Progress® Flowmon

The Pulse of Cybersecurity in APAC: Resilience in the Age of AI

Insights Into How Organizations Overcome Barriers and Build Future-Ready Defenses

WHITEPAPER

Executive Summary

This whitepaper presents the findings from a comprehensive survey commissioned by Progress Software and conducted by Foundry. The survey explored cybersecurity priorities, challenges and investment strategies across key emerging markets in APAC. Some of the findings include the increasing adoption of AI/ML in security operations, the prominence of cloud security and the evolving role of compliance.

Introduction

Cybersecurity remains a critical concern for organizations in APAC, driven by the rapid digital transformation and increasing cyberthreats. This research report aims to provide insights into the current cybersecurity landscape, helping organizations align their strategies with emerging trends and challenges.

Key conclusions

- Organizations are investing heavily in hybrid/multi-cloud protection and visibility, as cloud-first security strategies are now the norm.
- AI and machine learning (ML) are mainstream: 4 in 5 organizations are increasing AI/ML investments, primarily for threat detection and security automation. However, trust, explainability and skills remain major barriers—underscoring the need for intuitive, transparent and human-centric solutions.
- Network Detection and Response (NDR) is a rising priority but under-deployed. There's a clear gap between intent and current use.
- Security teams are stretched. Talent shortages, insider threats and complex infrastructures are driving demand for tools that reduce manual effort and accelerate response times.
- Compliance drivers are evolving from check-the-box to strategic priorities such as trust, resilience and risk reduction.

Findings

Cybersecurity Priorities: AI, Cloud and Threat Detection

Organizations across APAC are prioritizing cloud security and hybrid/multi-cloud security management, with over half of the respondents ranking it as their top concern. This focus reflects the increasing reliance on cloud infrastructure and the need to secure these environments. AI/ML adoption in security operations is also a significant priority, indicating

a shift towards leveraging advanced technologies for threat detection and response. Network Detection and Response (NDR) and threat intelligence are critical areas, highlighting the importance of proactive threat management.

- Cloud Security and Hybrid/Multi-Cloud Security Management: 53% of respondents ranked this as their top priority.
- AI/ML Adoption in Security Operations: 40% of respondents are focusing on this area.
- Network Detection and Response (NDR) / Threat Intelligence and Detection: 39% of respondents highlighted this as a key priority.

What are your organization's top priorities in cybersecurity for the next 12-18 months?

What are your organization's top priorities in cybersecurity for the next 12-18 months?	India	Malaysia	Indonesia	Philippines
Cloud Security and Hybrid/Multi-Cloud	58%	45%	58%	52%
Enhancing Security Analytics and Risk Prediction	50%	39%	30%	40%
NDR/Threat Intelligence and Detection	27%	47%	36%	42%
Security Awareness/Human Risk Mitigation	33%	33%	53%	38%
Zero Trust Architecture	31%	22%	30%	35%
Ransomware Protection and Recovery	17%	24%	34%	8%
Regulatory Compliance and Data Governance	17%	24%	15%	29%
Healthcare/Pharma	21%	31%	13%	10%
Security Orchestration, Automation and Response (SOAR)	27%	18%	19%	25%
Endpoint Detection and Response (EDR)	27%	18%	11%	21%

Comparative Table Showing the Top Three Cybersecurity Priorities by Country (India, Malaysia, Indonesia, Philippines).

Insights by Country

India

- Cloud security is top-ranked at 58%.
- AI/ML is second (50%), suggesting higher readiness or openness to intelligent automation.
- SOAR (27%) and EDR (19%) are higher than the regional average, signaling growing interest in automation and endpoint resilience.
- Emphasis on modernization and operational response maturity.

Malaysia

- Shows the highest prioritization for enhancing analytics & risk prediction (47%).
- Balanced priorities across cloud, compliance and AI/ML.
- Regulatory compliance (31%) is more prominent here—possibly due to strong local data laws like PDPA.
- Market shows greater concern around structured governance and visibility.

Indonesia

- Cloud security (58%) is a standout top concern.
- NDR is very high at 53%, emphasizing the demand for network-based visibility and real-time threat detection.
- AI/ML is less of a focus (30%) compared to the others.
- Suggests a need-based adoption curve, where infrastructure modernization precedes AI layers.

Philippines

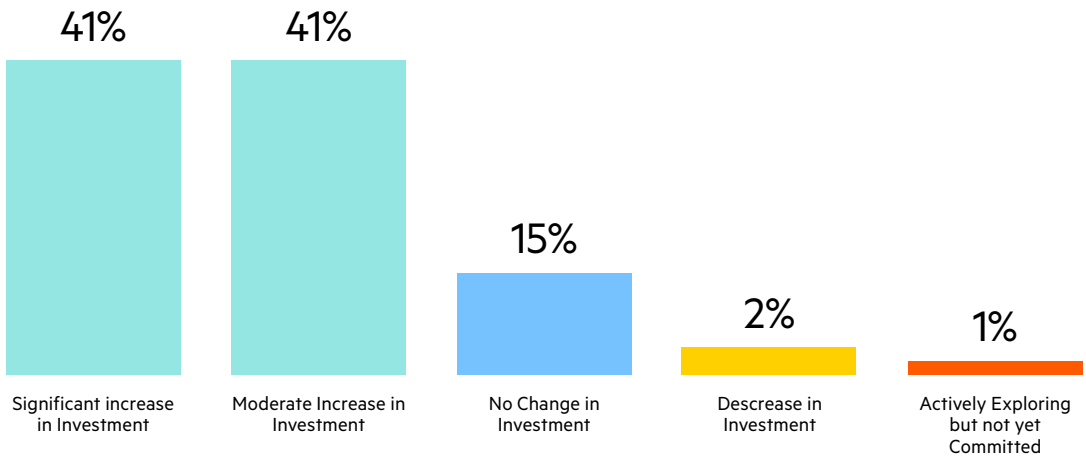
- Prioritizes enhancing analytics (42%) and cloud (52%), which closely align with regional trends.
- Security awareness training (35%) ranks higher than in other countries—indicating more focus on insider threats and human error.
- EDR (21%) and ransomware (29%) are slightly elevated, suggesting high concern over endpoint threats and attack recovery.

AI/ML Adoptions

Investment in AI/ML-based security solutions is set to rise significantly, with 41% of respondents planning substantial increases in their budgets. This trend underscores the growing recognition of AI/ML's potential to enhance security operations through automation and improved threat detection. Another 41% of respondents are planning moderate increases, indicating widespread commitment to integrating AI/ML technologies into their cybersecurity strategies.

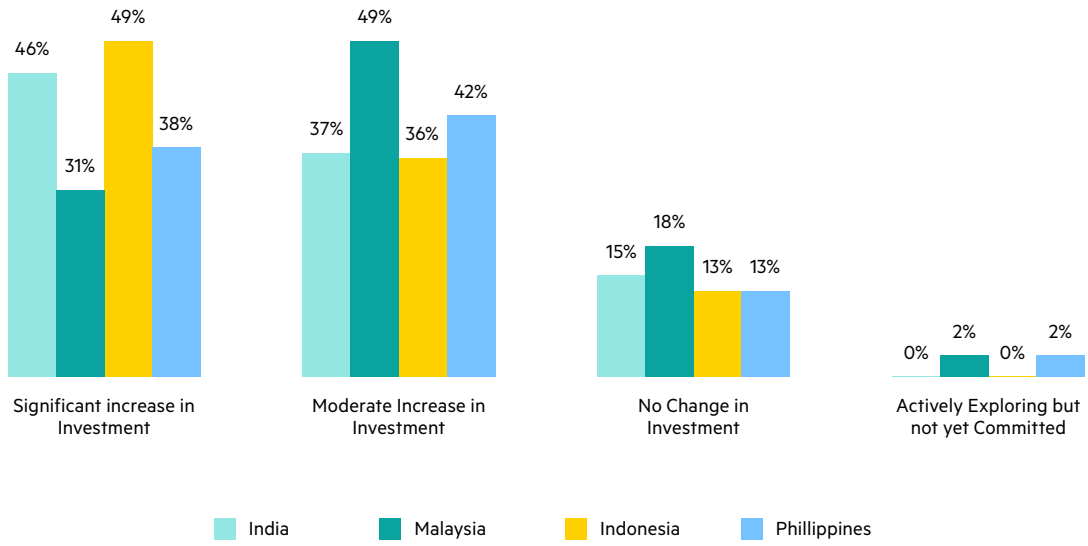
- More than 81% of respondents plan a significant increase in AI/ML investments.

How is your organization planning to invest in AI/ML-based security solutions in the next 12-18 months?



Market-level Summary of AI/ML Investment Plans

How is your organization planning to invest in AI/ML-based security solutions in the next 12-18 months? By Country



Insights by Country

- **Indonesia** shows the strongest intent, with 49% planning a significant investment boost.
- **India** follows closely at 46%, affirming the region's AI security leadership.
- **Malaysia** leans toward moderate investment (49%)—suggesting a gradual adoption mindset.
- **The Philippines** is more cautious, with slightly higher moderate (42%) and the highest decrease + not committed (6%).

AI Adoption Challenges

Despite the enthusiasm for AI/ML, organizations face significant challenges in adoption. Data privacy and ethical concerns are the most prominent, affecting 59% of respondents. These concerns highlight the need for transparent and trustworthy AI solutions. Integration with existing tools and infrastructure is another major hurdle, with nearly half of the respondents struggling to incorporate AI/ML into their current systems.

- Data Privacy and Ethical Concerns: 59% of respondents identified this as a major challenge.
- Integration with Existing Tools and Infrastructure: 48% of respondents face this challenge.

What are the main challenges your organization faces in adopting AI/ML for cybersecurity?

What are the main challenges your organization faces in adopting AI/ML for cybersecurity?	Overall	India	Malaysia	Indonesia	Philippines
Data Privacy and Ethical Concerns	59%	29%	32%	25%	50%
Integration with Existing Tools and Infrastructure	48%	41%	25%	34%	48%
AI Reliability, Explainability and Trust	48%	53%	49%	42%	54%
Regulatory, Compliance and Legal Constraints	37%	43%	48%	54%	46%
Budget constraints & cost justification	34%	41%	42%	38%	35%
Lack of skilled professionals / training gaps	34%	56%	55%	69%	27%
Unclear ROI / measuring effectiveness	21%	18%	21%	23%	17%
AI/ML security not currently a priority	19%	18%	26%	15%	21%

Market-Level Insights

India

- Top Concern: Skills gap (56%).
- AI trust and explainability (53%) and integration challenges (41%) also rank high.
- Privacy is notably lower (29%), suggesting India is more focused on implementation than ethics.

Malaysia

- Shows broad concern across many categories including:
    - Skills gap (55%)
    - AI trust (49%)
    - Privacy (32%) is mid-tier, but AI not being a priority is relatively high (26%), possibly signaling slower adoption curve.

Indonesia

- #1 Challenge: Skills gap (69%) – highest of all countries.
- Also concerned about regulation (54%) and trust (42%).
- Suggests a strong need for education, training and plug-and-play AI tools.

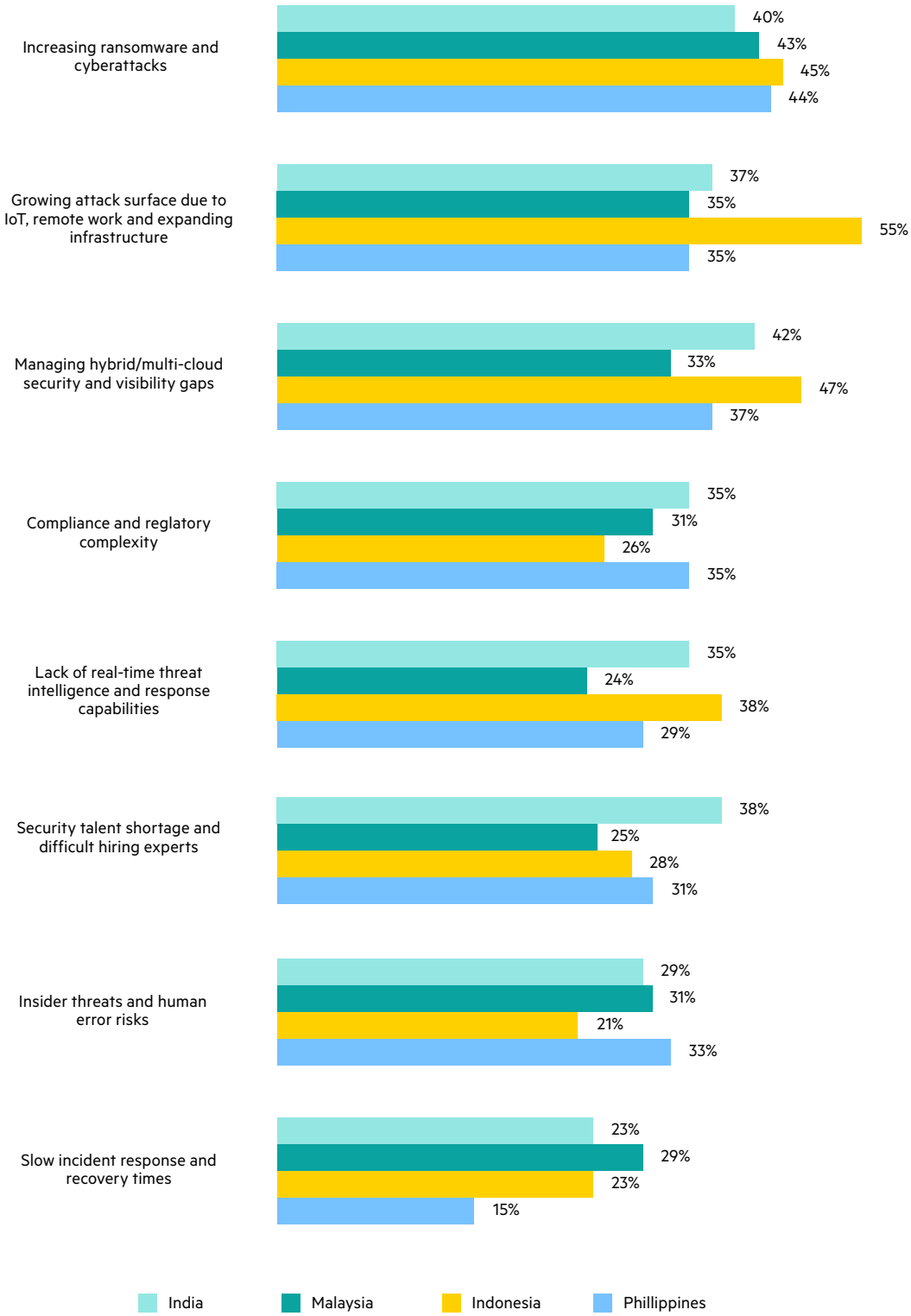
Philippines

- Top issue is AI trust (54%), indicating a cautious outlook.
- Lower concern around skills gap (27%), possibly due to smaller teams or higher reliance on managed services.
- Privacy is a top priority (50%), suggesting sensitivity to data governance.

Cybersecurity Challenges

Ransomware and cyberattacks remain top concerns for organizations, with 43% of respondents highlighting these threats. The growing attack surface, exacerbated by IoT and remote work, is another critical issue, affecting 40% of respondents. These challenges underscore the need for robust security measures and proactive threat management strategies.

Most Concerning Cybersecurity Challenges by Country

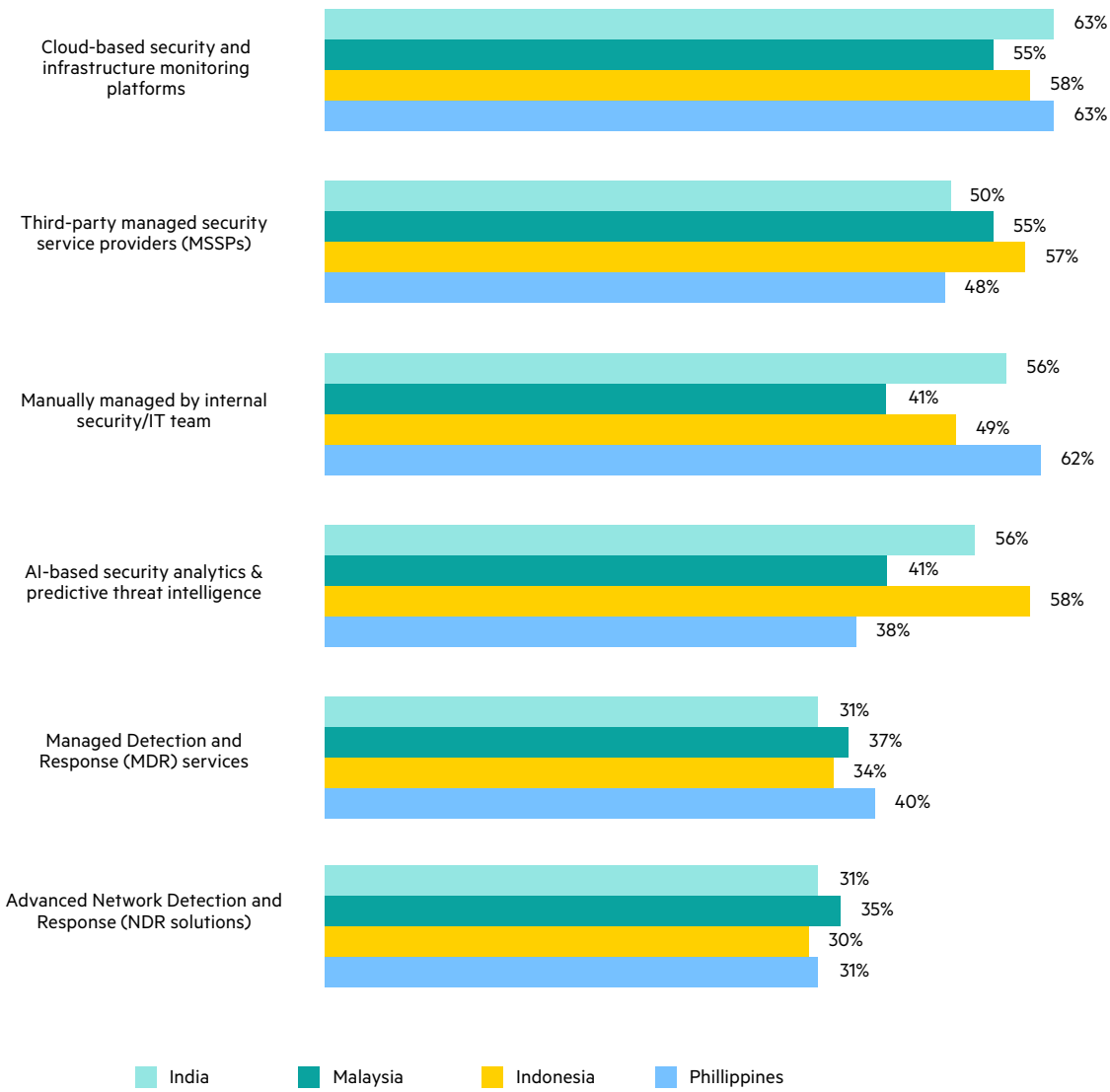


Monitoring Approaches

Organizations are increasingly adopting cloud-based security and infrastructure monitoring, with 60% of respondents using these solutions. Third-party managed security service providers (MSSPs) are also popular and are relied upon by 52% of respondents. These approaches reflect the need for scalable and efficient monitoring solutions to manage complex and distributed IT environments.

- Cloud-Based Security and Infrastructure Monitoring: 60% of respondents use this approach.
- Third-Party Managed Security Service Providers (MSSPs): 52% of respondents rely on MSSPs.

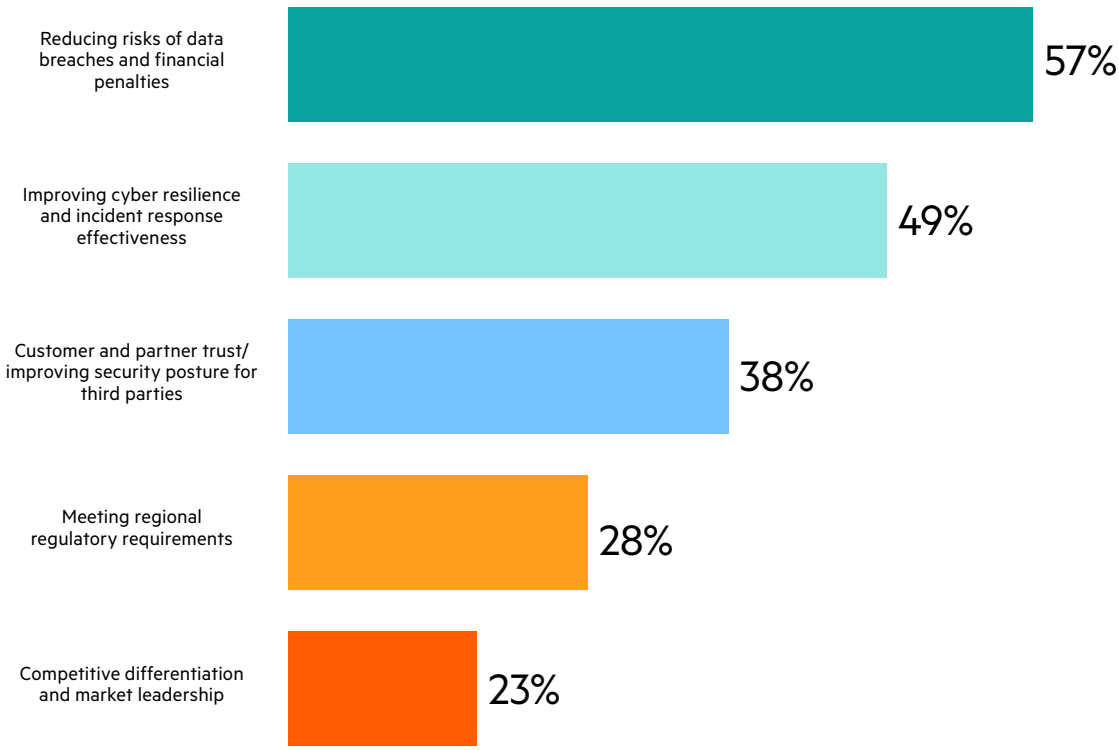
Adoption of Different Monitoring Approaches by Country



Regulation and Compliance Drivers

Compliance isn't just about ticking boxes—it's about protecting your business from financial loss, restoring trust quickly and detecting risks before they escalate. One of the most critical reasons driving the focus on security compliance and regulatory frameworks is reducing risks of data breaches and financial penalties. This aspect alone accounts for 57% of the motivation behind implementing robust security measures.

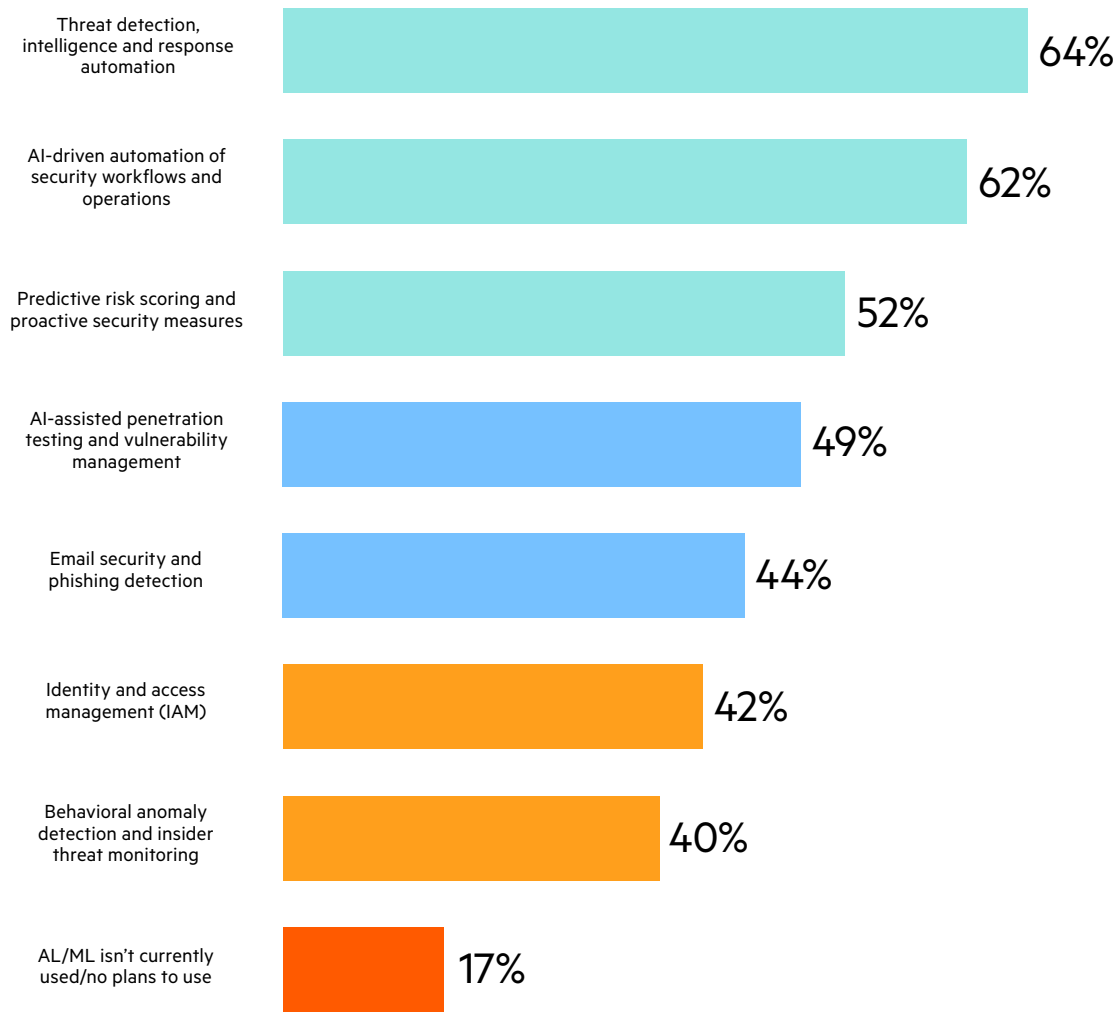
Key Reasons Driving your Focus on Security Compliance and Regulatory Frameworks



AI Enhanced Cybersecurity: Key Adoption Areas

Organizations increasingly adopt AI to enhance their defense mechanisms and expedite response times. A significant portion of this adoption is concentrated in three key areas. Firstly, 64% of organizations are utilizing AI for threat detection, intelligence and response, underscoring the critical role of AI in identifying and mitigating threats. Secondly, 62% of organizations are leveraging AI to automate security operations, thereby streamlining processes and improving efficiency. Thirdly, 49% of organizations are employing AI-assisted methods to prevent security vulnerabilities, highlighting a proactive approach to cybersecurity. These trends reflect a growing reliance on AI to bolster security measures and help safeguard against potential risks.

From detection to automation, organizations are turning to AI to effectively and efficiently defend and respond



Conclusion

The survey highlights the critical role of AI/ML in enhancing cybersecurity operations and the need for organizations to address integration and skills challenges. By focusing on cloud security and leveraging AI/ML, organizations can better protect their digital assets and improve their overall security posture.

Methodology

The survey targeted IT decision-makers from companies with employees between 100 and 10,000 across India, Malaysia, Indonesia and the Philippines. A total of 208 respondents participated, providing valuable insights into their cybersecurity priorities and strategies.

Empower Your Security Team

Whether defending against ransomware, insider threats, zero-day exploits, or lateral movement, Flowmon NDR solution help IT teams stay ahead of evolving cyberthreats.

Request Your Trial and Strenghten Your Network Security with Flowmon Threat Detection and Response

Worldwide Headquarters

Progress Software Corporation
15 Wayside Rd, Suite 400, Burlington, MA01803, USA
Tel: +1-800-477-6473

facebook.com/progresssw
twitter.com/progresssw
youtube.com/progresssw
linkedin.com/company/progress-software
progress_sw_

Progress