illumio

EBOOK

Getting Started with Security Graphs: A Roadmap to Resilience

How security graphs can help you detect threats faster, strengthen Zero Trust, and make better risk decisions

Contents

Introduction: The case of the disappearing workloads 3
- Why relationships matter
- The graph opportunity

Understanding security graphs 5
- Graph theory origins
- The Königsberg Bridge Problem: where graph theory began
- What is a modern security graph?
- A versatile tool for security

High-value use cases for graph-based security 7
- Network visibility and asset mapping
- Threat detection and incident response
- Prioritizing vulnerabilities
- Insider threat detection

Graphs and Zero Trust: a perfect match 9
- Graphs support every core tenet
- Microsegmentation with graphs
- Relationship-based access control (ReBAC)
- Caught in the graph: stopping attacks before they spread

Strategic value for the business 11
- For enterprises: order to complexity
- For SMBs: cost-effective visualization that levels the field

What's next: the future of security graphs 12
- Graphs + AI = predictive defense
- Security in the hybrid multi-cloud era

Challenges to solve 13
- Data privacy and governance
- Scale and performance
- Complexity and skills

Getting started: a practical roadmap 13
- Find your first graph problem
- Start with what you have now
- What's 'graphable?' Your risk map, revealed
- Know when to invest in more capable tools
- Build skills and buy-in

Final takeaways 15

Unlock your free Illumio Insights trial 16

INTRODUCTION

The case of the disappearing workloads

A large enterprise asked for help with a strange alert. Its security platform had flagged outbound TeamViewer traffic, the kind often linked to state-sponsored attacks. The customer was skeptical. Its tools found no trace of TeamViewer anywhere — no running process, no installed software, no signs of compromise.

A small team of outside security experts took a different approach. Using a security graph, it traced the anomaly to a specific Azure resource. When the customer checked, the resource was gone. It left behind no container, log, or footprint.

"It's like the attacker would pop up on a hill, shoot at you, and then go away," recalled one of the experts involved. "Then they're shooting from another hill, and you never know where they're attacking from." [1]

> It's like the attacker would pop up on a hill, shoot at you, and then go away. Then they're shooting from another hill, and you never know where they're attacking from.

But the graph showed what the victim's tools couldn't: containers spinning up for just seconds, long enough to establish remote access, then vanishing without a trace.

The victim's tools searched in isolation. The graph connected the dots. It revealed how the ephemeral container briefly linked to other systems, creating a traceable pattern even after it disappeared.

This fleeting attack wasn't an edge case; it was a preview of what's coming. And it's why the future of cybersecurity is about mapping relationships, not chasing isolated events.

[1] Illumio. "The case of the disappearing workload – and what it says about the future of cyber-security." July 2025.

Why relationships matter

Modern cyber threats are growing fast. Global cybercrime has more than tripled over the last decade to an estimated $10.5 trillion this year.[2] And today's complex IT environments are making things worse. Organizations operate across data centers, public clouds, and edge computing nodes. And each of these produces thousands and thousands of security events every day.

Security teams must sift through this flood to find what matters. The challenge isn't just volume. It's context. Traditional tools examine events in isolation, missing the bigger picture. When attacks span multiple systems over time, connection points get lost.

This is what attackers count on. They move laterally through networks, escalating privileges and establishing persistence. They exploit relationships between systems that defenders can't see. The average breach in modern IT environments takes 276 days to detect and contain.[3] During this time, attackers map networks, understand system relationships, and move toward objectives.

Attacks hide in relationships — network connections, trust relationships, data flows, dependencies, and user behaviors. That's why understanding connections is critical for defense.

The graph opportunity

Graph theory offers a powerful solution by modeling complex relationships as nodes (entities) and edges (connections). In cybersecurity, this transforms abstract log data into intuitive visual maps.

A security graph is a living map of your digital ecosystem. Each user, device, application, and cloud resource becomes a node. And each connection, login, file access, and data transfer becomes an edge. This creates a comprehensive model showing not just what exists, but how everything connects. Security graphs give you:

- **Complete visibility.** A unified view spanning all domains instead of dozens of separate dashboards.
- **Attack path analysis.** Shows how attackers could move through your environment by following edges from entry points to valuable assets.
- **Real-time intelligence.** Updates continuously as your environment changes, crucial in dynamic cloud environments.
- **Intuitive communication.** Translates complex relationships into visuals that technical teams and business stakeholders understand.

Teams using graph-based security reduce risk in smart ways that don't impede business. They catch threats that they would otherwise miss. And when the inevitable breach happens, they resolve it faster.

[2] Steve Morgan (Cybercrime Magazine). "Cybercrime To Cost the World $9.5 trillion USD annually in 2024." October 2023.
[3] IBM. "Cost of a Data Breach Report 2025." July 2025.

Understanding security graphs

Before we can harness the power of security graphs, it's worth understanding where this approach comes from. What makes it different? And why is it so essential in today's cyber landscape?

Graph theory origins

Graph theory dates back to 1736, when Swiss mathematician Leonhard Euler tackled the Königsberg Bridge problem. (The challenge asked whether one could walk through the city and cross each of its seven bridges only once. See sidebar, this page.) Euler showed it was impossible. In doing so, he introduced the idea of modeling land masses as nodes and bridges as links. This breakthrough laid the groundwork for modern graph theory.

Over the centuries, this concept evolved from a mathematical curiosity into a practical tool for mapping relationships. In the aftermath of 9/11, intelligence agencies turned to graph-based analysis to "connect the dots" between people, places, and events across sprawling datasets — something other approaches couldn't match.

Soon after, the commercial world embraced graphs at scale. Google's PageRank algorithm revolutionized web search by ranking sites based on link structures. Facebook leveraged the "social graph" to model connections between users. These breakthroughs demonstrated the enormous value of relationship-based thinking—and paved the way for today's security graphs.

Using what would come to be known as graph theory, Leonhard Euler proved that the Königsberg Bridge Problem was impossible to solve.

The Königsberg Bridge Problem: where graph theory began

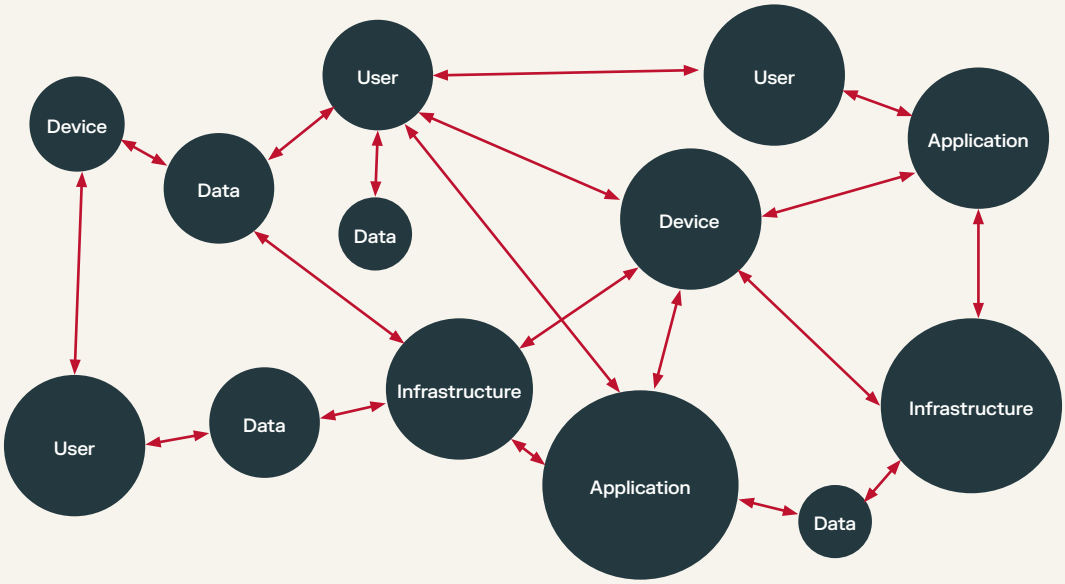
In 18th-century Prussia, the city of Königsberg posed a riddle that stumped its citizens: could one walk through the city and cross each of its seven bridges exactly once, without retracing steps? Mathematician Leonhard Euler took on the challenge and, in 1736, proved it was impossible. His breakthrough wasn't just the solution to a local curiosity — it marked the birth of graph theory.

Euler transformed the map of Königsberg into something abstract: land masses became "nodes," bridges became "edges," and the route became a matter of connection rather than geography. He realized that for such a walk to be possible, each landmass (or node) needed an even number of bridges (or edges) connected to it — a condition Königsberg didn't meet. This insight led to the first theorem of graph theory, what Euler called the "geometry of position."

Today, this seemingly quaint puzzle has profound implications for cybersecurity. Graph theory's power lies in its ability to model complex, real-world systems — from network flows and user permissions to attack paths and vulnerabilities. Just as Euler's graph exposed the limits of movement in Königsberg, security graphs expose the paths attackers could take through a digital environment — and help defenders break those paths before they're used.

What is a modern security graph?

A security graph is a dynamic map of your digital environment. Following in Euler's footsteps, it models cybersecurity as a set of interconnected relationships. Unlike traditional tools that examine systems in isolation, it treats your infrastructure as a living ecosystem.



Nodes - Users, devices, applications, infrastructure, data assets, and security events

Edges - Network communications, access patterns, privilege relationships, data flows, and dependencies

Together, the nodes and edges of your security graph create a holistic view, integrating all security tools into one model. You can query the graph instantly with things like:

- "Show me attack paths from the internet to our customer database."
- "Which users access both HR and financial systems?"
- "If this server gets compromised, what else could an attacker reach?"

Security graphs update continuously. When new virtual machines spin up, they appear automatically with their connections. This real-time accuracy is crucial. Environments are constantly changing; attackers move quickly.

A versatile tool for security

Graph analysis works across every security domain. Network teams use it for asset discovery and mapping. SOC analysts tap it to detect threats and respond to them. Risk teams apply it to prioritize which vulnerabilities to fix. Compliance teams generate audit reports.

Security graphs can also help teams explain complex information to non-technical stakeholders. Business leaders often understand risk visually, not in abstruse technical reports. Because of their inherently visual nature, security graphs can improve communication and help justify investments.

Most of all, graphs enable proactive security. Instead of just responding to alerts, teams can anticipate where attacks might succeed and quickly reduce their risk.

High-value use cases for graph-based security

Security graphs aren't just theoretical tools. They deliver real-world value across core security functions.

Here are a few use cases showing how graph-based approaches are solving some of today's toughest challenges.

Network visibility and asset mapping

Enterprises have long struggled to maintain accurate inventories of devices, applications, and data flows. Cloud services and hybrid environments are only making that harder.

Graph-based mapping addresses this by automatically building a living infrastructure model. It shows how assets connect and configure. This is crucial for attack surface management, because you can't protect what you can't see. A graph gives a visual map of the digital ecosystem — from servers linking to databases to cloud instances connecting storage to user accounts tied to devices.

What's more, this visibility updates continuously. Unlike static spreadsheets, graphs reflect changes as virtual machines spin up or devices connect. Gaps and unknown systems become apparent instantly.

Graphs offer regulatory compliance benefits too. A well-designed one can generate GDPR data flow maps or PCI network diagrams automatically. This proves to auditors that organizations understand and control where sensitive data travels.

As Zero Trust creator John Kindervag recently put it:

"A map forces clarity. It reveals blind spots. It shows where the gaps are — and where the enemy will go. In cybersecurity, the modern equivalent of a field map is the security graph. It's a real-time visualization of how workloads communicate, where users go, and which services are exposed. It's not just a list of IPs. It's your operational reality rendered intelligible."[4]

> "In cybersecurity, the modern equivalent of a field map is the security graph.

[4] Business Reporter. "Hold the High Ground: Cyber Terrain and Strategic Advantage." August 2025.

Threat detection and incident response

Graph analysis shines in threat detection. That's because modern attacks are multi-stage and move quickly through the environment.

For instance, an attacker might phish a user, pivot through systems, escalate privileges, and steal data. Tracking this through logs is like finding needles in multiple haystacks.

Graph analytics automatically connect attack dots. By correlating events, they find patterns that indicate coordinated intrusion. Failed logins on one node, successful admin login on another, and unusual data transfer can link as a chain. Together, these signs point to one thing: lateral movement.

Attack graphs map all possible attack paths in an environment. Before an attack, they show how vulnerabilities could combine to reach critical assets. During an attack, they help responders see how far attackers got and what connections they used.

What security graphs help illuminate

Before the attack
How vulnerabilities could give attackers a path to critical systems

During the attack
How far attackers got and what connections they used

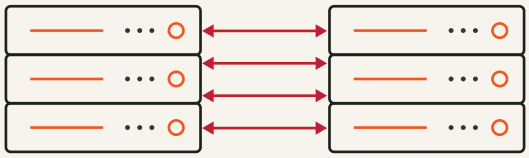
Interactive visualization is essential in security operations centers. Instead of scrolling through thousands of alerts, graphs let threat analysts see relationships at a glance. If one workstation connects to 50 alerts linking to known malware, they know where to focus.

Prioritizing vulnerabilities

Even the best enterprise environments have thousands of vulnerabilities. Graph analysis can show you where they are.

Vulnerability graphs highlight weaknesses that could combine to endanger your critical assets. Rather than treating each vulnerability alone, teams can use graph algorithms to assess attack paths.

For instance:



Server A
Missing a patch might allow remote code execution.

Server B
Has weak credentials.

If those two servers are connected, an attacker could exploit A, then move to B to do some real damage.

Graph visualization makes the danger palpable to non-technical stakeholders. Instead of explaining dozens of CVEs, teams can show simple graphs that highlight critical systems and the vulnerability chains that lead to them.

Insider threat detection

Insider threats are hard to detect. They stem from trusted users who have credentials and legitimate access. Graph analysis provides new ways to uncover insider risks by modeling user behaviors and relationships.

In a healthy organization, certain patterns are expected. Managers access HR systems. Engineers access source code repositories. But if a finance clerk suddenly accesses software-build servers, that's a problem.

Graph-based detection can reveal contextual clues by linking communication logs, file access logs, and social structures. An insider stealing data might show a unique pattern — visiting unusual external websites while accessing internal data they've never touched before.

When alerted to suspicious users, analysts can visually trace their connections. They see which systems users touched, who they communicated with, and what data flows they joined. This consolidated view quickly differentiates true malicious insiders from false positives.

Graphs and Zero Trust: a perfect match

Zero Trust has emerged as a guiding cybersecurity model. It shifts from the old perimeter-centric mindset to "never trust, always verify." Core tenets include:

- Assuming breach
- Enforcing least privilege
- Performing continuous verification

Graphs support every core tenet

Graphs aren't just compatible with Zero Trust. They make it operational. From segmentation to access control to monitoring, graphs give security teams the context and precision they need to enforce Zero Trust principles at scale.

Graph-based strategies align naturally with these principles. At its core, Zero Trust is about making dynamic, context-aware access decisions and monitoring all activities in real time. These tasks suit graph-based approaches perfectly.

Microsegmentation with graphs

Zero Trust networks aim for tight segmentation. Each service or application should communicate only what's necessary. Graph analysis can help define and enforce these boundaries. Here's how:

1. Real-time network-monitoring data streams into the graph.
2. By analyzing communication patterns as a graph, security teams identify clusters of systems that naturally talk to each other.
3. They also find "choke points" between segments where controls should apply.
4. Any edge that doesn't match approved patterns triggers alerts or automatic blocking.

For example, a graph of network flows might reveal that an application server talks to a database and cache. That's fine if those three make up a single segment. But there's no good reason for that app server to connect to an HR system in a different segment. If such a connection appears, we know that it's either misconfiguration or malicious.

Relationship-based access control (ReBAC)

Zero Trust challenges include how to enforce fine-grained authorization. Moving from coarse network rules to identity- and relationship-based rules can be tricky.

The good news: graph-based technology directly supports relationship-based access control models. Instead of simple roles, you might want a policy more along the lines of: "Allow access if the user reports to a manager who owns the resource's project and the request comes during business hours."

In traditional security, such nuance can be daunting — if not impossible. But with a graph, it's straightforward. Users, managers, and projects are simply nodes, with edges defining relationships.

Modern identity and access management systems built on graph backends can quickly determine whether access requests meet all the policy strictures. Graphs retrieve the entire entity context in just one query; this is much faster than computing separate policy checks.

Today's IT environments are dynamic — org charts change, priorities shift, and compute workloads are in constant flux. ReBAC means constantly reevaluating relationships within the environment. If a device's security posture changes, the graph edge representing "trusted device" might be removed. Instantly, any open sessions from that device can be rechecked and potentially terminated.

Graph-based security makes this kind of nuanced, context-rich access control not just possible, but practical and fast.

Caught in the graph: stopping attacks before they spread

What does graph-based security look like in the real world? Here are two examples of how organizations are using security graphs to catch threats and close risky gaps — in real time.

Bank stops lateral movement

A major bank was deep into its Zero Trust journey when it deployed a security graph. It stitched together data from Active Directory, endpoint management, network logs, and HR systems.

One day, the graph flagged something unusual: a user from the finance department trying to access a software repository in R&D using a personal laptop the system had never seen before.

There was no history of interaction between the user and that system, no business justification, and no trust relationship. That was enough for the graph-based policy engine to take action. Access was blocked automatically, and a security alert was triggered.

The investigation that followed uncovered a serious breach attempt. Attackers had stolen credentials and were trying to move laterally, likely to steal intellectual property. Thanks to the graph, the threat was caught and contained before any damage was done.

Tech firm finds exposed microservices

In another case, a tech company used graph visualization to prepare for microsegmentation.

By mapping real communication patterns between microservices, the team discovered several risky surprises: a backend service with a direct line to third-party APIs, and legacy systems quietly reaching into production databases.

These weren't in the architecture diagrams, but they were in the graph. The team quickly redesigned its segments, closing the gaps and locking down unnecessary pathways.

The result: a tighter, more resilient network — and a clear understanding of how everything actually connects.

Strategic value for the business

Graph-based cybersecurity is both a technical breakthrough and a strategic advantage. Whether you're a global enterprise or a resource-constrained SMB, graphs help you secure more, waste less, and make smarter decisions.

For enterprises: order to complexity

For large enterprises, the value of graph-based security lies in its ability to bring order to complexity. It delivers clarity, speed, and precision across sprawling environments.

Scalable monitoring of complex systems
Large enterprises maintain incredibly complex IT environments. Thousands of employees, devices, and applications span on-premises and hybrid multi-cloud platforms. Traditional monitoring tools struggle to provide unified views. But graph-based solutions scale naturally for complex, connected data.

A graph integrates data from disparate sources into one model. This unified visibility means security teams can ask broad questions spanning multiple domains. They can visualize "the big picture" and anticipate how small issues might impact critical assets elsewhere.

Enterprises benefit from advanced analytics on graphs. Algorithms for centrality and community detection identify essential nodes that, if compromised, would reach many others. This informs risk management and architecture decisions at a strategic level.

Improved incident response
Graph visualizations serve as common references that all stakeholders understand. During incidents, graph-based maps show what's affected and how attacks unfold. This clarity improves communication across security, IT, engineering, and management teams.

Regulatory compliance
Graphs simplify compliance documentation with clear evidence of network segmentation and data flow restrictions. A bank can show customer data segregation from the internet through multiple controls in one diagram. Live graphs auto-generate updated documentation and flag new connections that violate compliance rules.

For SMBs: leveling the cybersecurity field

Small and medium businesses face limited budgets and cybersecurity expertise shortages. At the same time, more than half of all cyberattacks target SMBs. Graph-based approaches offer cost-effective solutions that help level the playing field. They give SMBs enterprise-grade visibility and control without enterprise-sized budgets.

Cost-effective visualization
SMB environments can be surprisingly complex. Cloud services, on-site servers, and remote workers are all interconnected. And it might fall on just one person to manage it all. Graph-based tools make this more manageable with unified views of all systems and relationships, streamlining security operations.

Efficient resource use
SMBs must make the most of every dollar, every resource, and every second. Graph analysis helps teams prioritize focus areas and work smarter. A graph-based analysis might reveal that fixing, say, five key weaknesses would have a much bigger impact than fixing five others.

Graph visualization also helps SMB leadership understand cyber risks. For example, network graphs showing main databases directly accessible from employee PCs vividly illustrate risks that might require more budget.

Modern platforms
SMBs can take advantage of cloud-based graph security services that need no added infrastructure. By tapping into subscription services that offer graph analytics to correlate alerts and guide response, SMBs can get enterprise-grade power that helps them "punch above their weight."

What's next: the future of security graphs

As graph adoption accelerates, its future will be shaped by powerful new combinations — especially with AI. Together, they promise smarter, faster, and more proactive security. What was once reactive defense becomes predictive insight.

Graphs + AI = predictive defense

One of the most exciting security frontiers combines graph analysis with artificial intelligence and machine learning. Graphs provide rich contextual features that AI models can then use to make better predictions.

Machine learning algorithms can use graph-derived metrics as inputs to better determine whether an event is malicious or benign. If a model knows an endpoint is connected to critical systems, for instance, it might give alerts from that endpoint a higher urgency.

Graph-based neural networks represent a growing field of AI models built for graph data. They can learn complex connection patterns. And threat hunters can apply them to detect cyberattacks by learning from graphs of system behavior.

Consider the possibilities. Predictive threat analytics might analyze historical incident graphs to predict how future attacks might propagate or which vulnerabilities they will target. Unsupervised learning on graphs could surface unusual activity groupings that warrant investigation, even without matching known attack signatures.

In the future, we may even see graphs powering automated detection-and-response loops. AI agents could observe paths being traversed and instantly trigger defensive actions without waiting for human input.

Security in the hybrid multi-cloud era

Modern infrastructure is no longer confined to a single environment. It's a sprawling, fast-moving mix of clouds, platforms, and architectures. Servers spin up and terminate on demand, data flows change quickly, and traditional perimeters dissolve.

This complexity introduces new blind spots, fragmented controls, and unpredictable dependencies — problems that traditional tools have long struggled to manage.

A single misconfiguration in the cloud can lead to breaches. Often, these stem from insecure relationships, such as storage buckets open to the public or roles with overly broad trust permissions.

Fortunately, graph-based security is uniquely equipped to solve them. Graphs excel at capturing the fluid, interconnected nature of modern cloud environments. That includes everything from shifting configurations to complex relationships between services and identities.

That's why cloud security posture management increasingly relies on graph databases to model and monitor these dynamic systems. Graph queries can spot issues instantly, even across thousands of resources.

The ultimate vision is a global knowledge graph of the entire digital footprint, spanning on-premises networks, cloud accounts, SaaS apps, and mobile devices. Everything is linked through the users, data, and workflows that connect them.

Challenges to solve

As powerful as security graphs are, they're not without hurdles. To reach their full potential, organizations must navigate a few key technical, ethical, and operational challenges.

Data privacy and governance

Security graphs collect detailed information about systems and user behaviors. If not handled carefully, this raises privacy concerns and can actually create new targets for attackers. Organizations must enforce strict access controls and ethical guidelines for anyone who queries or views these graphs.

Graphs should strengthen security, not become tools of overreach. Striking the right balance between protection and privacy is essential (and non-negotiable).

Scale and performance

Analyzing large security graphs takes serious computing power. At the enterprise level, these graphs can include millions of nodes and tens of millions of connections. Processing that data in near real time is no small feat.

Fortunately, new technologies are rising to meet the challenge, including distributed graph databases and high-performance analytics engines that use in-memory computing and GPUs.

Complexity and skills

Graph techniques are powerful, but they require skills that can be in short supply. Security analysts must learn how to write graph queries and interpret the results. That can be a major shift for teams used to more traditional tools.

Fortunately, better interfaces and training are making graph analysis more accessible. As visualizations improve, understanding graph output is becoming as intuitive as reading a network diagram.

Making it easy: a practical roadmap

Adopting graph-based security doesn't have to be overwhelming. Start small, stay focused, and build momentum one use case at a time. The most successful teams begin with a single problem where relationships matter, then use early wins to drive broader adoption.

Here's a roadmap.

Find your first graph problem

The key to success is starting with a focused use case. Look for areas where relationships are crucial to understanding the problem:

- **Network visibility challenges.** Can't visualize how your systems connect?
- **Incident investigation gaps.** Missing context when piecing together attacks?
- **Cloud permission confusion.** Struggling to understand who can access what?
- **Vulnerability prioritization.** Don't know which patches matter most?

Pick one focused area and pilot a graph-based approach. For example, map user access privileges or visualize an attack sequence from past incident data.

Start with what you have now

You don't need to build graph solutions from scratch. More security platforms now offer some form of graph visualization or analysis features:

- SIEMs and XDRs often incorporate attack graphs or entity relationship views
- Cloud providers offer tools to map resource relationships
- Open-source graph databases like Neo4j can be used with exported security data

Explore existing features and see how they integrate into current workflows. Even a proof-of-concept graph of a network subset can yield immediate insights.

What's 'graphable?' Your risk map, revealed.

Every environment hides connections you can't see — and those connections are where attackers move. From orphaned accounts to unpatched systems linked to critical assets, a security graph turns invisible risk into a clear map you can act on.

Here are some of the potential security issues that go from hidden to obvious when they're mapped with a security graph.

Network and infrastructure

- Unknown or unmanaged devices connecting to the network
- Unnecessary open ports or firewall rules creating risky paths
- Direct connections between sensitive systems and the internet
- Flat network segments with no isolation
- Unexpected peer-to-peer communication between endpoints
- Shadow IT services or rogue network nodes

Vulnerabilities and misconfigurations

- Unpatched systems that connect to critical assets
- Vulnerabilities that chain together across multiple systems
- Misconfigured cloud storage buckets with public access
- Weak or default credentials on connected devices
- Misaligned segmentation rules exposing sensitive data paths
- Insecure dependencies between applications or services

Insider risk

- Users accessing resources far outside their normal scope
- Data exfiltration paths from internal to external nodes
- Sudden new connections between internal and personal devices
- Multiple employees connecting to the same external risky domain
- Unusual collaboration patterns that bypass normal workflows

Access and identity

- Excessive user privileges or privilege creep over time
- Orphaned accounts (especially from former employees or contractors)
- Users with access to unrelated high-risk systems (e.g., HR + finance)
- Lateral movement paths between accounts and systems
- Overly broad role-based access control (RBAC) permissions
- Dormant accounts that still have active credentials

Threat and attack activity

- Lateral movement across multiple nodes
- Command-and-control infrastructure linking to internal systems
- Phishing entry points leading to credential use in unusual places
- Unusual spikes in data transfer between nodes
- Multi-stage kill chains involving several systems or services
- Repeated failed logins followed by a successful privileged login

Cloud and hybrid environments

- Cross-cloud trust relationships that bypass security controls
- Overly permissive IAM role relationships
- Serverless functions with unnecessary network access
- Container workloads communicating outside their intended cluster
- API endpoints exposed without authentication
- Forgotten cloud resources still accessible via old credentials

Know when to invest in more capable tools

While many existing platforms offer basic graph features, they often come with limitations, such as static views, siloed data, or restricted query capabilities. As your use cases grow more complex, you may find that these tools can't keep up.

That's when it makes sense to explore purpose-built graph solutions. Modern graph-based security platforms offer real-time analysis, support for massive datasets, and dynamic queries across users, workloads, vulnerabilities, and more.

Upgrading doesn't mean starting over. It means unlocking deeper insight, faster detection, and stronger decisions at scale. For many teams, investing in graph-native tools is the next logical step in making security more connected and context-aware.

Build skills and buy-in

Encourage security analysts and IT staff to become familiar with graph concepts. This might involve:

- Training on graph query languages
- Workshops on visual analytics
- Cultivating a mindset that asks "Can we graph this?" for complex problems

Designate a "graph champion" to lead initial efforts and share success stories internally. Don't underestimate the power of graph visualizations in executive presentations. Concise visuals of threat landscapes or top risks can underscore interconnected risks and rally support for new security initiatives.

Final takeaways

In the vanishing container case we opened with, traditional security tools missed the attack entirely. Only graph-based analysis revealed the fleeting connections that exposed the threat. This points to a fundamental truth: attackers already think in graphs. They move through networks by exploiting relationships between systems.

From the attacker's perspective, the logic is simple: I'm in this node — what's my next node? That mindset lets them move with purpose, taking advantage of connections defenders often can't see.

If defenders want to stand a chance, they need to do the same, before that next shot comes from another hill.

Graph-based cybersecurity isn't just another tool. It's a new way of seeing and thinking about security that matches how attacks actually work. Organizations that embrace this approach today will have decisive advantages tomorrow, armed with insight, speed, and agility in the face of evolving threats.

The future belongs to those who can see the connections, understand what they mean, and act on them quickly.
Make sure you're one of them.

Unlock your free Illumio Insights trial

Attackers think in graphs, and they're using that perspective to find and exploit the hidden connections in your environment.

Illumio Insights gives you the same advantage. See hidden risk with a real-time map of every workload, user, and data flow. Detect active attacks as they unfold by spotting suspicious paths and behaviors. And contain threats with one click to stop lateral movement instantly.

Start your free Insights trial today and see your network the way attackers do — before they strike.

Experience Insights today at www.illumio.com/insights-free-trial