KPMG

Emerging Technology & Threats

2026 CAPA Conference

August 18, 2026

Risk velocity

The speed at which risk can emerge, spread, and impact your organization.

Why it matters

In today's dynamic environment, the impact of risk is no longer just about how big it is- but how fast it moves.

Understanding risk velocity helps organizations anticipate change, prioritize effectively, and respond before impact escalates.

Key drivers

Technology acceleration
New technologies and connectivity increase speed of change

Interconnected risks
Risks are more correlated and can trigger cascade effects

Information velocity
Information spreads faster- so do risks and reactions

External volatility
Geopolitical, economic, and societal shifts are accelerating

The risk velocity formula

Risk velocity = **Change rate** x **Propagation rate** x **Impact intensity** x **Exposure**

- **Change rate**: How quickly risk factors are changing
- **Propagation rate**: How quickly risk spreads across the organization or ecosystem
- **Impact intensity**: The potential impact if the risk materializes
- **Exposure**: The organization's vulnerability to the risk

Visualizing risk velocity

LOW VELOCITY → HIGH VELOCITY

1. Risk emerges
A new risk factor appears in the environment.

2. Risk spreads
The risk rapidly moves across functions, systems, or geographies.

3. Impact escalates
The risk begins to disrupt operations, performance, or stakeholder trust.

4. Value at stake
Financial, operational, regulatory, or reputational impact intensifies.

5. Window to respond narrows
The time to detect, decide, and act becomes critical.

Move from reactive to ready

By measuring and monitoring risk velocity, organizations can build earlier warning systems, focus on the right risks, and act with speed and confidence.

What you can do

- Monitor leading indicators of change
- Assess how quickly risks can spread
- Strengthen agility and response capability

Threat velocity

The speed at which a threat can emerge, move, and impact your organization.

Why it matters

Attackers move fast-leveraging automation, AI, and global reach.
Threat velocity measures how quickly threats outpace your ability to prevent, detect, and respond.
Understanding threat velocity helps organizations strengthen defenses, prioritize risks, and reduce time to containment.

Key drivers

Adversary speed
Attackers can scan, exploit, and move laterally faster than ever.

Attack surface expansion
Cloud, third parties, identities, and devices increase exposure.

Automation & AI
Tools and AI enable attackers to scale and adapt in real time.

Information & access
Dark web, leaked data, and easy-to-buy tools accelerate threat execution.

Weak signals to impact
The time from initial activity to material impact is shrinking.

The threat velocity formula

Threat velocity = **Adversary speed** How fast threat actors can act and adapt **X** **Propagation rate** How quickly a threat moves across your environment **X** **Impact potential** The potential harm if the threat is successful **X** **Exposure** The organization's vulnerability to the threat

Visualizing threat velocity

LOW THREAT VELOCITY > HIGH THREAT VELOCITY

1. Threat emerges
Adversary identifies a vulnerability or opportunity (e.g., exposed asset, phishing lure, misconfig).

2. Threat moves
Adversary gains access and moves quickly across systems, users, or applications.

3. Threat spreads
Lateral movement or propagation increases reach and data or system exposure.

4. Impact realized
Data loss, disruption, fraud, or other material impact occurs.

5. Window to respond closes
The time to detect and respond is too short for traditional controls to be effective.

Move from reactive to resilient

Reduce threat velocity by shrinking the attacker's window of opportunity and accelerating your detection and response.

Reduce exposure | Detect earlier | Respond faster | Strengthen continuously

What you can do

- Continuously monitor external and internal threat activity
- Prioritize remediation based on exploitability and impact
- Use threat intelligence to anticipate and disrupt adversaries
- Automate detection and response to reduce attacker dwell time
- Test, learn, and adapt to stay ahead

Threat velocity vs. risk velocity

Related but distinct: One focuses on the adversary, the other on the organization.

Threat velocity

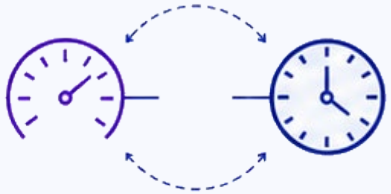
The speed at which a threat can emerge, move, and impact your organization.

Risk velocity

The speed at which risk can emerge, spread, and impact your organization.

DIMENSION	THREAT VELOCITY	RISK VELOCITY
Focus	Adversary behavior and capabilities	Business impact and organizational exposure
Primary question	How quickly can an attacker execute their objectives?	How quickly could the resulting risk impact our organization?
Perspective	Outside-in (adversary-centric)	Inside-out (business-centric)
Key drivers	Adversary speed, tools, tactics, infrastructure, automation, and reach	Change rate, propagation across the organization, impact intensity, and exposure
What it measures	Speed of the threat lifecycle: emerge -> move -> impact	Speed of risk realization: emerge -> spread -> impact
Purpose	Strengthen detection, prevention, and response to adversaries	Prioritize risks, allocate resources, and protect value
Example	A threat actor can move from initial access to privilege escalation in minutes.	A ransomware attack could encrypt critical systems across the business in hours.

HOW THEY CONNECT



Higher threat velocity increases the likelihood of risk- and can increase risk velocity.

Reducing **threat velocity** slows the attacker.

Reducing **risk velocity** limits the damage.

Do both to build a more resilient organization.

KEY TAKEAWAY

You can't stop every threat, but you can influence both velocities. Slow the attacker down. Limit the impact when they get through.

- Measure both.
- Improve both.

Outpace the threat.

Threat Snapshot

Cyber risk is shifting toward blended attack paths that combine automation, identity abuse, extortion, exploited vulnerabilities and third-party access. Leadership should focus on how quickly these paths can create business impact.

01 AI Acceleration

- Generative AI is boosting attack techniques, including reconnaissance and extortion workflows.
- The leadership issue is lower attacker effort, faster execution and convincing social engineering.
- Treat AI as an accelerator across current attack paths.

02 Identity/SaaS

- Vishing, MFA capture, token abuse and help-desk manipulation can turn one identity into broad access.
- SaaS platforms concentrate customer and employee data, creating exfiltration exposure.
- Focus on high-risk accounts, reset paths and integrations.

03 Ransomware

- Verizon reports ransomware involvement in nearly half of breaches, keeping extortion on the agenda.
- Readiness depends on tested recovery, decision rights, communications and escalation paths.
- Data theft can create pressure without full encryption.

04 Vulnerability Chain

- Software flaws, malicious code paths, CI/CD secrets and extensions can move from weakness to interruption.
- Oversight should include patch thresholds, exposure, repository controls and access.
- DevOps pathways can carry both speed and hidden risk.

05 Mobile/Social

- Attack pressure is shifting toward texts, calls and mobile workflows where users respond quickly.
- Awareness should test vishing, smishing and high-pressure approval prompts, not only email.
- Controls need to follow the channel attackers use.

KPMG

Top 20 emerging technologies for 2027 to 2030

Technologies set to reshape business and society over the next horizon

2027
Near term (1-2 years)

1	AI-augmented software engineering	Accelerates development, improves quality and lowers costs.
2	Intelligent agents (enterprise)	Automates complex work and enhances human productivity.
3	Hybrid cloud (including sovereign cloud)	Delivers flexibility, control and resilience in a cloud-first world.
4	Cybersecurity mesh	Strengthens security by enabling adaptive, zero-trust protection.
5	Data fabric	Unifies data across sources to power trusted insights and AI.
6	Composable applications	Enables faster innovation through modular, reusable building blocks.
7	Private 5G/6G (in early adoption)	Provides secure, high-performance connectivity for edge and IoT.

2028–2029
Mid term (2–3 years)

8	AI TRiSM (trust, risk and security management)	Builds trust in AI and ensures safe, responsible adoption at scale.
9	Digital twins (enterprise scale)	Optimizes operations and reduces cost, risk and downtime.
10	Quantum technologies (post-quantum cryptography)	Protects data and systems from quantum computing threats.
11	Edge AI	Enables real-time decisions closer to where data is created.
12	Climate tech (enabling net zero)	Accelerates the transition to a low-carbon, more sustainable future.
13	Synthetic biology (industrial applications)	Creates new materials, processes and solutions for health and sustainability.
14	Robotics (collaborative and autonomous)	Augments the workforce and improves safety, quality and productivity.

2030
Long term (3+ years)

15	Artificial general intelligence (AGI)	Has the potential to revolutionize knowledge work and innovation.
16	Spatial computing (advanced XR)	Transforms how we interact, collaborate and experience the world.
17	Quantum computing (advantage in practice)	Solves complex problems today's computers cannot.
18	Neuromorphic computing	Enables ultra-efficient AI at the speed and scale of the human brain.
19	Space technologies (commercial scale)	Expands access to space and unlocks new economic opportunities.
20	Decentralized physical infrastructure networks (DePIN)	Builds resilient, scalable networks owned and operated by communities.

Top 10 watchlist: breakout technologies post 2030

1	Brain-computer interfaces	Enabling direct communication between brain and digital systems.
2	Nanotechnology (advanced)	Engineering matter at the atomic scale to create new materials and devices.
3	Molecular computing	New computing paradigms using molecules for ultra-efficient information processing.
4	Programmable matter	Materials that can change shape, properties and function on demand.
5	Long-duration energy storage	Next-gen storage enabling reliable, clean energy at scale.
6	Fusion energy	Unlocking abundant, clean and sustainable energy.
7	Autonomous everything	Fully autonomous systems across mobility, logistics and operations.
8	Swarm intelligence systems	Distributed systems that collaborate and adapt like natural swarms.
9	Superintelligent AI systems	AI systems that exceed human intelligence across domains.
10	Geoengineering technologies	Large-scale interventions to restore earth systems and climate balance.

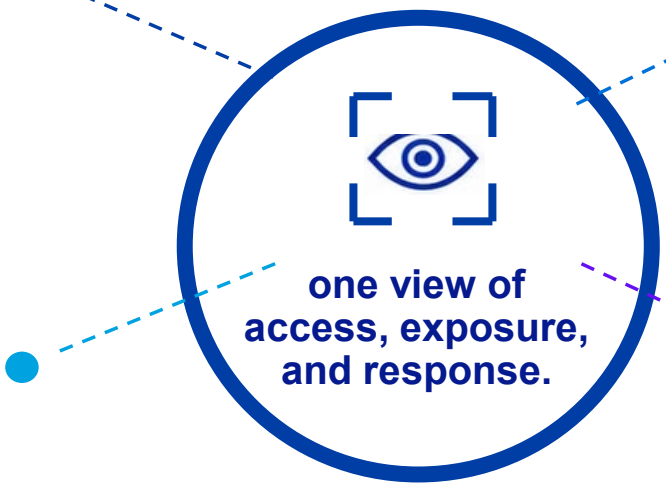
ATTACK SURFACE

The organization perimeter is fragmenting across control planes that attackers can chain together faster than teams can hand off

Cloud workloads, edge infrastructure, SaaS platforms, and third parties need one view of access, exposure, and response.

Mission — **Reduce cross-domain blind spots**

Vision — **Detect, govern, and contain access across endpoint, identity, cloud, edge, SaaS, and supplier pathways.**



Edge devices

- Find exposed appliances.
- Patch or isolate quickly.
- Monitor remote access.

Cloud workloads

- Baseline configurations.
- Centralize cloud logs.
- Tie access to identity.

SaaS data

- Control admin rights.
- Monitor exports.
- Rotate risky tokens.

Third parties

- Review access paths.
- Test response handoffs.
- Limit shared privilege.

KPMG

Agentic AI and Multi-Agent AI

Intelligent agents. Autonomous action. Exponential impact.

AI is evolving from tools that assist to agents that act. From a single agent executing tasks to networks of agents collaborating to achieve outcomes- this shift is unlocking new levels of autonomy, adaptability and value.

AGENTIC AI

One agent. Autonomous and goal-driven.

Agentic AI refers to AI systems that can perceive their environment, reason, make decisions and take actions autonomously to achieve specific goals with minimal human intervention.

KEY CHARACTERISTICS

Perceives Environment
Gathers information from data and context in real time.

Reasons and Plans
Understands objectives and determines the best course of action.

Takes Action
Executes tasks and interacts with systems or tools.

Learns and Adapts
Improves performance over time through feedback and experience.

Goal Focused
Works toward defined outcomes with minimal human oversight.

EXAMPLES

IT service resolution agent
Diagnoses issues, executes fixes and logs outcomes.

Intelligent research agent
Finds, analyzes and summarizes information to answer complex queries.

Procurement agent
Identifies suppliers, negotiates terms and places orders within policy guardrails.

MULTI-AGENT AI

Many agents. Working together to achieve outcomes.

Multi-agent AI systems consist of multiple AI agents that interact, collaborate, negotiate or compete with each other to achieve individual or shared goals.

KEY CHARACTERISTICS

Multiple Agents
Specialized agents with different roles, skills or perspectives.

Interaction & Communication
Agents exchange information to coordinate and collaborate.

Coordination & Collaboration
Work together to solve complex tasks beyond individual capabilities.

Negotiation & Adaptation
Adjust plans and resolve conflicts to optimize outcomes.

Shared or Individual Goals
Pursue shared objectives or aligned individual outcomes.

EXAMPLES

Fraud detection network
Agents monitor transactions, share signals and act to prevent fraud.

Supply chain optimization
Agents forecast demand, manage inventory and coordinate logistics.

Marketing campaign team
Agents create content, test variants, optimize spend and measure impact.

HOW THEY WORK TOGETHER

Agentic AI is the building block. Multi-agent AI is the multiplier. Together, they enable scalable autonomy and intelligent coordination at enterprise scale.

Agentic AI
Individual agents act autonomously to achieve defined goals.

+

Multi-Agent AI
Agents collaborate and orchestrate to deliver superior outcomes.

→

Business Value
Greater agility, better decisions, lower costs and new opportunities through intelligent automation.

Agentic AI and Multi-Agent AI

Intelligent agents. Autonomous action. Exponential impact.

AI is evolving from tools that assist to agents that act. From a single agent executing tasks to networks of agents collaborating to achieve outcomes- this shift is unlocking new levels of autonomy, adaptability and value.

AGENTIC AI

One agent. Autonomous and goal-driven.

Agentic AI refers to AI systems that can perceive their environment, reason, make decisions and take actions autonomously to achieve specific goals with minimal human intervention.

KEY CHARACTERISTICS

Perceives Environment
Gathers information from data and context in real time.

Reasons and Plans
Understands objectives and determines the best course of action.

Takes Action
Executes tasks and interacts with systems or tools.

Learns and Adapts
Improves performance over time through feedback and experience.

Goal Focused
Works toward defined outcomes with minimal human oversight.

EXAMPLES

IT service resolution agent
Diagnoses issues, executes fixes and logs outcomes.

Intelligent research agent
Finds, analyzes and summarizes information to answer complex queries.

Procurement agent
Identifies suppliers, negotiates terms and places orders within policy guardrails.

MULTI-AGENT AI

Many agents. Working together to achieve outcomes.

Multi-agent AI systems consist of multiple AI agents that interact, collaborate, negotiate or compete with each other to achieve individual or shared goals.

KEY CHARACTERISTICS

Multiple Agents
Specialized agents with different roles, skills or perspectives.

Interaction & Communication
Agents exchange information to coordinate and collaborate.

Coordination & Collaboration
Work together to solve complex tasks beyond individual capabilities.

Negotiation & Adaptation
Adjust plans and resolve conflicts to optimize outcomes.

Shared or Individual Goals
Pursue shared objectives or aligned individual outcomes.

EXAMPLES

Fraud detection network
Agents monitor transactions, share signals and act to prevent fraud.

Supply chain optimization
Agents forecast demand, manage inventory and coordinate logistics.

Marketing campaign team
Agents create content, test variants, optimize spend and measure impact.

Relevance to CAPA: These technologies can act independently, make decisions, and collaborate with other AI agents, creating new security, governance, and operational risks.

Edge AI and Connected Devices

Edge AI is the use of AI techniques embedded in non-IT products (consumer/commercial, industrial), Internet of Things (IoT) endpoints, gateways and edge servers. Capabilities span consumer, commercial and industrial uses, such as mobile devices, autonomous vehicles, enhanced medical diagnostics and streaming analytics. While predominantly focused on AI inference, more sophisticated systems include local training capabilities to optimize models at the edge.

How Edge AI Works

Edge AI processes data with AI on or near the device, enabling faster, real-time decisions without sending everything to the cloud.

Why it matters

- ✓ Real-time insights and actions where it happens
- ✓ Lower latency and reduced bandwidth costs
- ✓ Enhanced privacy and data security
- ✓ Greater reliability, even offline
- ✓ Scalable intelligence across distributed environments

How it works

1	2	3	4	5
Connected Devices	**Edge Processing with AI**	**Real-time Decision**	**Connected Ecosystem**	**Continuous Improvement**
Devices collect data from the physical world.	AI models analyze data locally on the edge device.	Insights are used instantly to trigger actions.	Only relevant data or events are sent to the cloud.	Models are updated and optimized continuously.

Business impact

Operational efficiency
Automate processes and reduce downtime

Customer experience
Deliver personalized, real-time interactions

Innovation at scale
Enable new smart products and services

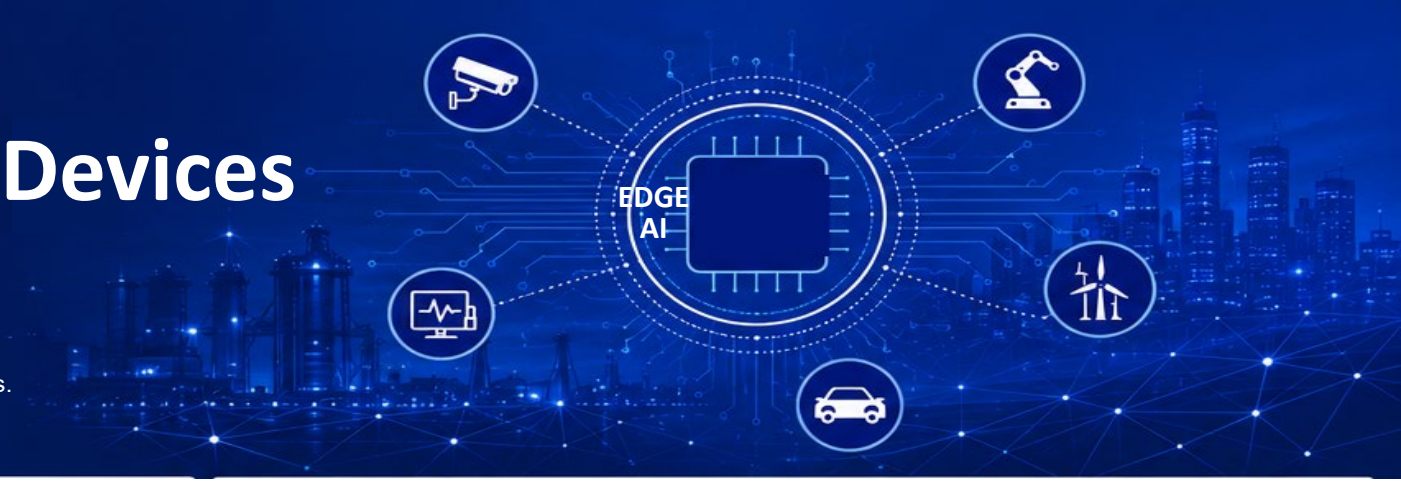
Resilience and agility
Respond faster in dynamic environments

KPMG

Edge AI and Connected Devices

Risks and Threats

Edge AI and connected devices deliver real-time intelligence and operational value while expanding the attack surface across devices, data, and distributed environments.



KEY RISKS

Edge AI and connected devices introduce unique risks across technology, data and operations.

Expanded attack surface

A large number of distributed devices and endpoints increase the number of potential entry points.

Data exposure and privacy

Sensitive data processed at the edge may be exposed due to weak protections or improper handling.

Device and model tampering

Edge devices and AI models can be manipulated, leading to incorrect decisions or malicious actions.

Insecure connectivity

Weak or unencrypted communications between devices, edge nodes and cloud create risk.

Lack of visibility and control

Limited visibility into device health, data flows and model behavior hinders threat detection.

Operational disruption

Attacks or failures can disrupt critical operations and impact safety, uptime and revenue.

THREATS TARGETING EDGE AI AND CONNECTED DEVICES

Adversaries are increasingly targeting edge environments to disrupt operations, steal data or gain a foothold in IT/OT systems.

Malware and ransomware

Malicious software can infect edge devices, encrypt data or disrupt services.

Credential theft and abuse

Stolen or weak credentials can be used to access and compromise devices.

Lateral movement and pivoting

Compromised edge devices can be used as a stepping stone to access broader networks.

AI model attacks

Adversaries can poison training data, manipulate models or exploit inference behavior.

Eavesdropping and man-in-the-middle

Attackers can intercept or alter data in transit between devices, edge and cloud.

Supply chain compromise

Vulnerabilities in hardware, firmware or third-party software can be exploited.

MITIGATE THE RISK. STRENGTHEN RESILIENCE.

A layered security approach is essential to protect Edge AI and connected environments.

Secure by design

Embed security into devices, AI models and infrastructure from the start.

Strong identity and access management

Enforce least privilege and multifactor authentication for users and devices.

Data protection

Encrypt data at rest and in transit. Minimize and anonymize where possible.

Continuous monitoring

Gain visibility across edge environments and detect anomalies in real time.

Vulnerability and patch management

Keep devices, firmware and models up to date and reduce exposure.

Resilience and response

Plan for incident response, recovery and business continuity at the edge.

Relevance to CAPA: They introduce new cybersecurity, privacy, and operational risks by increasing the attack surface and some devices are outside an organization’s ‘boundaries’.

KPMG

What is Zero Trust?

Zero Trust is a modern security approach that eliminates implicit trust and continuously verifies every user, device and connection-before granting access to resources.

Zero Trust in one sentence

Never trust, always verify.

Always authenticate, authorize and continuously validate based on least privilege access and context.

The 5 pillars of Zero Trust

1. **Verify explicitly**
   Authenticate and authorize based on all available data points-user, device, location, time, behavior and more.
2. **Use least privilege access**
   Grant only the minimum access required to perform a specific action-nothing more, nothing less.
3. **Assume breach**
   Design for the assumption that threats are already inside the network.
4. **Continuous validation**
   Continuously monitor user activity and re-verify trust before and during access.
5. **Protect everything**
   Secure all resources-apps, data, workloads and APIs-across on-prem, cloud and edge.

Zero Trust vs. Traditional security

Traditional approach: Trust but verify

Implicit trust once inside the network

User → Inside the network → Resources

Once users are inside the network, they have broad access to resources.

Zero Trust approach: Never trust, always verify

Continuous verification and least privilege access

User → Verify → Least privilege access → Monitor & validate continuously → Resources

Access is never assumed. It is continuously verified, limited to least privilege and monitored in real-time.

The outcome

Reduces risk
Minimizes the impact of breaches and lateral movement.

Strengthens security
Ensures the right access for the right users and devices.

Enables business agility
Secure access for a modern workforce across any location, any device.

Secure access. Protect data. Build by zero.

KPMG

Zero Trust: Risks to the Organization and Threats Against Zero Trust

Zero Trust strengthens security by eliminating implicit trust and continuously verifying every access request. However, organizations must understand the risks of implementing Zero Trust and the evolving threats that adversaries use to target it.

Risks Zero Trust Introduces to the Organization

While Zero Trust reduces risk, it also introduces new challenges that organizations must manage.

Higher implementation and operational costs

Zero Trust requires investment in technology, integration, automation and skilled resources. Ongoing monitoring and policy management increase operational overhead.

Complexity and operational disruption

Integrating Zero Trust across people, processes and technology can be complex and may disrupt business operations if not planned and executed carefully.

User experience and productivity impact

Continuous verification and least privilege access can introduce friction, potentially impacting user productivity and adoption if not well designed.

Performance and scalability challenges

Real-time verification, inspection and monitoring can impact application performance and may be challenging at scale without the right architecture.

Policy misconfiguration and over-restriction

Overly restrictive policies or misconfigurations can block legitimate access, cause outages, and lead to shadow IT or insecure workarounds.

Visibility and data privacy concerns

Extensive monitoring and data collection can raise privacy concerns and require strong governance and compliance controls.

Threats Against Zero Trust

Adversaries continuously evolve their tactics to bypass controls, steal identities and exploit trusted access.

Credential theft and account takeover

Phishing, malware and credential stuffing can steal valid credentials and bypass access controls.

Exploitation of vulnerabilities

Attackers exploit vulnerabilities in applications, endpoints, network devices and identity systems to gain initial access.

Abuse of legitimate access and permissions

Compromised accounts or excessive permissions can be abused to move laterally and access sensitive resources.

Misconfiguration and weak policies

Poorly configured policies, exceptions and overly broad access can be exploited to bypass Zero Trust controls.

Social engineering and insider threats

Attackers use manipulation to trick users or malicious insiders to bypass controls and gain trusted access.

Supply chain and third-party risks

Compromised vendors, partners and third-party applications can be a pathway to your environment.

Key takeaway

Zero Trust is not a product-it is a journey. Success depends on balancing security and business outcomes while continuously assessing risks and adapting to evolving threats.

Focus on:

- Strong identity security
- Least privilege access
- Continuous monitoring
- Automation and policy orchestration
- Ongoing assessment and improvement

Understand the risks, defend against threats and continuously strengthen your Zero Trust strategy to protect your organization, data and reputation.

Adaptive Zero Trust

Trust no one. Verify everything. Secure access for what matters.

Adaptive Zero Trust is a dynamic security approach that continuously verifies every user, device and connection-adapting in real time to risk and context.

THE ZERO TRUST PRINCIPLES

Verify explicitly
Always authenticate and authorize using strong identity.

Use least privilege
Grant minimal access based on need and context.

Assume breach
Continuously validate and monitor. Reduce blast radius.

Secure end-to-end
Encrypt, protect and monitor across all environments.

Adapt continuously
Use real-time signals and analytics to adjust access.

HOW ADAPTIVE ZERO TRUST WORKS

1. **Request** — User or device requests access to a resource.
2. **Verify** — Verify identity, device posture, and contextual risk in real time.
3. **Authorize** — Grant least privilege access based on policy and risk assessment.
4. **Monitor** — Continuously monitor behavior and environment for anomalies.
5. **Adapt** — Dynamically adjust access as risk and context change.

Continuous intelligence drives adaptation

Signals from users, devices, applications, data and the environment feed analytics and automation to refine access decisions in real time.

BUSINESS OUTCOMES

Stronger security
Reduce risk and prevent breaches.

Seamless experience
Enable secure access without compromising productivity.

Operational efficiency
Automate decisions and reduce security complexity.

Business agility
Adapt to change and support modern workloads.

Compliance and trust
Meet regulatory requirements and build stakeholder trust.

Relevance to CAPA: As technology gets more complex and diverse (cloud, Saas, data lakes) Zero Trust deals with threats more effectively by always verifying every user, device and application.

Digital Twins

Model the present. Predict the future.

Optimize real-world outcomes.

What are Digital Twins?

A digital twin is a dynamic virtual representation of a physical asset, process, system, or environment that is continuously updated with real-time data.

By mirroring the real world, digital twins enable organizations to monitor, simulate, analyze and optimize performance--helping to drive better decisions and outcomes.

Real-time connection

Continuously synced with live data from sensors, systems and sources.

Simulate and predict

Run scenarios and AI-driven models to predict outcomes and assess impact.

Monitor and analyze

Visualize performance, identify anomalies and uncover insights.

Optimize and act

Use insights to optimize operations, improve outcomes and drive value.

Why it matters

Digital twins bridge the gap between physical and digital--turning data into actionable insights, enabling smarter decisions, and creating sustainable competitive advantage.

Digital Twins

Model the present. Predict the future.
Optimize real-world outcomes.

What risks/threats do digital twins create?

While digital twins deliver significant value, they can also introduce new risks to organizations if not managed effectively.

Overreliance on models
Over-trust in simulations may lead to poor decisions if models are inaccurate or incomplete.

Bias and inaccurate outcomes
Poor data quality or biased algorithms can result in misleading insights and unfair outcomes.

Privacy and data exposure
Digital twins may process sensitive data about people, assets or operations, creating privacy risks.

Cost, complexity and vendor lock-in
High investment, complex integrations and proprietary platforms can limit agility and increase total cost.

Liability and accountability
Unclear accountability for decisions made using twin insights may increase legal risk.

What threats are there to digital twins themselves?

Digital twins are valuable assets that must be protected throughout their lifecycle from data ingestion to insight and action.

Cybersecurity threats
Risk of hacking, ransomware and unauthorized access that can disrupt operations or compromise safety.

Data integrity and quality
Inaccurate, incomplete or tampered data can compromise twin reliability and lead to flawed decisions.

Model drift and degradation
Models can become less accurate over time without recalibration and ongoing validation.

Availability and resilience
System outages or connectivity failures can disrupt twin operations and the delivery of critical insights.

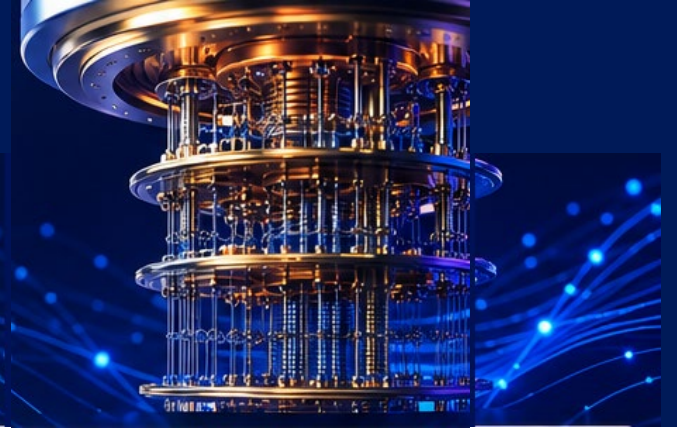
Access and insider threats
Excessive permissions or malicious insiders can lead to misuse, data manipulation or theft.

Third-party and supply chain risk
Vulnerabilities in third-party software, APIs or platforms can expose twins to external risk.

Relevance to CAPA: Digital twin can be used to simulate the current IT environment and landscape without need for complete duplicate environments. This allows for testing and simulation without impacting production.

Quantum computing & quantum safe

Quantum computing has the potential to solve problems beyond the reach of today's computers - unlocking innovation, but also introducing new risks. Organizations must act now to protect their data and systems, while understanding the new threats quantum capabilities and quantum safe cryptography may present.



RISKS TO TODAY: QUANTUM COMPUTING

Quantum computers could break many of today's widely used cryptographic algorithms.

1. Cryptographic breakthrough

Shor's algorithm could break widely used public-key cryptography (e.g., RSA, ECC), exposing encrypted data and digital signatures.

2. Data at risk today, decrypted tomorrow

"Harvest now, decrypt later" threats mean encrypted data captured today could be decrypted once quantum computers are powerful enough.

3. Impact across industries

Highly regulated sectors - including financial services, healthcare, government, and critical infrastructure - face significant exposure.

4. Loss of trust and integrity

Compromised cryptography could undermine trust in digital services, transactions, and communications.

5. Compliance and legal risk

Failure to prepare for post-quantum risks could result in regulatory breaches, legal liability, and reputational damage.

THREATS TOMORROW: QUANTUM COMPUTING AND QUANTUM SAFE CRYPTOGRAPHY

As quantum capabilities and quantum safe cryptography emerge, new risks and challenges will need to be managed.

1. Misuse of quantum computing

Quantum computers could be used to break encryption, accelerate attacks, or solve complex problems for malicious actors.

2. New attack vectors

Quantum capabilities may enable entirely new types of attacks that don't exist in classical environments.

3. Implementation and adoption risks of PQC

Poorly implemented quantum safe cryptography could introduce vulnerabilities or weaken security.

4. Performance and operational impact

Quantum safe algorithms may have larger key sizes and higher computational costs, impacting systems and operations.

5. Ecosystem and supply chain risk

Dependence on third parties, vendors, and evolving standards may introduce compatibility and security risks.

Build your quantum readiness journey

1. Assess

Assess crypto-agility, inventory cryptographic assets and data flows.

2. Prioritise

Prioritise use cases and systems based on risk and criticality.

3. Plan

Develop a transition roadmap to quantum safe cryptography.

4. Implement

Test, implement and integrate quantum safe solutions.

5. Monitor

Continuously monitor advances and adapt as standards evolve.

Relevance to CAPA: The road to quantum is going to be here sooner than we think with most predictions put some quantum availability between now and 2030. Post quantum cryptography will require planning and a roadmap for migration.

Data Loss Prevention

Discover. Classify. Protect. Monitor. Respond. Protect sensitive data across your organization.

What is Data Loss Prevention (DLP)?

DLP is a set of policies and technologies designed to help organizations identify, monitor, and protect sensitive data and prevent its unauthorized access, sharing, or exfiltration.

DLP helps you:

Protect sensitive data

Prevent exposure or misuse of critical data.

Meet compliance requirements

Support regulatory obligations and governance.

Reduce risk

Minimize breaches, fraud, and reputational damage.

Increase visibility and control

Understand data movement and enforce policies.

How DLP works

DLP provides an end-to-end solution to discover, classify, protect, and monitor sensitive data using adaptive policies and insights.

1 Discover

Automatically discover sensitive data across your environment using content scanning and analytics.

Examples
- Data map
- Content explorer
- Risk assessment

2 Classify

Apply sensitivity labels and trainable classifiers to categorize data based on content and context.

Examples
- Sensitivity labels
- Trainable classifiers
- Text and exact match

3 Protect

Create DLP policies to monitor and protect data in use, in motion, and at rest.

Examples
- DLP policies
- Encryption
- Authenticated activities

4 Monitor

Detect policy matches and get alerts with real-time and historical monitoring and reports.

Examples
- Policy match notifications
- Insider risk management
- Activity explorer

5 Respond

Investigate incidents and take action to stop data leaks and remediate risks.

Examples
- Incident investigation
- Policy overrides
- User coaching

Data Security Platforms

(DSPM + AI-powered DLP + Insider Risk)

A modern, integrated approach to discovering, protecting and monitoring sensitive data across your digital ecosystem.

Why It Matters

Data is everywhere
Spans cloud, SaaS, endpoints, databases, and AI tools.

Traditional security controls aren't enough
Perimeter-based solutions can't see or protect modern data flows.

Risk is dynamic
Insiders, compromised accounts, and AI usage create new exposure every day.

Regulators expect more
Stricter privacy, data residency, and breach reporting requirements.

Business depends on trust
Protecting sensitive data drives customer confidence and competitive advantage.

The Power of Integration

DSPM + AI-powered DLP + Insider Risk =

Data Security Posture Management

Discover, classify and continuously assess sensitive data and misconfigurations.

AI-powered Data Loss Prevention

Prevent sensitive data from leaving the organization using context, intent and AI understanding.

Insider Risk Management

Detect and mitigate risky insider behavior and potential threats in real time

Key Capabilities

Data Discovery & Classification
Find and classify sensitive data accurately

Continuous Posture Assessment
Identify risky exposures and configuration issues

AI-powered DLP & Context Awareness
Understand content, context and behavior to stop data loss

Insider Risk Detection
Spot risky activity before it becomes a breach

Monitoring & Analytics
Real-time insights and risk prioritization with dashboards

Policy Orchestration & Automation
Enforce consistent policies across environments

Compliance & Reporting
Simplify audits and meet regulatory requirements

Business Outcomes

Reduce data risk
Protect sensitive data across the entire lifecycle.

Prevent data loss
Stop exfiltration and misuse before it happens.

Manage insider risk
Detect and respond to risky internal behavior.

Strengthen compliance
Meet regulatory obligations with confidence.

Enable secure innovation
Adopt cloud and AI safely with visibility and control.

Lower cost and complexity
Consolidate tools and streamline operations

Relevance to CAPA: As technology gets more complex and diverse (cloud, Saas, data lakes) and threat actors and insider threats increase the need to manage data movement increases.

Data Security Platforms

(DSPM + AI-powered DLP + Insider Risk)

An integrated approach to discover, protect and monitor sensitive data and mitigate risks across your digital ecosystem.

Discover & Classify

Protect & Prevent

Monitor & Detect

Investigate & Respond

AI-Powered Insights

Reduce Risk

DSPM
Discover, classify and continuously assess sensitive data

AI-powered DLP
Prevent data loss using AI understanding and context

Insider Risk
Detect and mitigate insider threats in real time

RISKS TO IMPLEMENTING DATA SECURITY PLATFORMS

Implementing a Data Security Platform is complex. Organizations face strategic, operational and technical risks that can impact value realization.

Unclear Scope and Strategy	• Lack of clear objectives and success metrics • Poor alignment with business and risk priorities
Data Discovery and Classification Challenges	• Incomplete discovery across hybrid/cloud environments • Inaccurate classification leading to false positives/negatives
Complex Integration and Interoperability	• Integrating with multiple tools (IAM, SIEM, CASB, EDR, etc.) • API, data format, and workflow incompatibilities
Change Management and User Adoption	• Resistance from business users and IT teams • Lack of awareness and training reduces effectiveness
Policy Tuning and Operational Overhead	• Overly strict policies disrupt productivity • Under-tuned policies create alert fatigue and risk exposure
Cost, Resources and ROI Risk	• High total cost of ownership and tool sprawl • Difficulty proving ROI and securing ongoing investment
Privacy, Compliance and Legal Risk	• Misalignment with regulatory requirements • Cross-border data handling and residency concerns
Evolving Threats and Technology Obsolescence	• Rapidly changing threat landscape • Risk of platform not keeping pace with innovation

THREATS TO DATA SECURITY PLATFORMS

Data Security Platforms unify critical capabilities—making them a high-value target. Attackers and malicious insiders can exploit weaknesses across the platform.

Data Exfiltration Across Channels
Attackers can bypass controls to exfiltrate sensitive data via email, cloud, APIs, endpoints or removable media.

Privilege Abuse and Account Takeover
Compromised accounts or excessive privileges can be used to disable controls or access sensitive data.

Misconfigured Policies and Controls
Incorrect configurations, overly permissive rules or gaps can expose sensitive data.

Insider Threats and Data Theft
Malicious insiders can access, steal or leak data with legitimate access.

AI Model Manipulation and Evasion
Attackers can manipulate AI models to evade detection or generate false results.

Shadow Data and Unmanaged Assets
Sensitive data in unsanctioned apps, AI tools or shadow IT can bypass platform visibility and controls.

Supply Chain and Third-Party Risk
Vulnerabilities in third-party integrations or vendors can be exploited to access sensitive data.

Data Poisoning and Integrity Attacks
Attackers can alter data used for classification, training or analytics to corrupt insights or weaken controls.

Denial of Service and Platform Disruption
Attackers may disrupt platform availability, delaying detection and response to data risks.

Bottom line:
The more capabilities you integrate, the more critical it is to secure the platform itself. Continuous monitoring, strong access controls and adaptive defenses are essential.

KEY SUCCESS FACTORS

- Define a clear strategy and roadmap
- Start with high-value use cases
- Invest in data discovery and quality
- Operationalize with strong governance
- Continuously monitor, tune and improve
- Build a culture of security awareness

LEADERSHIP PRIORITIES

Leadership should fund a 2027 cyber agenda that prioritizes speed, identity, AI governance, and resilience proof over broad control sprawl

The priority is tighter leadership focus on the controls that reduce disruption, data exposure, fraud, and decision latency.

Priority area		Leadership action
Speed	1	Set board-visible metrics for detection, decision, containment, and high-risk vulnerability triage.
Access	2	Fund automation where it shortens response time without removing human decision rights.
	3	Prioritize phishing-resistant authentication for privileged, leadership, and high-risk workflow users.
	4	Extend identity governance to non-human identities, SaaS sessions, tokens, and AI agents.
Resilience	5	Define minimum viable operations for the processes that matter most during disruption.
	6	Run leadership exercises that test ransomware, extortion, supplier, and AI impersonation scenarios.

Key Takeaway: The leadership agenda should reduce the time between signal, decision, containment, and trusted business recovery.