Gartner Keynote: Top Trends for Cybersecurity 2024

Richard Addiscott
Patrick Hevesi

Gartner®

Persistent Forces

Influencing Cybersecurity Programs

Gartner

Persistent Forces

Influencing Cybersecurity Programs

Gartner

Persistent Forces

Influencing Cybersecurity Programs

Supply Chain
Interdependence

Gartner

Persistent Forces

Influencing Cybersecurity Programs

Gartner

Persistent Forces

Influencing Cybersecurity Programs

Gartner

Persistent Forces

Influencing Cybersecurity Programs

Gartner

Top Cybersecurity Trends

2024 Themes

Optimizing for

Resilience

Gartner

Top Cybersecurity Trends

2024 Themes

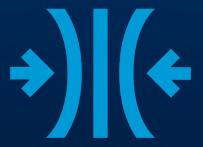
Optimizing for
Resilience

Optimizing for
Performance

Gartner

Top Cybersecurity Trends

2024 Themes



Optimizing for

Resilience

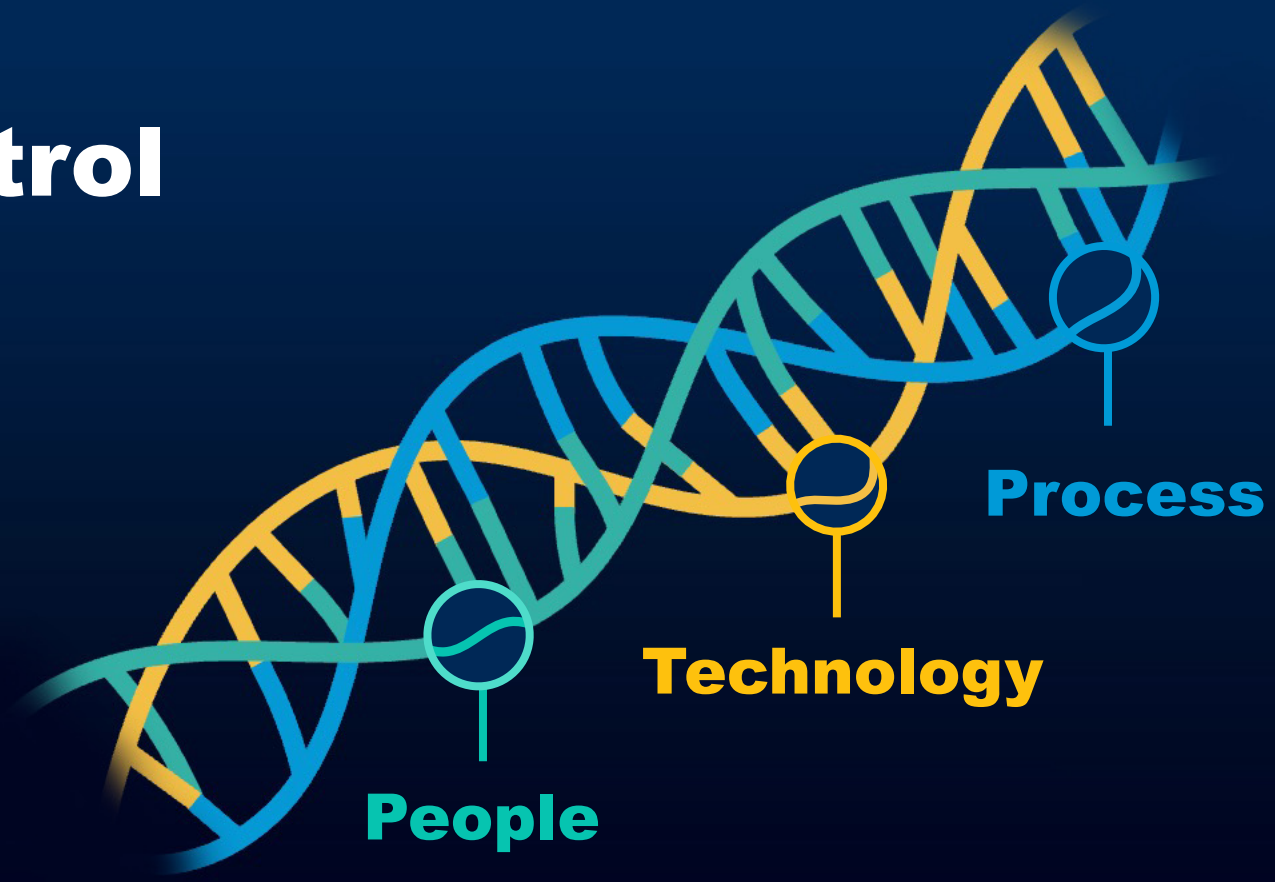
Optimizing for

Performance

Optimized Cybersecurity Programs

Gartner

The DNA of Security Control



Gartner

TREND 1

GenAI

Short-Term Skepticism, Longer-Term Hope

Analysis by:
Jeremy D'Hoinne, Avivah Litan, Angela Zhao, Mark Horvath

#newtrend #disruptive

Gartner

GenAI & Cybersecurity

- Application consumption
- Build GenAI applications
- Software supply chain

GenAI & Cybersecurity

GenAI & Cybersecurity

GenAI & Cybersecurity

Optimal
Next Steps

1

Inventory, monitor and manage in-house GenAI use cases.

2

Update provider requirements and implementation guidelines.

3

Learn how to secure new attack surfaces.

4

Experiment and measure.

Gartner®

Optimal
Next Steps

1

Inventory, monitor and manage in-house GenAI use cases.

2

Update provider requirements and implementation guidelines.

3

Learn how to secure new attack surfaces.

4

Experiment and measure.

Gartner®

Optimal Next Steps

1. Inventory, monitor and manage in-house GenAI use cases.
2. Update provider requirements and implementation guidelines.
3. Learn how to secure new attack surfaces.
4. Experiment and measure.

Gartner®

Optimal
Next Steps

1

Inventory, monitor and manage in-house GenAI use cases.

2

Update provider requirements and implementation guidelines.

3

Learn how to secure new attack surfaces.

4

Experiment and measure.

Gartner®

TREND 2

Cybersecurity Outcome-Driven Metrics

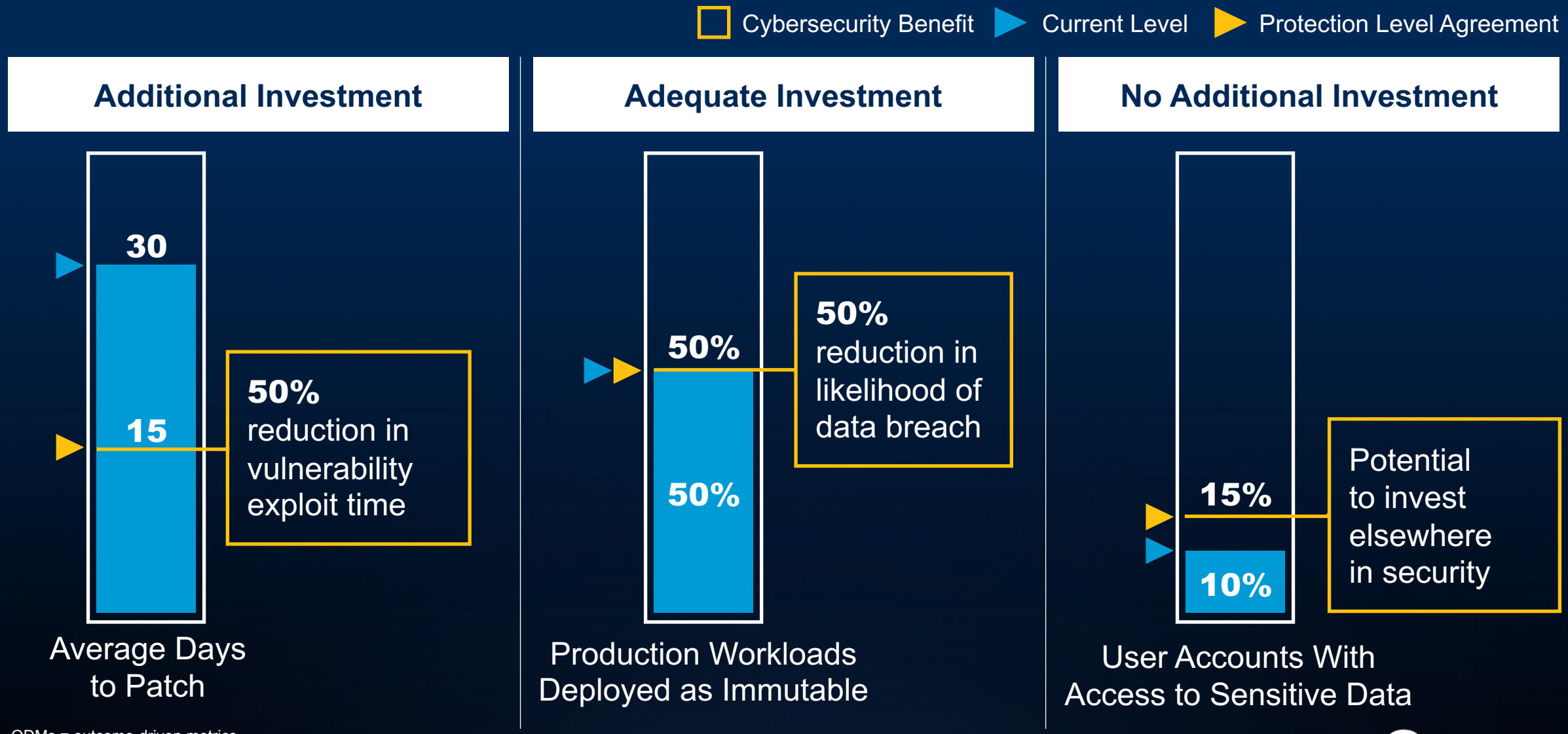
Bridging the Boardroom Communication Divide

Analysis by:
Paul Furtado, Christopher Mixter, Paul Proctor

#continuing

Gartner®

ODMs — Why They Work ...



ODMs = outcome-driven metrics

Gartner

Optimal Next Steps

1

Identify the key cybersecurity threats you're focused on, and the controls deployed against them. Develop ODMs for each.

2

Prepare your executive-level conversation based on ODM results.

3

Develop executive slide(s) to report on your positions.

Gartner®

Optimal
Next Steps

1

Identify the key cybersecurity threats you're focused on, and the controls deployed against them. Develop ODMs for each.

2

Prepare your executive-level conversation based on ODM results.

3

Develop executive slide(s) to report on your positions.

Gartner®

Optimal
Next Steps

1

Identify the key cybersecurity threats you're focused on, and the controls deployed against them. Develop ODMs for each.

2

Prepare your executive-level conversation based on ODM results.

3

Develop executive slide(s) to report on your positions.

Gartner®

TREND 3

Security Behavior & Culture Programs

Gain Increasing Traction to Reduce Human-Born Cybersecurity Risks

Analysis by:
Richard Addiscott, Andrew Walls, Christine Lee, Victoria Cason

#continuing #disruptive

Gartner®

Security Behavior and Culture Program

84%

Seek measurable behavior change as the primary objective of security awareness programs.

Gartner

SBCP focuses on

fostering new ways of thinking and embedding new behavior with the intent to provoke new, more secure ways of working across the organization.

SBCP = security behavior and culture program

Gartner

SBCP and the Gartner PIPE Framework

Gartner®

Optimal Next Steps

1. Ensure you extend your risk focus beyond the end-user behavior.
2. Review security incident history to focus on riskiest employee behaviors.
3. Adopt the Gartner PIPE Framework to guide your SBCP.
4. Use outcome-driven metrics to assess SBCP efficacy and sustain executive support.

Gartner®

Optimal Next Steps

1. Ensure you extend your risk focus beyond the end-user behavior.
2. Review security incident history to focus on riskiest employee behaviors.
3. Adopt the Gartner PIPE Framework to guide your SBCP.
4. Use outcome-driven metrics to assess SBCP efficacy and sustain executive support.

Gartner

Optimal Next Steps

1. Ensure you extend your risk focus beyond the end-user behavior.
2. Review security incident history to focus on riskiest employee behaviors.
3. Adopt the Gartner PIPE Framework to guide your SBCP.
4. Use outcome-driven metrics to assess SBCP efficacy and sustain executive support.

Gartner

Optimal Next Steps

1. Ensure you extend your risk focus beyond the end-user behavior.
2. Review security incident history to focus on riskiest employee behaviors.
3. Adopt the Gartner PIPE Framework to guide your SBCP.
4. Use outcome-driven metrics to assess SBCP efficacy and sustain executive support.

Gartner®

TREND 4

Evolving Cybersecurity Operating Models

Shifting Sands

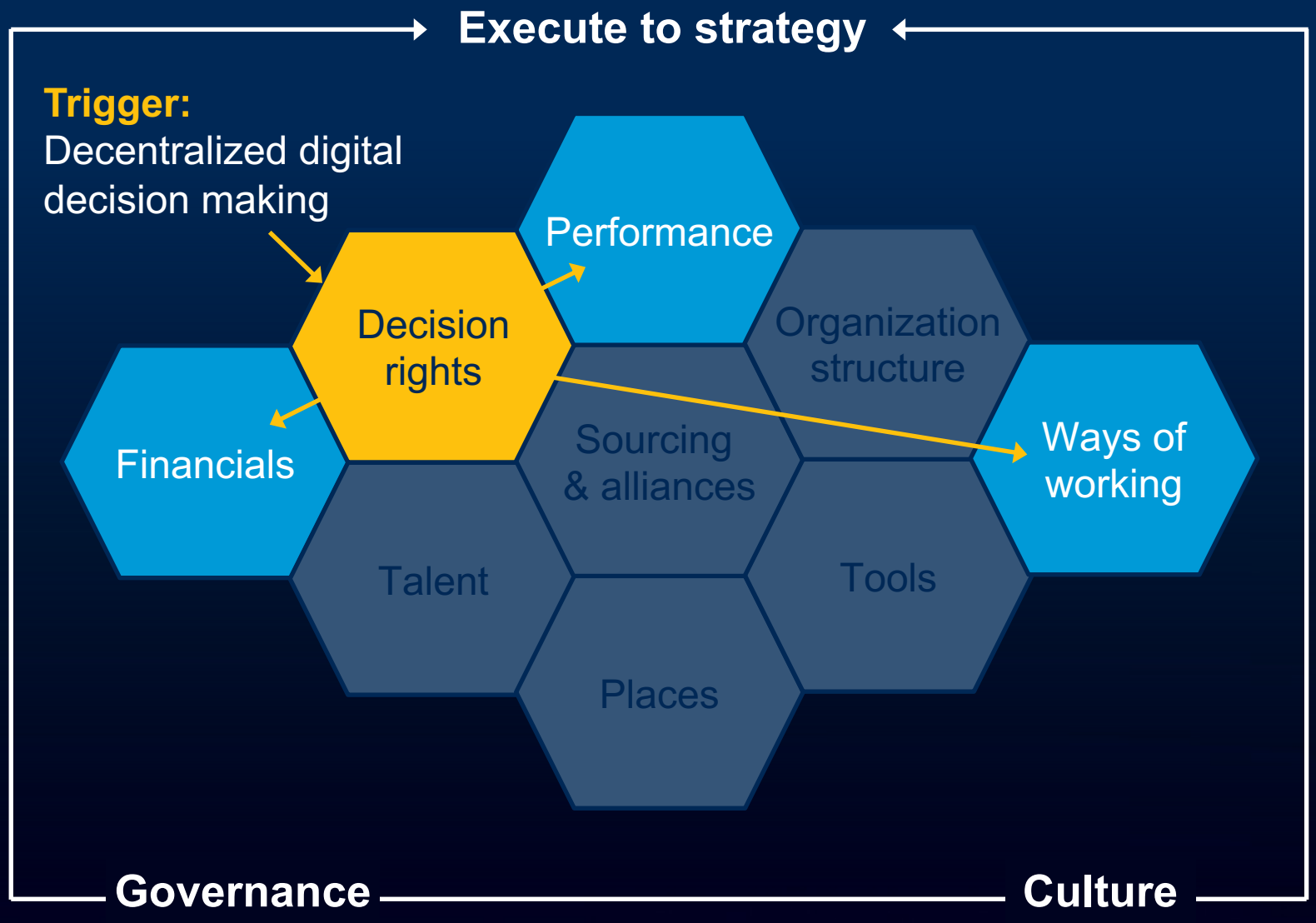
Analysis by:
Tom Scholtz, Oscar Isaka, William Candrick, Michael Kranawetter

#continuing #disruptive

Gartner®

Evolving Security Operating Model (Current State)

Evolving Security Operating Model (Change Triggered)



Evolving Security Operating Model

Evolving Security Operating Model

Evolving Security Operating Model

Evolving Security Operating Model (Future State)

Optimal Next Steps

1. Agree and establish owner accountability.
2. Centralize security risk decision making with business and information asset owners.
3. Formalize end-to-end enterprise risk management practices.
4. Liberalize policy and standards regime.

Gartner®

Optimal Next Steps

1. Agree and establish owner accountability.
2. Centralize security risk decision making with business and information asset owners.
3. Formalize end-to-end enterprise risk management practices.
4. Liberalize policy and standards regime.

Gartner®

Optimal Next Steps

1. Agree and establish owner accountability.
2. Centralize security risk decision making with business and information asset owners.
3. Formalize end-to-end enterprise risk management practices.
4. Liberalize policy and standards regime.

Gartner®

Optimal Next Steps

1. Agree and establish owner accountability.
2. Centralize security risk decision making with business and information asset owners.
3. Formalize end-to-end enterprise risk management practices.
4. Liberalize policy and standards regime.

Gartner®

TREND 5

Third-Party Cybersecurity Risk Management

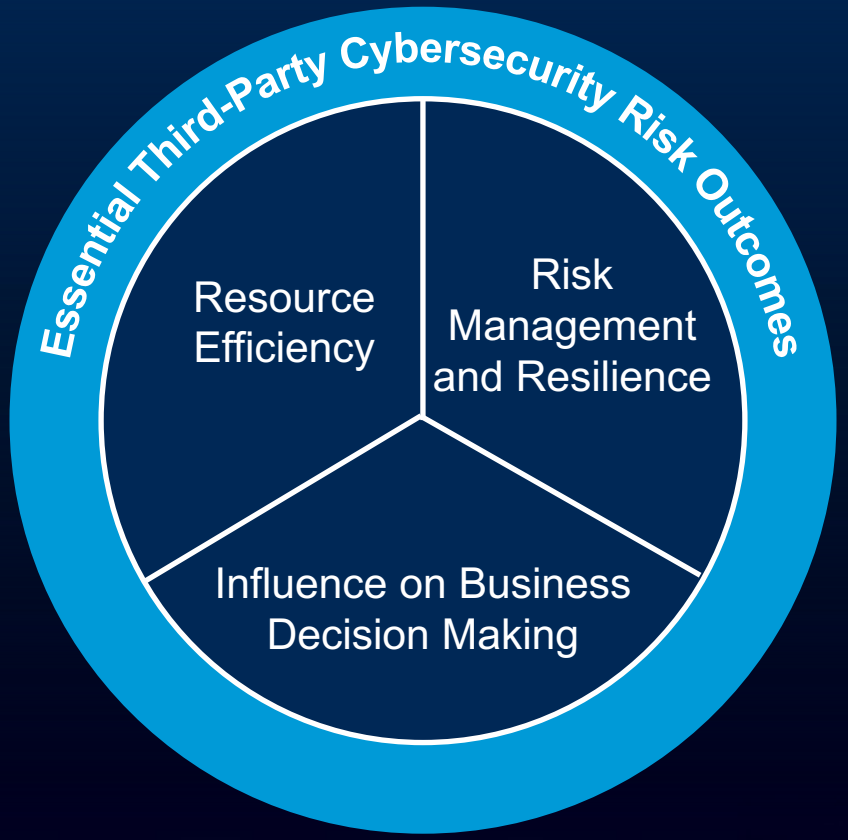
Resilience-Driven, Resource Efficient

Analysis by:
Chiara Girardi, Rahul Balakrishnan,
Luke Ellery, Christopher Mixter

#newtrend

Gartner®

Resilience-Driven, Resource-Efficient Third-Party Cybersecurity Risk Management



Resilience-Driven, Resource-Efficient Third-Party Cybersecurity Risk Management

Driven by cross-enterprise collaboration (e.g., partner with procurement, legal, enterprise risk management, business owners)

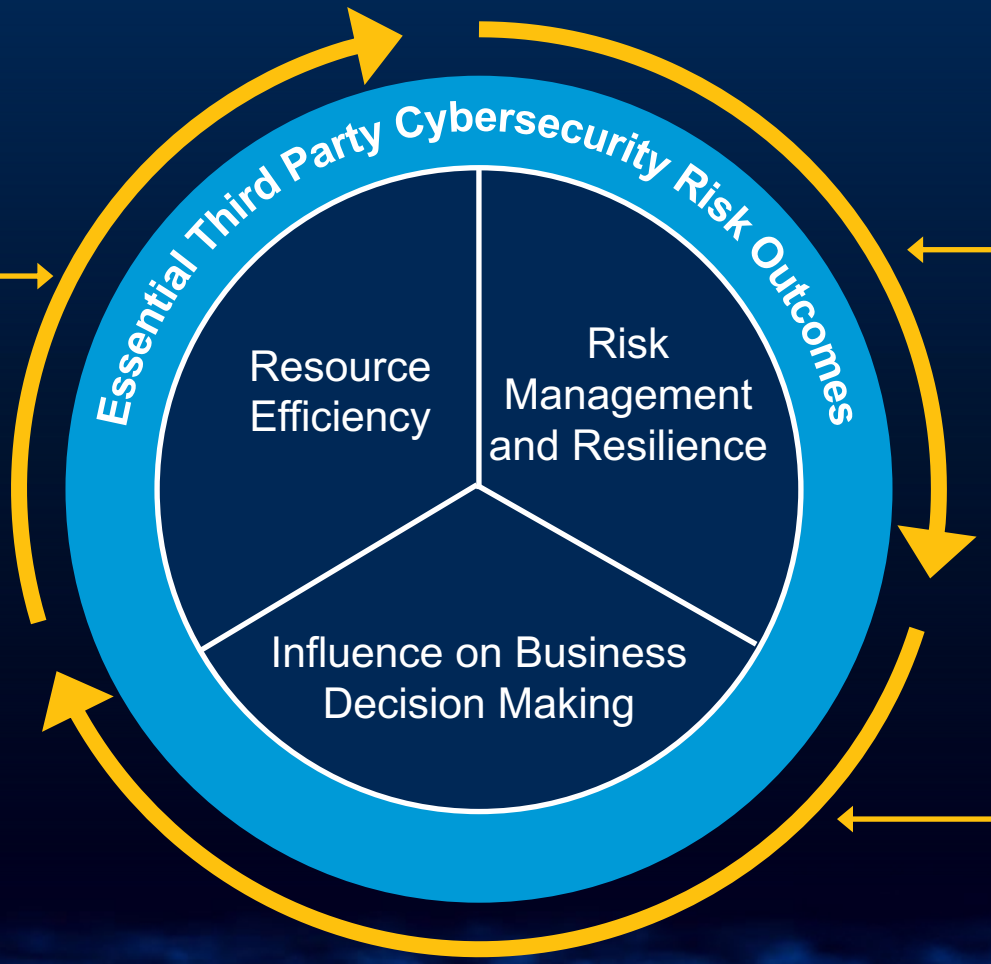
Resilience-Driven, Resource-Efficient Third-Party Cybersecurity Risk Management

Driven by cross-enterprise collaboration (e.g., partner with procurement, legal, enterprise risk management, business owners)

Focused on contingency planning (e.g., create third-party-specific playbooks, conduct table-top exercises, and define an offboarding strategy)

Resilience-Driven, Resource-Efficient Third-Party Cybersecurity Risk Management

Driven by cross-enterprise collaboration (e.g., partner with procurement, legal, enterprise risk management, business owners)



Focused on contingency planning (e.g., create third-party-specific playbooks, conduct table-top exercises, and define an offboarding strategy)

Centered on mutually beneficial relationships with critical third parties (e.g., share incident management best practices, recommend controls for managing risks)

Optimal
Next Steps

1

Strengthen your contingency plans for third-party engagements with the highest cybersecurity risk.

2

Reallocate resources to resilience-driven activities by making precontract due diligence more efficient.

3

Build mutually beneficial relationships with your most critical third parties.

Gartner®

Optimal
Next Steps

1

Strengthen your contingency plans for third-party engagements with the highest cybersecurity risk.

2

Reallocate resources to resilience-driven activities by making precontract due diligence more efficient.

3

Build mutually beneficial relationships with your most critical third parties.

Gartner®

Optimal
Next Steps

1

Strengthen your contingency plans for third-party engagements with the highest cybersecurity risk.

2

Reallocate resources to resilience-driven activities by making precontract due diligence more efficient.

3

Build mutually beneficial relationships with your most critical third parties.

Gartner®

TREND 6

Continuous Threat Exposure Management

Programs Gain Momentum

Analysis by:
Pete Shoard, Angela Zhao, Jeremy D'Hoinne, Jonathan Nunez

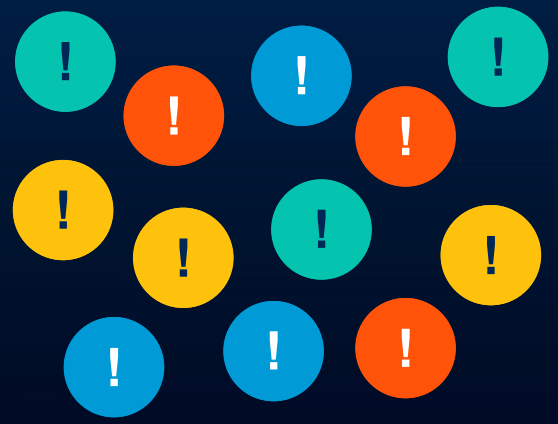
#continuing #disruptive

Gartner

CTEM

Steps Toward Producing Prioritized and Validated Risk Exposure

Exposures

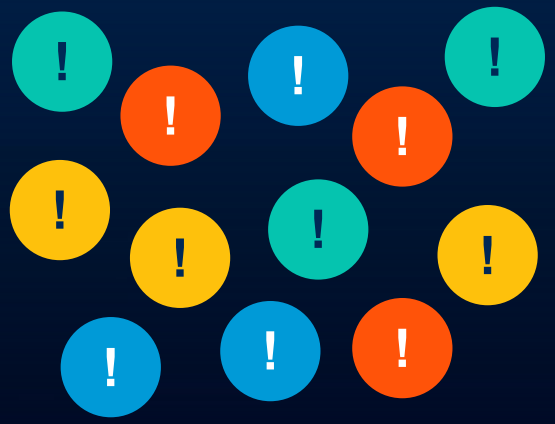


Explosion in attack surface leads to high volume, unscoped issue identification

CTEM

Steps Toward Producing Prioritized and Validated Risk Exposure

Exposures



Explosion in attack surface leads to high volume, unscoped issue identification

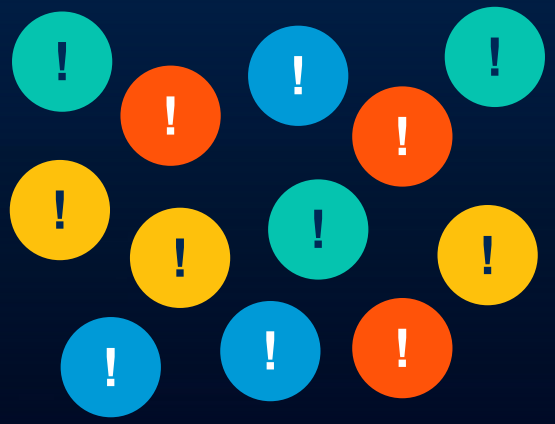
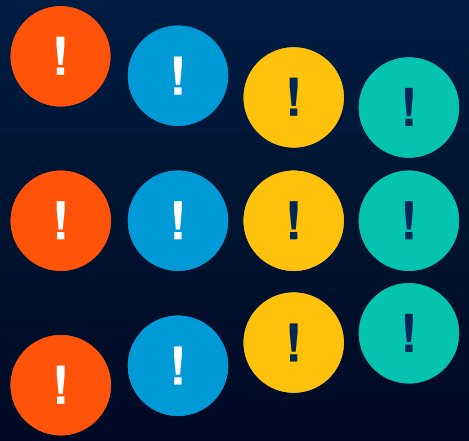
Prioritization

Issues are organized into business-driven scopes and prioritized by importance

Gartner

CTEM

Steps Toward Producing Prioritized and Validated Risk Exposure

Exposures	Prioritization	Validation
		
Explosion in attack surface leads to high volume, unscoped issue identification	Issues are organized into business-driven scopes and prioritized by importance	Validation works as a filter to prove which discovered exposures could actually impact the organization

CTEM

Steps Toward Producing Prioritized and Validated Risk Exposure

Exposures	Prioritization	Validation	Mobilization

Explosion in attack surface leads to high volume, unscoped issue identification	Issues are organized into business-driven scopes and prioritized by importance	Validation works as a filter to prove which discovered exposures could actually impact the organization	Prioritized and validated risk exposures are mobilized with the respective teams

Optimal Next Steps

1

Begin creating scoped exposure management target sets.

2

Expand the telemetry associated with exposure to incorporate broader risks.

3

Establish relationships and plan mobilization with departments outside of security.

4

Centralize the measurement and management of all exposure into a single view.

Gartner

Optimal Next Steps

1

Begin creating scoped exposure management target sets.

2

Expand the telemetry associated with exposure to incorporate broader risks.

3

Establish relationships and plan mobilization with departments outside of security.

4

Centralize the measurement and management of all exposure into a single view.

Gartner

Optimal Next Steps

1. Begin creating scoped exposure management target sets.
2. Expand the telemetry associated with exposure to incorporate broader risks.
3. Establish relationships and plan mobilization with departments outside of security.
4. Centralize the measurement and management of all exposure into a single view.

Gartner

Optimal Next Steps

1. Begin creating scoped exposure management target sets.
2. Expand the telemetry associated with exposure to incorporate broader risks.
3. Establish relationships and plan mobilization with departments outside of security.
4. Centralize the measurement and management of all exposure into a single view.

Gartner

TREND 7

Cybersecurity Reskilling

Helping Future-Proof the Organization

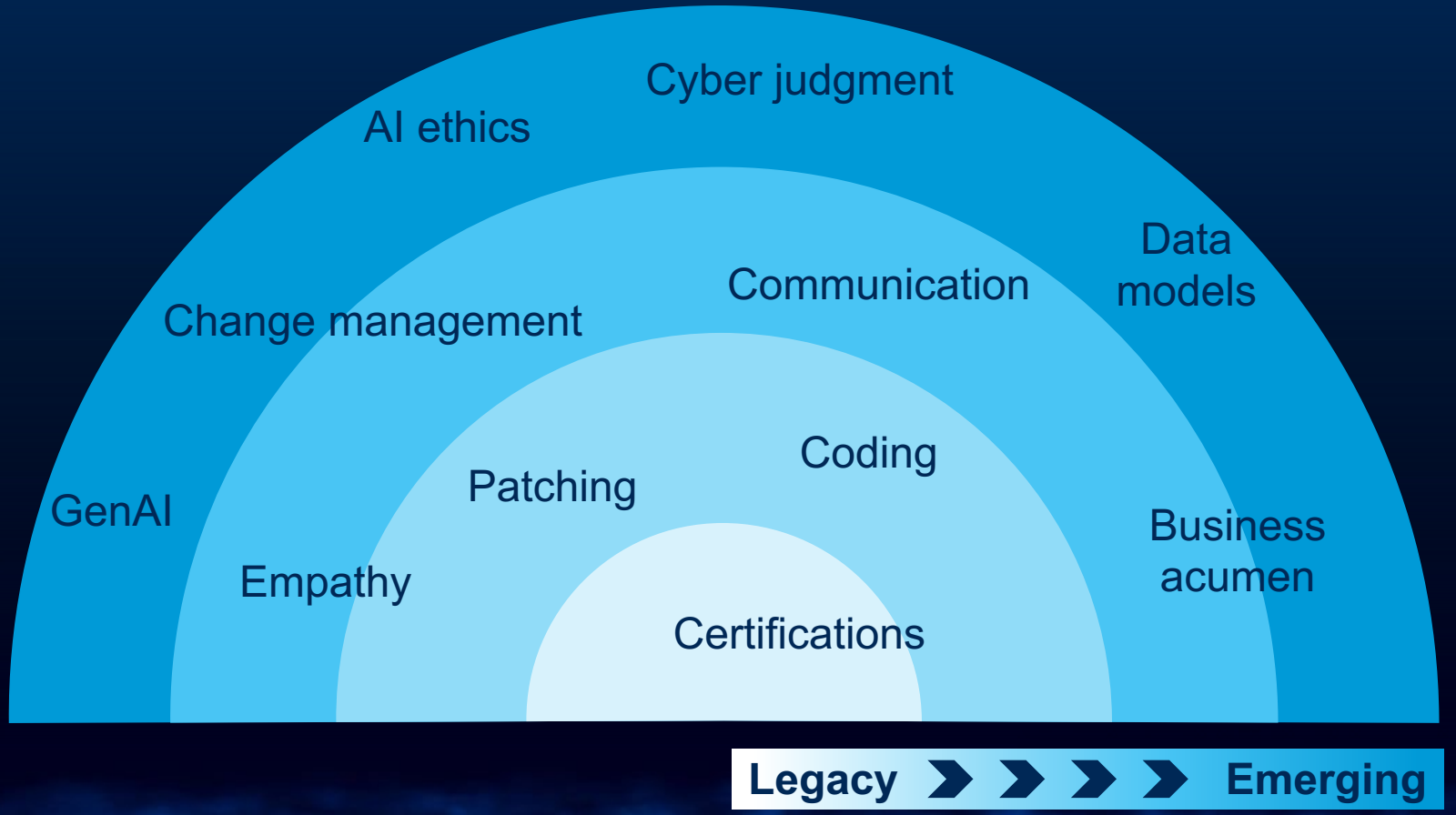
Analysis by:
William Candrick, John Watts, Jeremy D'Hoinne, Alex Michaels, Craig Porter

#continuing

Gartner®

Cybersecurity Reskilling

Evolving cybersecurity skills and requirements (illustrative examples)



Gartner

Optimal Next Steps

1

Develop a cybersecurity workforce plan.

2

Hire for the future — not the past.

3

Adopt an agile learning culture.

4

Monitor for new and emerging roles.

Gartner®

Optimal Next Steps

1. Develop a cybersecurity workforce plan.
2. Hire for the future — not the past.
3. Adopt an agile learning culture.
4. Monitor for new and emerging roles.

Gartner®

Optimal **Next Steps**

1

Develop a cybersecurity workforce plan.

2

Hire for the future — not the past.

3

Adopt an agile learning culture.

4

Monitor for new and emerging roles.

Gartner®

Optimal Next Steps

1

Develop a cybersecurity workforce plan.

2

Hire for the future — not the past.

3

Adopt an agile learning culture.

4

Monitor for new and emerging roles.

Gartner®

TREND 8

Extending IAM's

Role to Improve Cybersecurity Outcomes

Analysis by:
Felix Gaehtgens, Paul Rabinovich

#continuing #disruptive

Gartner®

IAM's Cybersecurity Role Extends

Gartner

IAM's Cybersecurity Role Extends

Optimal
Next Steps

1

Implement proper identity hygiene.

2

Expand identity threat detection and response (ITDR).

3

Evolve your identity infrastructure into an identity fabric.

Gartner®

Optimal Next Steps

1. Implement proper identity hygiene.
2. Expand identity threat detection and response (ITDR).
3. Evolve your identity infrastructure into an identity fabric.

Gartner

Optimal
Next Steps

1

Implement proper identity hygiene.

2

Expand identity threat detection and response (ITDR).

3

Evolve your identity infrastructure into an identity fabric.

Gartner®

TREND 9

Privacy-Driven Application & Data Decoupling

Enhancing Operations in a Fragmented World

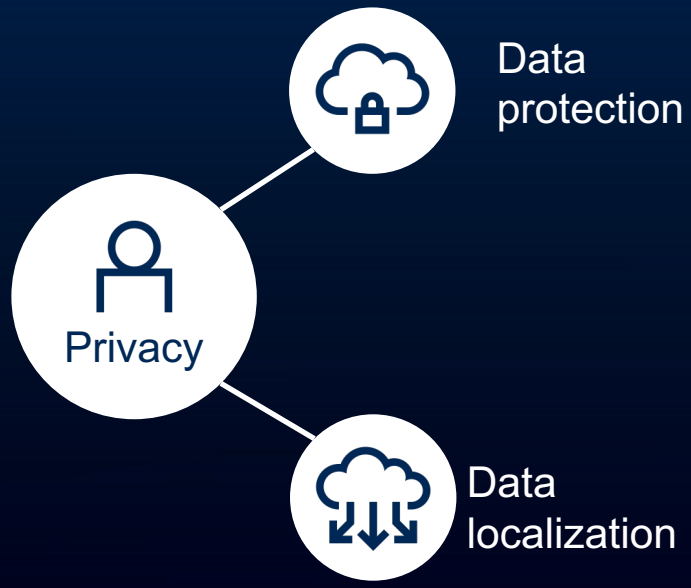
Analysis by:
Anson Chen, Bernard Woo

#continuing #disruptive

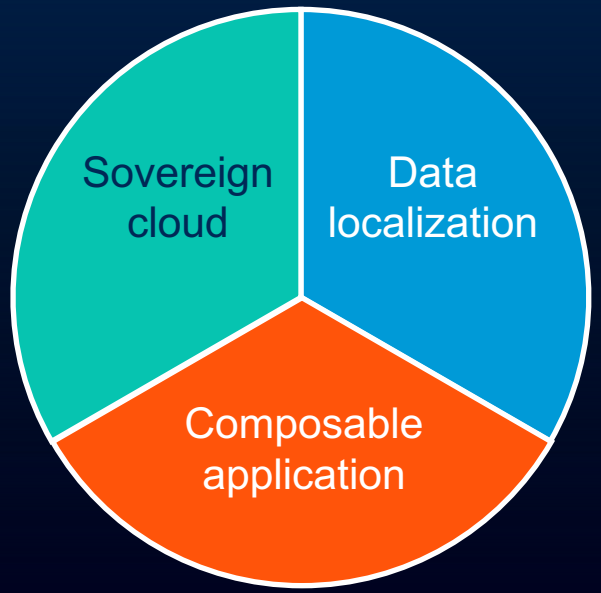
Gartner®

Privacy-Driven Application and Data Decoupling

Regulatory impact



Strategic decisions



Tactical initiatives

- Analyze data residency and privacy compliance
- Adopt data mapping and security strategy
- Apply security software development and privacy-focused threat modeling

Optimal
Next Steps

1

Collaborate with IT, business, and compliance leaders to identify localization requirements and compliance gaps.

2

Maintain data inventory and monitor flows of sensitive and personal data across geographies automatically.

3

Unify and align disparate security requirements and standards into the SDLC of decoupling applications.

SDLC = software development life cycle

Gartner®

Optimal
Next Steps

1

Collaborate with IT, business, and compliance leaders to identify localization requirements and compliance gaps.

2

Maintain data inventory and monitor flows of sensitive and personal data across geographies automatically.

3

Unify and align disparate security requirements and standards into the SDLC of decoupling applications.

SDLC = software development life cycle

Gartner®

Optimal Next Steps

1

Collaborate with IT, business, and compliance leaders to identify localization requirements and compliance gaps.

2

Maintain data inventory and monitor flows of sensitive and personal data across geographies automatically.

3

Unify and align disparate security requirements and standards into the SDLC of decoupling applications.

SDLC = software development life cycle

Gartner®

Recommendations

Utilize proactive collaboration with business stakeholders to help ensure the ethical, safe and secure use of GenAI.

Use business-aligned, outcome-driven metrics aligned to protection-level agreements to convey security program performance.

Focus on the human element to minimize the impact of insecure employee behavior and to reskill your existing team.

Optimizing for

Performance

Gartner

Recommendations

Utilize proactive collaboration with business stakeholders to help ensure the ethical, safe and secure use of GenAI.

Use business-aligned, outcome-driven metrics aligned to protection-level agreements to convey security program performance.

Focus on the human element to minimize the impact of insecure employee behavior and to reskill your existing team.

Optimizing for

Performance

Gartner

Recommendations

Utilize proactive collaboration with business stakeholders to help ensure the ethical, safe and secure use of GenAI.

Use business-aligned, outcome-driven metrics aligned to protection-level agreements to convey security program performance.

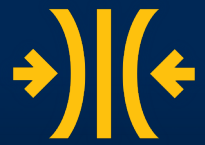
Focus on the human element to minimize the impact of insecure employee behavior and to reskill your existing team.

Optimizing for

Performance

Gartner

Recommendations



Optimizing for
Resilience

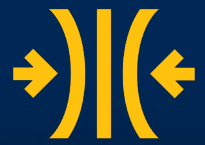
Establish mutually beneficial relationships with your most important external partners to improve third-party risk postures.

Continuously **monitor hybrid digital environments** to enable early identification and optimal prioritization of vulnerabilities to maintain a hardened organizational attack surface.

Sustain **focus on securing your identity fabric and leverage ITDR** to ensure your IAM capabilities are best positioned to support the breadth of the overall security program.

Gartner

Recommendations



Optimizing for
Resilience

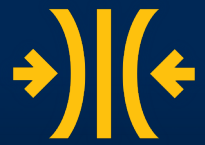
Establish mutually beneficial relationships with your most important external partners to improve third-party risk postures.

Continuously **monitor hybrid digital environments** to enable early identification and optimal prioritization of vulnerabilities to maintain a hardened organizational attack surface.

Sustain **focus on securing your identity fabric and leverage ITDR** to ensure your IAM capabilities are best positioned to support the breadth of the overall security program.

Gartner

Recommendations



Optimizing for
Resilience

Establish mutually beneficial relationships with your most important external partners to improve third-party risk postures.

Continuously **monitor hybrid digital environments** to enable early identification and optimal prioritization of vulnerabilities to maintain a hardened organizational attack surface.

Sustain **focus on securing your identity fabric and leverage ITDR** to ensure your IAM capabilities are best positioned to support the breadth of the overall security program.

Gartner

Top Cybersecurity Trends for 2024

Gartner

Recommended Gartner Research

- **Top Trends in Cybersecurity for 2024**
  Richard Addiscott, Jeremy D'Hoinne and Others
- **Implement a Continuous Threat Exposure Management (CTEM) Program**
  Jeremy D'Hoinne, Pete Shoard and Mitchell Schneider
- **4 Ways Generative AI Will Impact CISOs and Their Teams**
  Jeremy D'Hoinne, Avivah Litan and Peter Firstbrook
- **Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response**
  Henrique Teixeira, Peter Firstbrook and Others
- **Infographic: Minimize Disruption From Third-Party Cybersecurity Risks**
  Zachary Smith and Rahul Balakrishnan
- **Top Trends in Privacy Driving Your Business Through 2024**
  Nader Henein, Bart Willemsen and Bernard Woo

Recommended Gartner Research

- **CISO Foundations: Build a Culture of Security Consciousness: Introducing the Gartner PIPE Framework**
  Richard Addiscott, Andrew Walls and Others
- **Cybersecurity Business Value Benchmark**
  Christopher Mixter, Paul Proctor and Others
- **CISO Effectiveness: How to Attract, Retain and Release Cybersecurity Talent**
  Alex Michaels, Victoria Cason and Others
- **Predicts 2024: Augmented Cybersecurity Leadership Is Needed to Navigate Turbulent Times**
  Deepti Gopal, William Candrick and Others
- **Infographic: Building Cyber Judgment to Improve Risk Decision Making**
  Cybersecurity Research Team