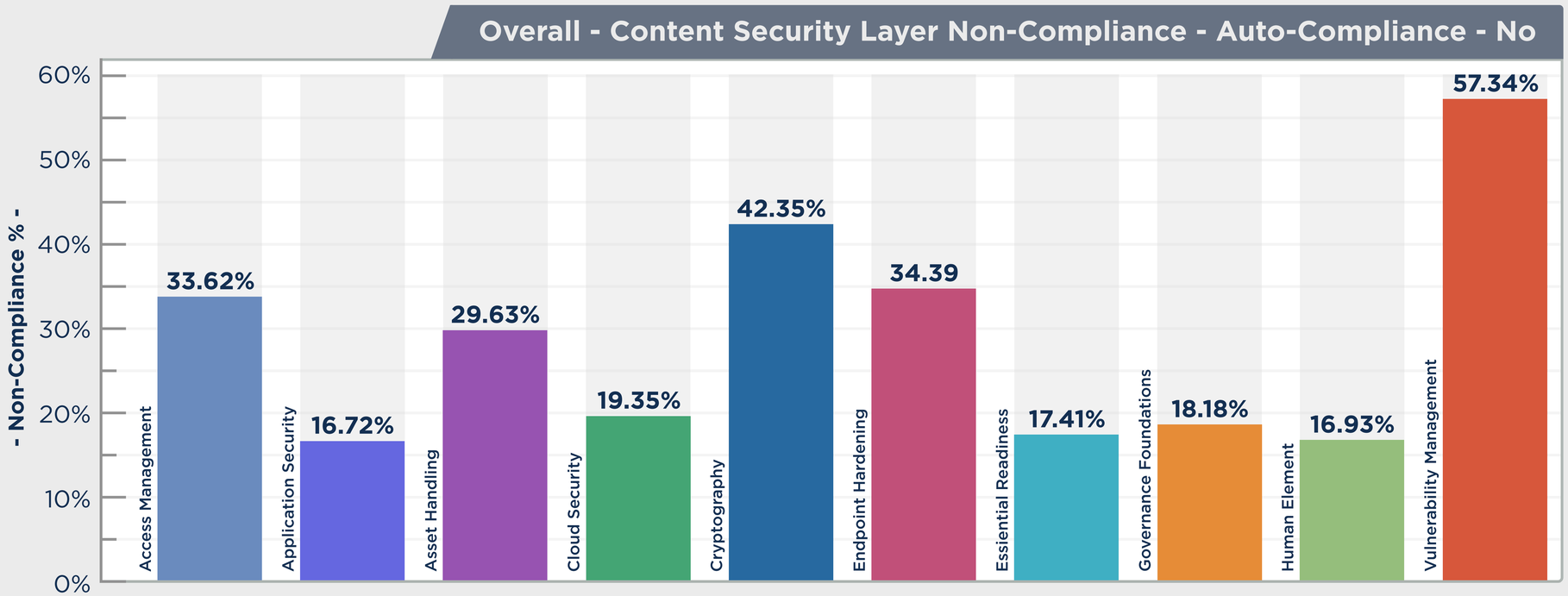


Reassessment
Overall Non-Compliance

17.99%

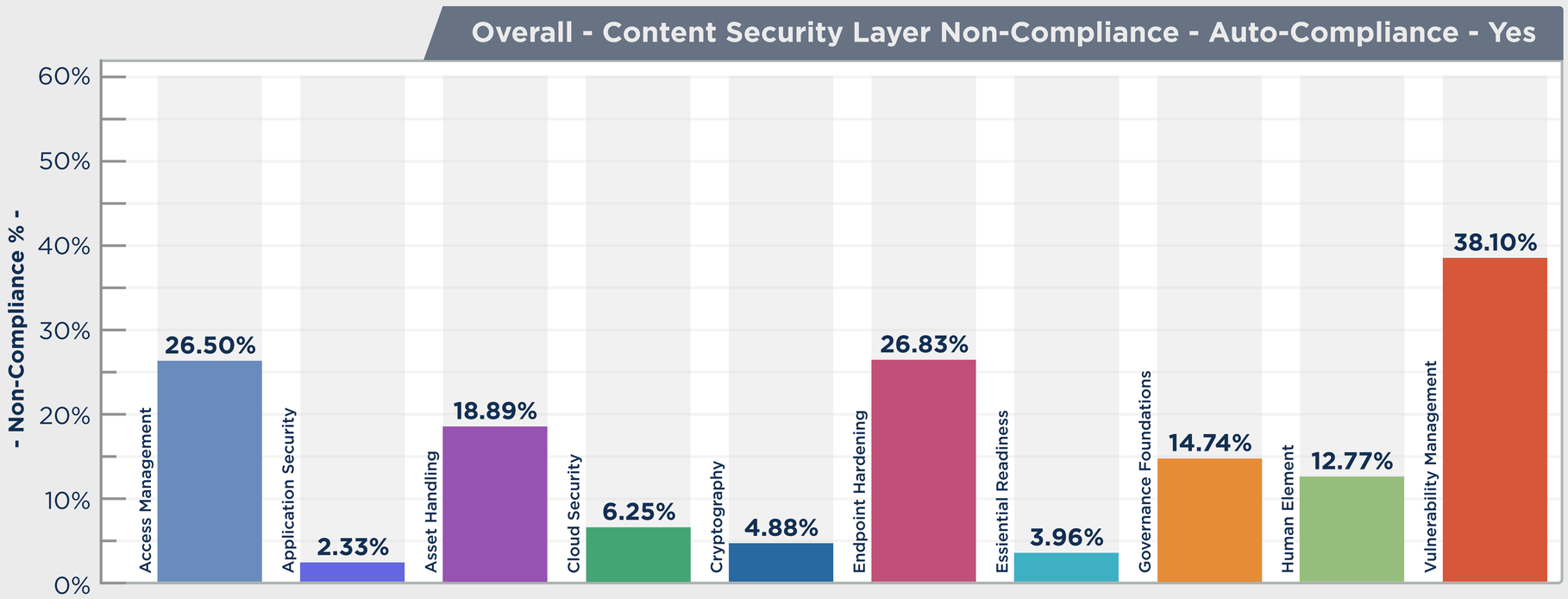
AUTO-COMPLIANCE ADOPTION NON-COMPLIANCE TRENDS

- Organizations using automated compliance report materially lower non-compliance, with the strongest improvements observed across Access Management, Application & Cloud Security, Cryptography, Endpoint Hardening, and Vulnerability Management



Does Not Use Auto Compliance
Overall Non-Compliance

24.06%



Uses Auto Compliance
Overall Non-Compliance

17.38%

The TPN STAR Report provides an objective, data-driven view of how security controls are being implemented, and where execution challenges persist across the global content supply chain.

Staying engaged with this data and the TPN program helps organizations track progress, prioritize remediation, and strengthen long-term security resilience.

TPN will continue to build on the STAR dataset through expanded analysis, deeper remediation tracking, and ongoing collaboration with industry partners through the TPN community network - supporting more informed decisions and measurable improvement over time.

Learn more and stay connected:

Follow Trusted Partner Network on LinkedIn
https://www.linkedin.com/company/trusted-partner-network/

STAR Report and TPN Resources
www.ttpn.org

Questions or Feedback
support@.ttpn.org