

The Double-Edge Sword

How AI is Both the Biggest Threat and Best Defense in Data Security

Sumit Nigam

Regional Leader, ASEAN – Cybersecurity Services
Concentrix

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council



THE CYBER CRIME REALITY 2026

GLOBAL UNDER ATTACK

AI is accelerating cybercrime at **machine speed.**
Cyber-enabled fraud, ransomware and identity attacks are reshaping business risk worldwide.
Cyber resilience has become a **board-level priority.**

$10.5 TRILLION

Estimated Global Annual Cybercrime Damage by 2026

Cybercrime has become one of the world's largest economic threats, impacting governments, critical infrastructure and enterprises across every industry.

Up **22%** from ~$8.6 Trillion in 2025

CYBER ATTACKS TARGET EVERY MAJOR ECONOMY

AI is reducing attacker effort and increasing attack scale globally.



Cyber attacks have no borders.
AI-enabled adversaries are operating faster, cheaper and at unprecedented scale.

94%
Security leaders believe AI will be the biggest force shaping cybersecurity.
↑ Up from **86%** in 2025

77%
Organizations report an increase in cyber-enabled fraud & phishing.
↑ Up from **63%** in 2025

87%
Organizations experienced increased AI-related cyber vulnerabilities.
↑ Up from **72%** in 2025

24–48 HOURS
Average time to exploit newly disclosed critical vulnerabilities. Attackers are faster than patch cycles.

1 ATTACK EVERY 39 SECONDS
Cyber attacks are happening faster than ever.

THE PRESSURES FACING ORGANIZATIONS GLOBALLY

68%
Data breaches involve human error, misuse or social engineering.
Source: Verizon DBIR 2026

77%
Organizations experienced increased phishing and cyber-enabled fraud.
Source: WEF GCO 2026

69%
Organizations report cybersecurity talent shortages.
Source: WEF GCO 2026

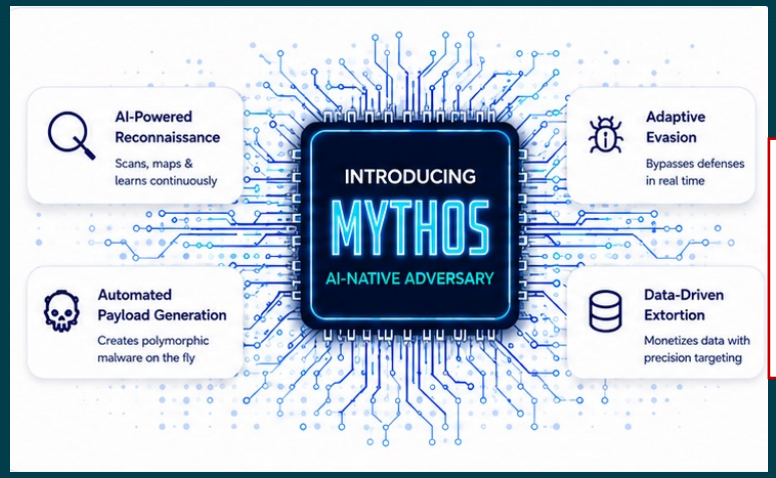
AI + GEOPOLITICS
AI, geopolitical conflict and digital sovereignty are now the primary drivers of cyber risk in 2026.
Source: WEF GCO 2026

REGULATORY PRESSURE
Rising compliance with NIS2, DORA, SEC Cyber Rules, AI Governance and Data Sovereignty.
Source: WEF GCO 2026

73%
People personally affected by cyber-enabled fraud.
Source: WEF GCO 2026

Next Level AI Threat .. ?

AI supercharges every phase of the attack lifecycle — faster, stealthier, and at scale.



MYTHOS IN THE REAL WORLD

67 : 0-Day Vulnerabilities Discovered

92% : Unknown Attack Surface Identified

36 Hrs : Mean Time to Detection Reduced

78% : Reduction in Security Incidents

The New Face of a Mythos AI Attack

Second 0

AI-Powered Reconnaissance

Minute 1

Exploit Weaponized

Minute 3

Stealth Entry Established

Minute 7

Lateral Movement at Machine Speed

Minute 15+

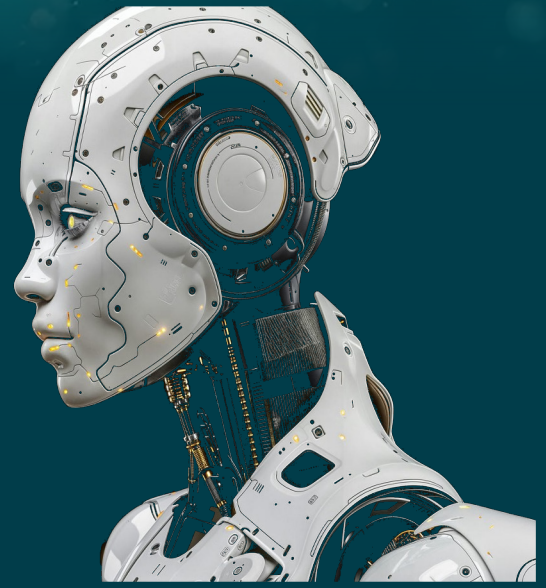
Business Impact Triggered

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

The Cybersecurity Paradigm Has Changed

Reactive cybersecurity cannot defend against autonomous cyber operations

- **89%** Rise in AI-enabled adversary attacks
- **87%** Organizations experienced AI-driven cyberattacks in the last year
- **84%** CEOs fear catastrophic AI-enabled cyber events



- **AUTONOMOUS**
- **AI-POWERED**
- **ELUSIVE**
- **EXPONENTIAL**

Leadership Alarm : From craft to assembly line

AI-driven Attack Evolution
Adversaries leverage AI to evolve tactics, techniques & procedures continuously.

Real-time Exploit Generation
AI generates and weaponizes exploits in real-time at scale.

Self-learning Attack Chains
Attacks adapt and optimize through continuous feedback and learning.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Top Root Causes of Emerging AI Breaches

Where AI meets existing security gaps in the CDE

01 AI & DATA EXPOSURE

- Shadow AI
- Data leakage
- Uncontrolled AI access

02 VULNERABLE CDE

- Unpatched systems
- Legacy technology
- Exploitable weaknesses

03 IDENTITY & ACCESS

- Credential theft
- Excessive privilege
- Weak authentication



4 ADAPTIVE ATTACKS

- AI-driven phishing
- Evolving malware
- Multi-stage attacks

05 HUMAN & PROCESS GAPS

- Social engineering
- Misconfiguration
- Delayed response

06 THIRD-PARTY EXPOSURE

- Payment ecosystem
- Service providers
- AI dependencies

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

AI IS ACCELERATING VULNERABILITY DISCOVERY

More intelligence. More findings. More fixes.

6.8X INCREASE
in total security fixes
(Dec 2025 – Jul 2026)

BEFORE FRONTIER AI

- Manual Research
- Slower Discovery
- Predictable Cycles

FRONTIER AI ERA

- AI-Assisted Discovery
- Autonomous Code Analysis
- Faster Remediation
- Shorter Window for Attackers

SECURITY FIXES BY TOP OEMs
(DEC 2025 – JUL 2026)

	DEC 2025	JAN 2026	FEB 2026	MAR 2026	FRONTIER AI ADOPTION	APR 2026	MAY 2026	JUN 2026	JUL 2026	
Microsoft	136	114	129	147		168	182	206	622	3.0X vs Dec 2025
Google Chrome	45	51	57	63		71	83	97	115	2.6X vs Dec 2025
Palo Alto Networks	16	18	20	23		25	29	34	41	2.6X vs Dec 2025
TOTAL (ALL 3)	197	183	206	233		264	294	337	778	3.9X vs Dec 2025

AI adoption accelerates discovery and fixes

TOTAL TREND



THE IMPACT

- More vulnerabilities identified
- Faster time to exploit
- Higher remediation demand
- Expanding attack surface
- Continuous defense is critical

Source: Microsoft MSRC, Google Chrome Release Notes, Palo Alto Networks Advisories | Period: Dec 2025 – Jul 2026

DEFENDING AT GLOBAL SCALE

AI-Powered Security. Layered Defense. Resilient Enterprise.

AI-POWERED THREATS

AI-Generated Phishing
Deceptive, personalized and harder to detect.

Synthetic Identity Fraud
AI creates fake identities at scale.

Automated Exploitation
AI-powered tools find and exploit weaknesses quickly.

AI-Powered Malware
Adaptive, polymorphic and designed to evade defense.

Data Exfiltration & Model Theft
Sensitive data and models are high-value targets.



CONTINUOUS DEFENSE

Attack Surface Intelligence
Continuously discover, classify and reduce exposure.

AI-Powered Detection
Detect anomalies and threats using AI and behavioral insights.

Identity-Centric Security
Verify every user, device and access path.

Automated Response
Contain and respond at machine speed.

Continuous Validation
Validate controls, configurations and remediation continuously.

AI-POWERED SECURITY FABRIC

IDENTITY
Unified visibility and strong access controls.

DATA SECURITY
Protect data across its entire lifecycle.

VULNERABILITY
Continuously find, prioritize and fix risks.

NETWORK
Secure connectivity everywhere.

DETECTION & RESPONSE
AI-driven detection and rapid response.

AI GOVERNANCE
Responsible use of AI with guardrails.

AUTOMATION
Orchestrate and automate security operations.

INTELLIGENCE-LED DEFENSE

From Noise to Action

NOISE

Too much data.

Too little context.

INTELLIGENCE THAT MATTERS

ACTION

Right intelligence.

Right context.

Right now.

Multi-source threat intelligence aggregation
Internal + External + PCI Ecosystem

Real-time correlation at gateway level
→ Pre-emptive blocking

Curated, actionable alerts
High fidelity. Low noise.

PCI DSS CONTROL FOUNDATION

1. PROTECT CARDHOLDER DATA
- Secure storage, transmission & encryption
- Tokenization & data minimization

2. SECURE SYSTEMS & NETWORKS
- Firewall, segmentation & secure configurations
- Protect CDE & connected environments

3. MANAGE ACCESS
- Least privilege access
- Strong authentication & access control

4. MONITOR & TEST
- Logging, monitoring & audit trails
- Vulnerability management & penetration testing

5. MAINTAIN POLICY
- Security policies & training
- Incident response & risk management

PCI DSS CONTROLS IN ACTION

24/7 SECURITY OPERATIONS

PEOPLE | PROCESS | TECHNOLOGY



THREAT PREVENTION

ANOMALY DETECTION

ALERT PRIORITIZATION & CONTEXT

SMARTER CORRELATION

CONTINUOUS MONITORING

AUTOMATED RESPONSE

Aligned to PCI DSS • Focused on CDE • Built for Compliance

BUSINESS IMPACT THAT MATTERS

- Reduce cyber risk to cardholder data and payment systems
- Prevent breaches & protect customer trust
- Improve security ROI and operational efficiency
- Ensure ongoing PCI DSS compliance
- Strengthen resilience of the payment ecosystem

ASHES TO ADAPTIVE RESILIENCE

AI-POWERED THREATS ARE EVOLVING. SO MUST WE.

TRADITIONAL SECURITY

Reactive. Manual. Static.

- **PERIMETER DEFENSES** — Network boundaries
- **LEGACY SIEM** — Too much noise
- **MANUAL OPERATIONS** — Slow and error-prone
- **STATIC POLICIES** — Rigid and outdated
- **ALERT FATIGUE** — Signals drowned
- **SILOED TOOLS** — Disconnected visibility
- **SLOW RESPONSE** — Minutes to hours
- **BUSINESS RISK** — Downtime. Data loss. Reputation damage.



FROM REACTIVE TO RESILIENT

Aligning security operations to PCI DSS controls for mastering outcomes.

PCI DSS CONTROLS IN ACTION

1. **PROTECT CARDHOLDER DATA** — Secure data & encryption
2. **SECURE SYSTEMS & NETWORKS** — Firewall, segmentation, secure configurations
3. **MANAGE ACCESS** — Least privilege, MFA, access control
4. **MONITOR & TEST** — Logging, monitoring, vulnerability management
5. **MAINTAIN POLICY** — Security policies, training, IR & change management



ADAPTIVE RESILIENCE

Integrated. Intelligent. Continuous.

- **EXPOSURE MANAGEMENT** — Continuous visibility across assets, users & data
- **PCI DSS ALIGNED DETECTION** — AI-powered detection mapped to PCI DSS risks
- **AUTONOMOUS CONTAINMENT** — Contain threats in real time to protect the CDE
- **THREAT INTELLIGENCE** — PCI ecosystem & global threat intelligence
- **IDENTITY PROTECTION** — Verify every identity and access
- **SOAR & AUTOMATION** — Orchestrate and automate response
- **CONTINUOUS VALIDATION** — Validate controls, configurations and security posture
- **RAPID RECOVERY & BUSINESS RESILIENCE** — Minimize impact. Recover faster.

THE FUTURE BELONGS TO ORGANIZATIONS THAT CAN SECURE CARDHOLDER DATA, ADAPT CONTROLS, AND RECOVER AT MACHINE SPEED.

STRONGER TOGETHER. People. Process. Technology.

BUILT FOR RESILIENCE. PCI DSS Aligned. Zero Trust Driven.

READY FOR ANYTHING. Protect Data. Protect Trust. Protect Business.

PCI DSS. SECURITY THAT PAYS OFF.

STRONG CONTROLS. SECURE PAYMENTS. TRUSTED BUSINESS.

PROTECT WHAT MATTERS MOST

PCI DSS focuses on securing the Cardholder Data Environment (CDE) and everything that touches it.

CARDHOLDER DATA
Protect data at rest, in transit and in use.

SECURE ENVIRONMENTS
Build and maintain secure networks and systems.

CONTROLLED ACCESS
Restrict access to those who need it, when they need it.

CONTINUOUS MONITORING
Track, detect and respond to anomalies across the CDE.

POLICIES & AWARENESS
Strong policies and trained teams reduce human risk.



OUTCOMES THAT MATTER

LOWER RISK
Reduce the risk of breaches and data compromise.

CUSTOMER TRUST
Build confidence with secure and reliable payments.

OPERATIONAL EXCELLENCE
Improve efficiency and strengthen control.

CONTINUOUS COMPLIANCE
Stay audit-ready. Stay ahead of change.

BUSINESS RESILIENCE
Protect payments. Protect revenue. Protect reputation.

ENABLERS OF COMPLIANCE & RESILIENCE

AI-POWERED INSIGHTS
Spot risks earlier.
Act smarter.

AUTOMATION
Reduce manual effort.
Eliminate gaps.

PEOPLE & PROCESS
Right skills. Right process.
Right mindset.

TECHNOLOGY INTEGRATION
Unified tools. Shared data.
Stronger outcomes.

THIRD-PARTY CONTROL
Secure partners.
Secure ecosystem.

PCI DSS ISN'T JUST A REQUIREMENT. IT'S A COMMITMENT TO SECURE EVERY PAYMENT, EVERY TIME.



THANK YOU

PROTECT
CARDHOLDER DATA

SECURE
EVERY LAYER

CONTROL
ACCESS

MONITOR
CONTINUOUSLY

RESPOND
EFFECTIVELY

COMPLY
CONTINUOUSLY