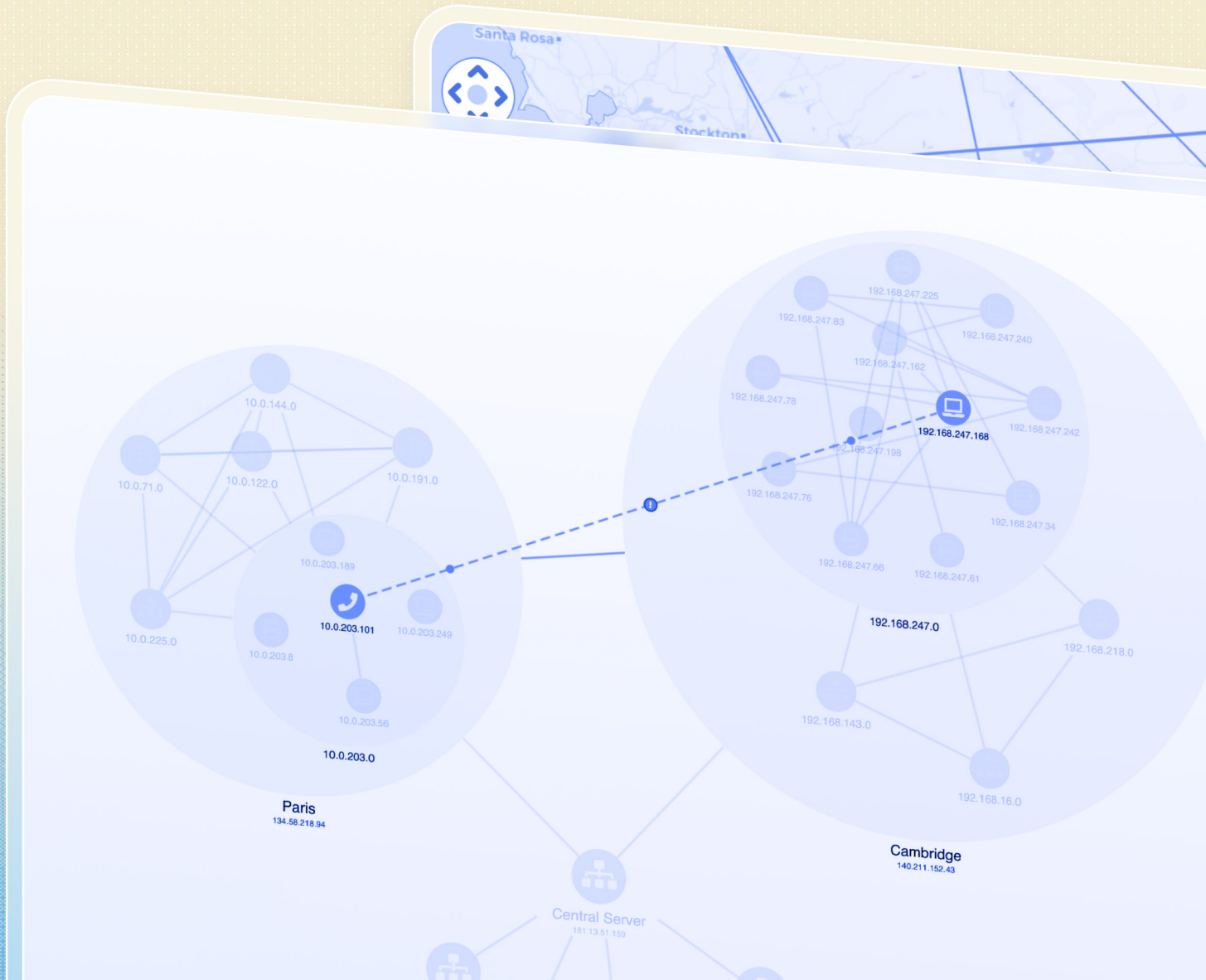
Cambridge Intelligence

Visualizing cybersecurity threats



Contents

The cybersecurity challenge

Cybersecurity is a big data challenge. Organizations collate and process terabytes of disparate information every day - from cloud infrastructure, identity systems, endpoints, applications and open-source intelligence - to uncover activity that could indicate risk or threat.

These processes generate thousands of alerts every day, but only a fraction matter. Failing to spot the right signal means real organizational risk. Analysts can't act reliably without seeing the full picture first. That's why data visualization is critical.

In this white paper, we'll share some of the ways our graph, timeline and geospatial visualization SDKs make complex cybersecurity data easier for analysts to understand - powering faster detection, sharper investigation, and better decisions.

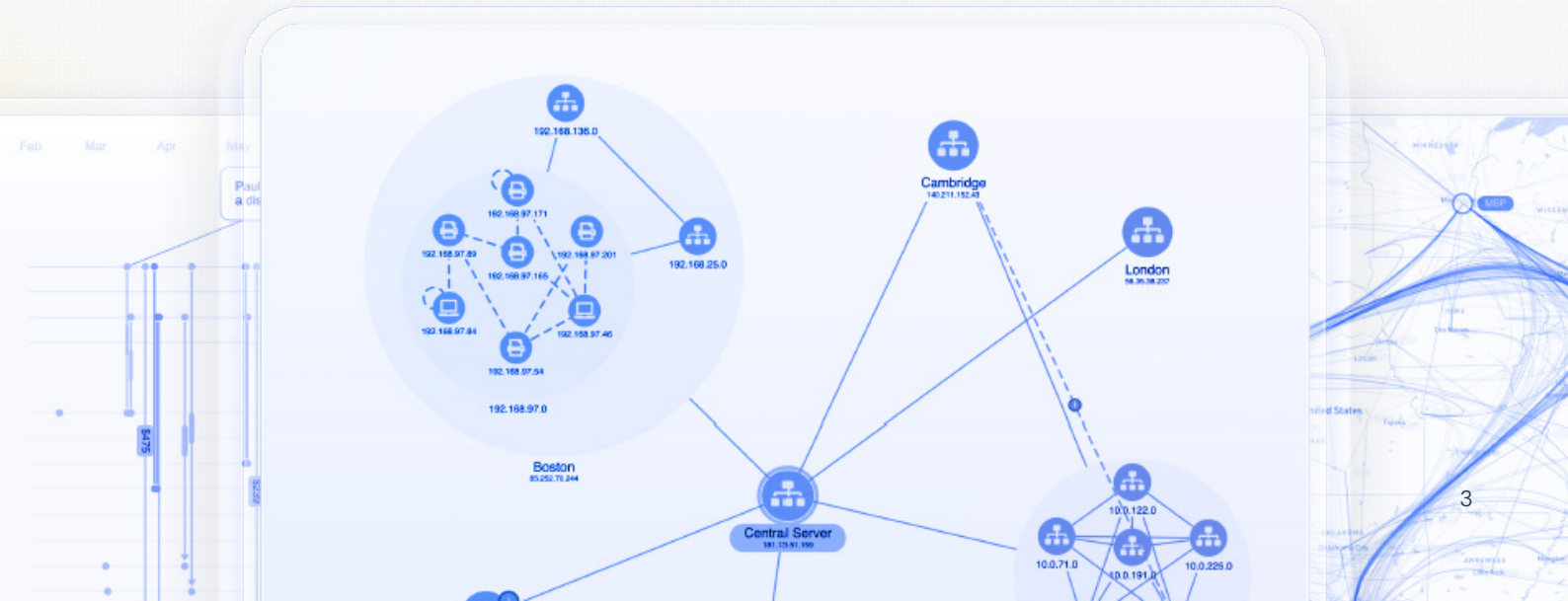
Introducing graph, timeline, and map visualization

Whenever an event occurs - two devices connect, a user logs into a system, or a piece of malware gets propagated around a network - it creates a digital footprint. Whether you're proactively securing your systems from malicious activity, combating an ongoing attack, or running post-attack forensics, you need to understand those connected footprints. Our toolkits provide three versatile ways to do that.

1. **Graph visualization**: visually representing complex connected data as interactive node-link diagrams. An intuitive and flexible way to 'join the dots' across attack paths and get a deep understanding of assets, relationships, and threat actor infrastructure.

2. **Timeline visualization**: a technique for visualizing sequences of events, how they unfold and how they link together. It gives cyber analysts a clear picture of the chronology of an attack, highlighting unusual patterns and pinpointing the moment of initial compromise.

3. **Geospatial visualization**: presenting data on a map mirrors how we naturally understand the world, helping analysts quickly recognize correlations, spot anomalies like unexpected foreign traffic, and deeply explore the geographic origins and spread of threats.



Visualizing cloud security

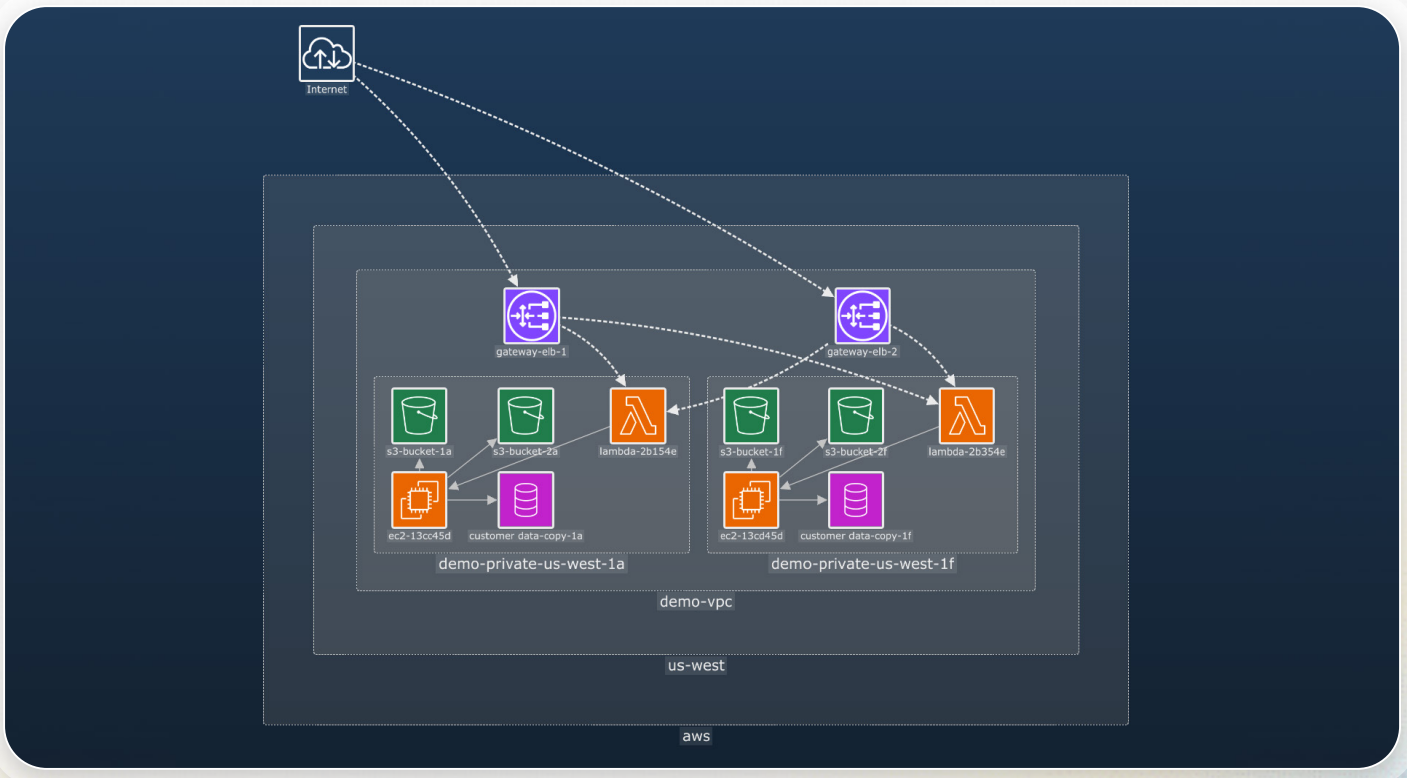
Cloud infrastructure has transformed the cybersecurity challenge. As organizations move to AWS, Azure and GCP, the assets that need protecting - compute instances, storage buckets, firewalls, identity roles - are no longer physical objects you can inventory. They scale on demand, they're defined in configuration files, and they connect to each other in ways that aren't always obvious even to the teams that built them.

If you can't see your cloud environment clearly, you can't protect it.

Mapping your cloud estate

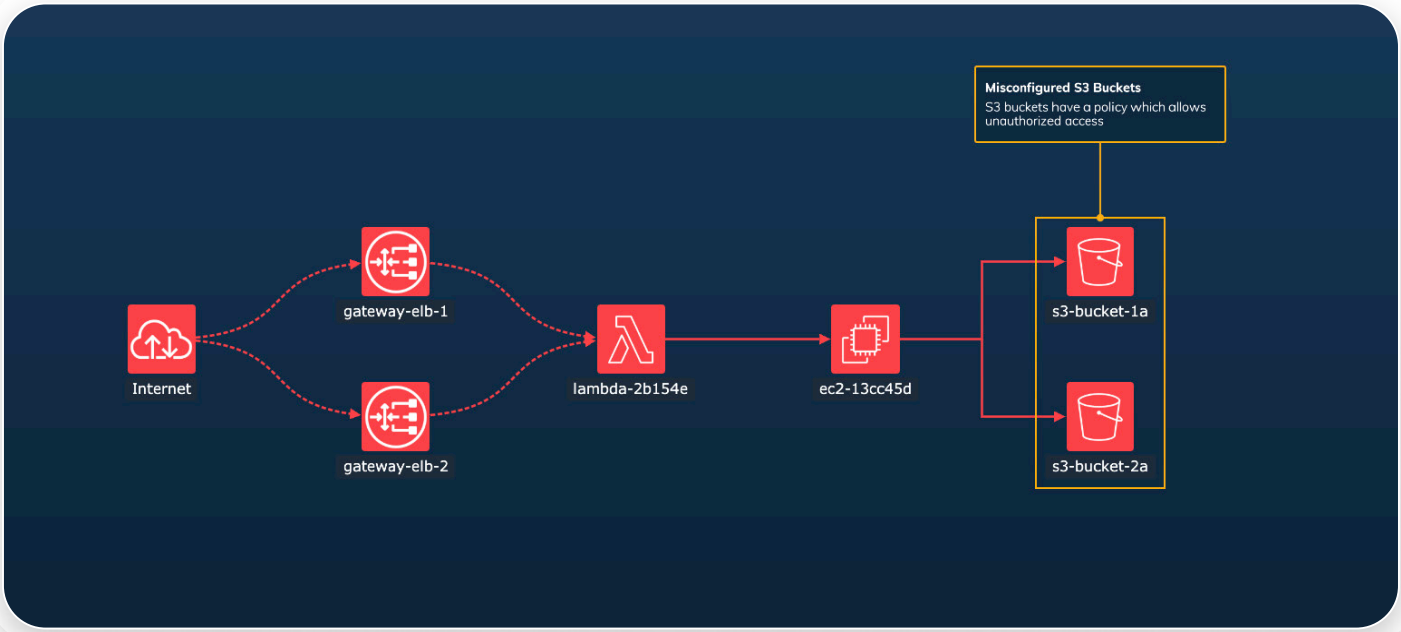
Graph visualization is the natural way to represent cloud infrastructure, because cloud security is fundamentally a connected data problem. Assets exist in hierarchies - regions contain availability zones, which contain VPCs and subnets, which contain services - but the security-relevant relationships cut across that hierarchy in every direction.

A well-designed graph view lets analysts see both dimensions simultaneously: the structural hierarchy of the environment, and the actual or potential traffic flows between services. Grouping assets into combos by region or account keeps large estates readable, while color-coded health indicators surface misconfigurations at a glance - without forcing analysts to dig through raw configuration data.



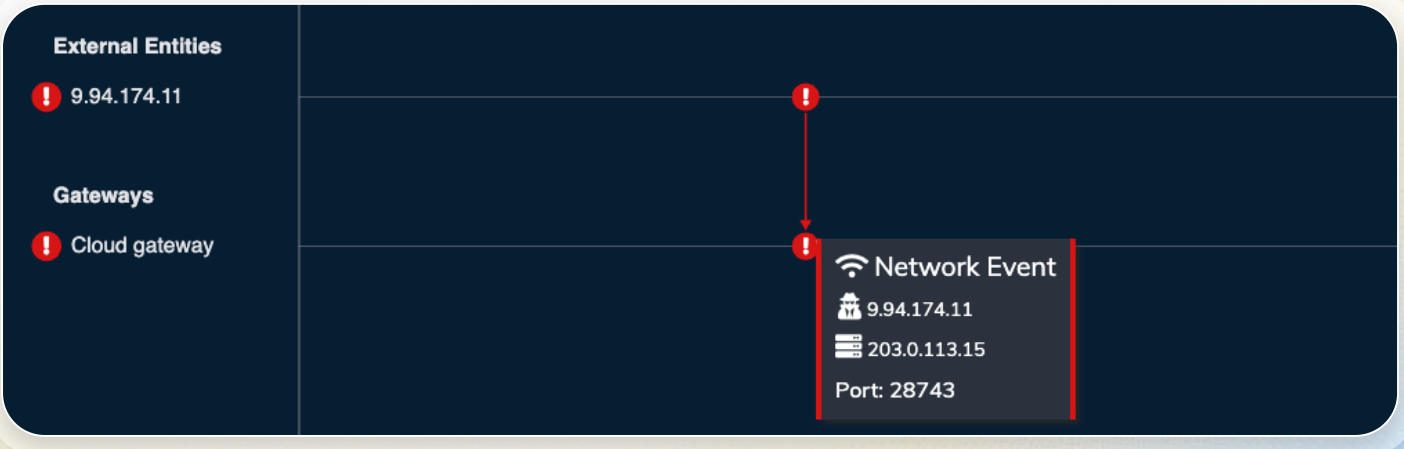
Attack path visualization

Understanding your posture means understanding how an attacker could move through your environment. Graph visualization makes attack paths explicit: when a misconfiguration creates a route from an exposed service to sensitive data, that path can be highlighted dynamically, filtered from the surrounding topology, and laid out sequentially so the risk is immediately legible to any stakeholder – not just the expert who found it.



Timeline visualization for cloud detection and response

Cloud environments generate continuous event streams – from CloudWatch, CloudTrail, and equivalent services in other providers. Timeline visualization gives analysts a structured way to work through that volume: a heatmap view for situational awareness across an entire estate, drilling down to individual event sequences when an alert fires. Paired with graph visualization, it answers both what happened and what was affected in a single investigation workflow.



Identity and access: the new attack surface

As organizations move to cloud and adopt non-human identities - service accounts, API keys, OAuth tokens, and increasingly AI agents - the identity layer has become one of the most exploited attack surfaces in cybersecurity. Attackers don't have to break in if they can log in.

Graph visualization is uniquely well-suited to identity security. Privilege relationships, role assignments and access paths are inherently connected data: who can access what, through which roles, and via which intermediary services.

Visualizing that as a graph makes overprivileged accounts, toxic permission combinations and lateral movement paths immediately visible - rather than buried in policy documents or IAM console exports.

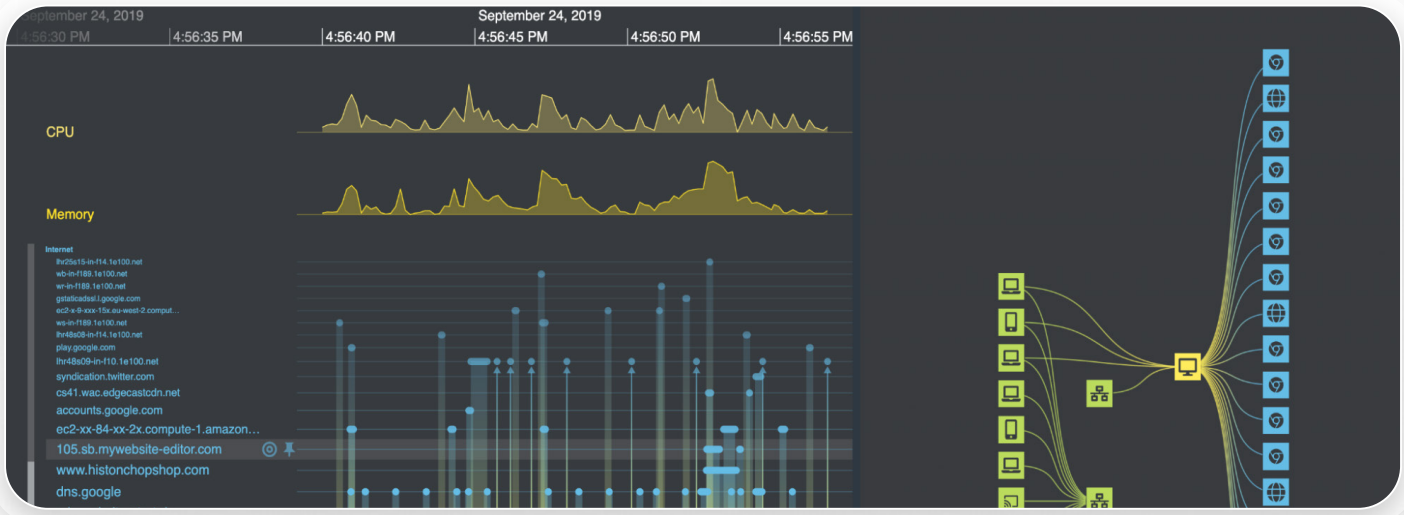
And when an alert fires on unusual privilege escalation, timeline visualization lets analysts see the sequence of events that led to a breach - cutting investigation time significantly.

[Explore our Detection and Response demo]

Visualizing cyber threats as graphs, timelines and maps

Incident forensics and log analysis

When a cyber attack occurs, analysts need to reconstruct exactly what happened: the sequence of events, the systems involved, and how the attacker moved through the network. They're working against the clock, under pressure, with data that is dense, high-velocity and often incomplete.



Most organizations have more log data than they can process, and the biggest challenge is making that data legible fast enough to matter.

Graph and timeline visualization working together solves this in a way that neither can alone. The timeline gives analysts a chronological view of events across every affected entity - devices, users, services - so patterns and sequences emerge naturally rather than having to be inferred from raw logs. The graph view shows the network relationships behind those events: which devices were communicating, which paths were used, and where the attack originated.

When event volumes are high, aggregation keeps the view manageable - dense bursts of activity can be summarized without losing the ability to drill into individual events when something warrants closer attention. Continuous data like CPU and memory load can be overlaid alongside discrete events, giving analysts the full context of what a system was doing at any given moment.

The result is a faster, more confident path from alert to root cause - with a shared visual record that's easier to communicate to stakeholders and use in post-incident reporting.

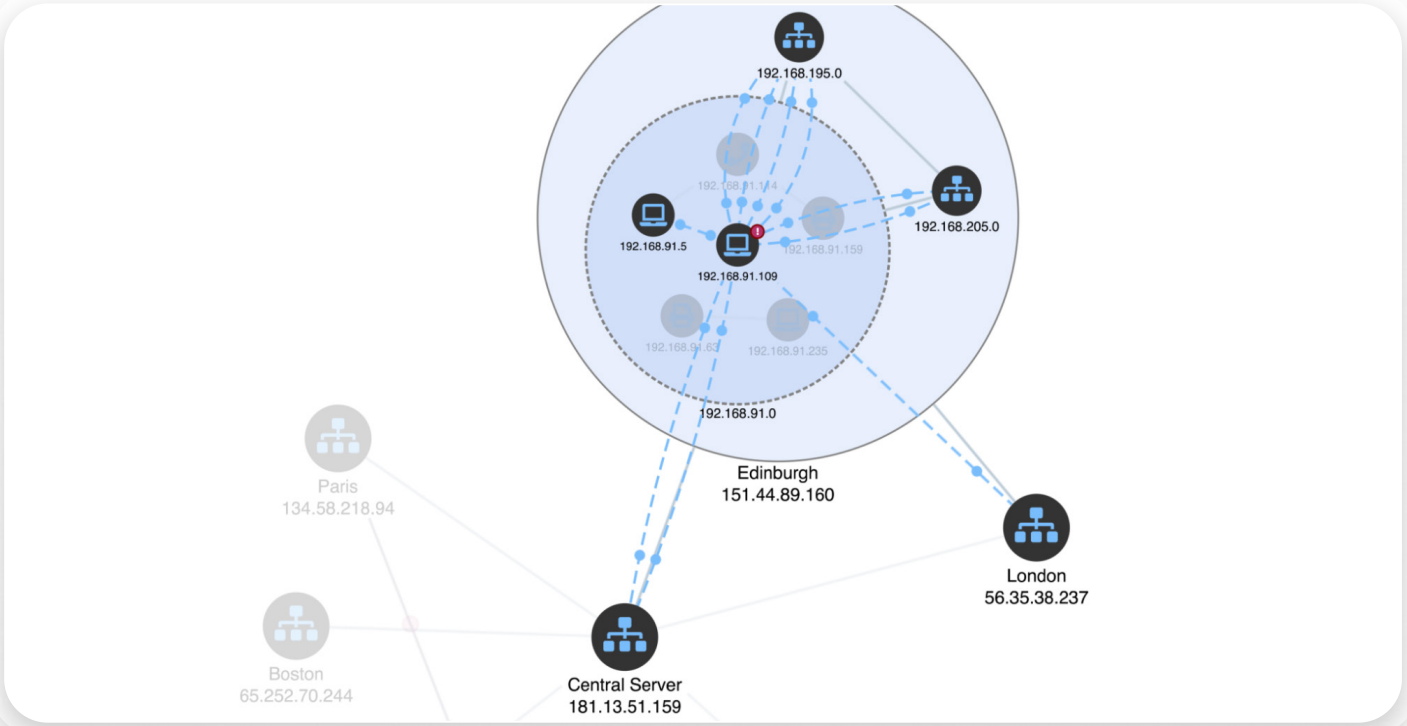
[See it in action in our interactive incident forensics demo]

Network alert management

Modern IT infrastructure - spanning cloud environments, on-premise networks and remote endpoints - generates a constant stream of alerts. The challenge here is in understanding where in a complex, interconnected network the problem originates, and what else might be affected.

Graph visualization brings structure to that complexity. Grouping assets by network segment or region keeps large topologies readable, while alert indicators surface issues at the right level of detail - giving analysts a high-level view of network health and the ability to drill into specific problem areas without losing context. The result is faster triage and fewer blind spots.

[Explore our interactive network alerts demo]

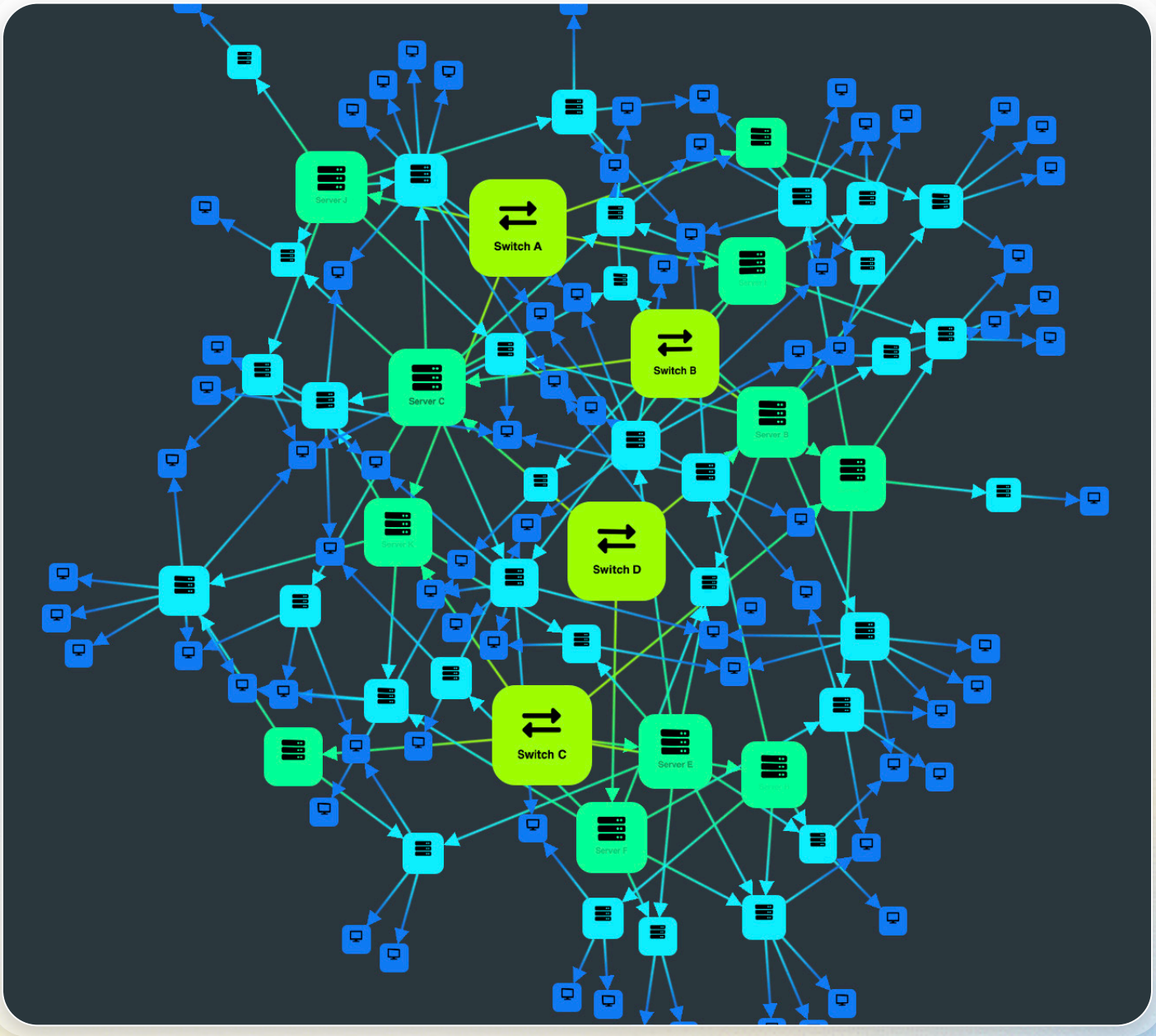


Impact analysis

Detecting a vulnerability is only the first step. Analysts then need to understand its blast radius – which dependent devices, processes, data or services could be affected if that vulnerability were exploited or if a node failed.

Graph visualization makes those dependencies explicit. Automated layouts present complex node hierarchies clearly, so analysts can see at a glance which assets are most critical to network function and which would cause the greatest disruption if compromised. This is particularly valuable in dense, interconnected environments where the knock-on effects of a single failure aren't obvious from configuration data alone.

Advanced graph analysis techniques – including centrality analysis to identify the most influential nodes in a network – give security teams the evidence they need for effective contingency planning and prioritized remediation.



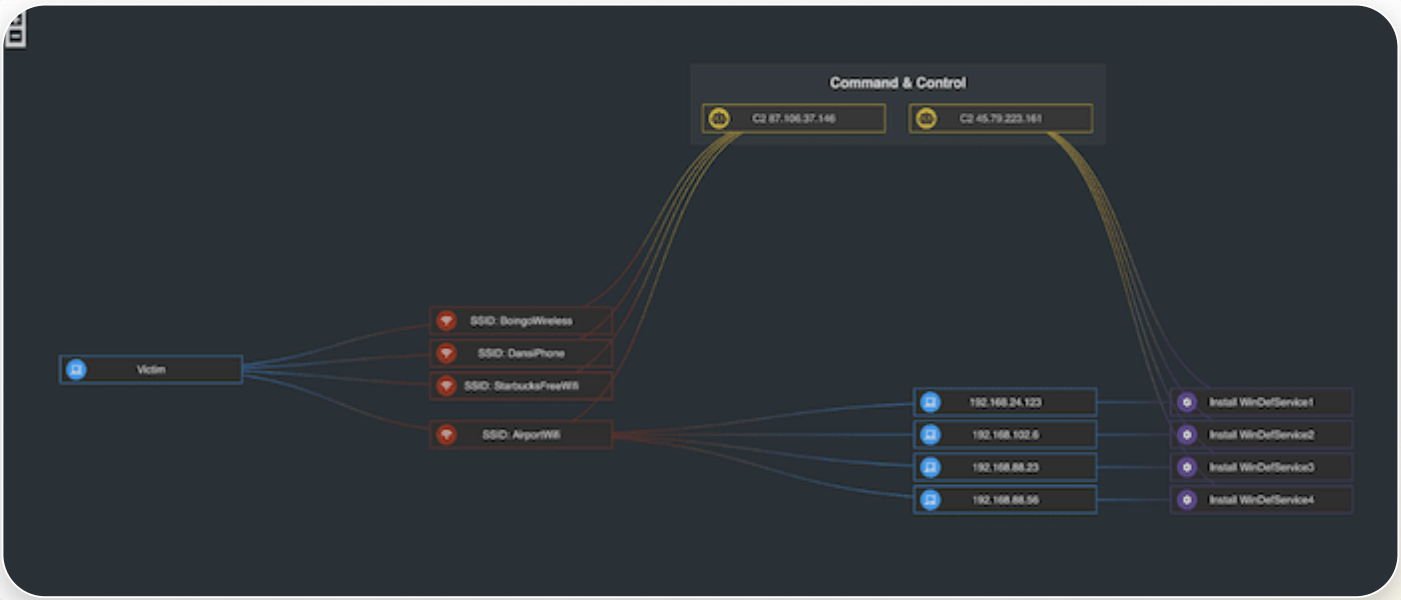
Visualizing the MITRE ATT&CK framework

To stay ahead of sophisticated adversaries, security teams need to understand not just the threats they've already faced, but the broader landscape of tactics and techniques used by cyber criminals. That means working with threat intelligence frameworks - and communicating findings clearly across teams.

The MITRE ATT&CK framework is the industry standard for this. It maps the tactics and techniques used by attackers across every phase of an attack, giving analysts a common language for describing threats and a structured way to assess their own defenses.

Graph visualization makes ATT&CK more useful in practice. Representing the framework as an interactive network - rather than a static matrix - lets analysts explore relationships between tactics, identify which techniques are most relevant to their environment, and map specific threat actors to the techniques they favour. The Emotet trojan is a good example: visualizing how it traverses wi-fi networks using ATT&CK taxonomy breaks a complex, multi-stage threat down into its constituent parts, showing analysts exactly how it fits into the wider threat landscape and where their defenses need to be strongest.

The result is threat intelligence that's faster to interpret, easier to act on, and simpler to communicate to stakeholders who don't live in the data every day.

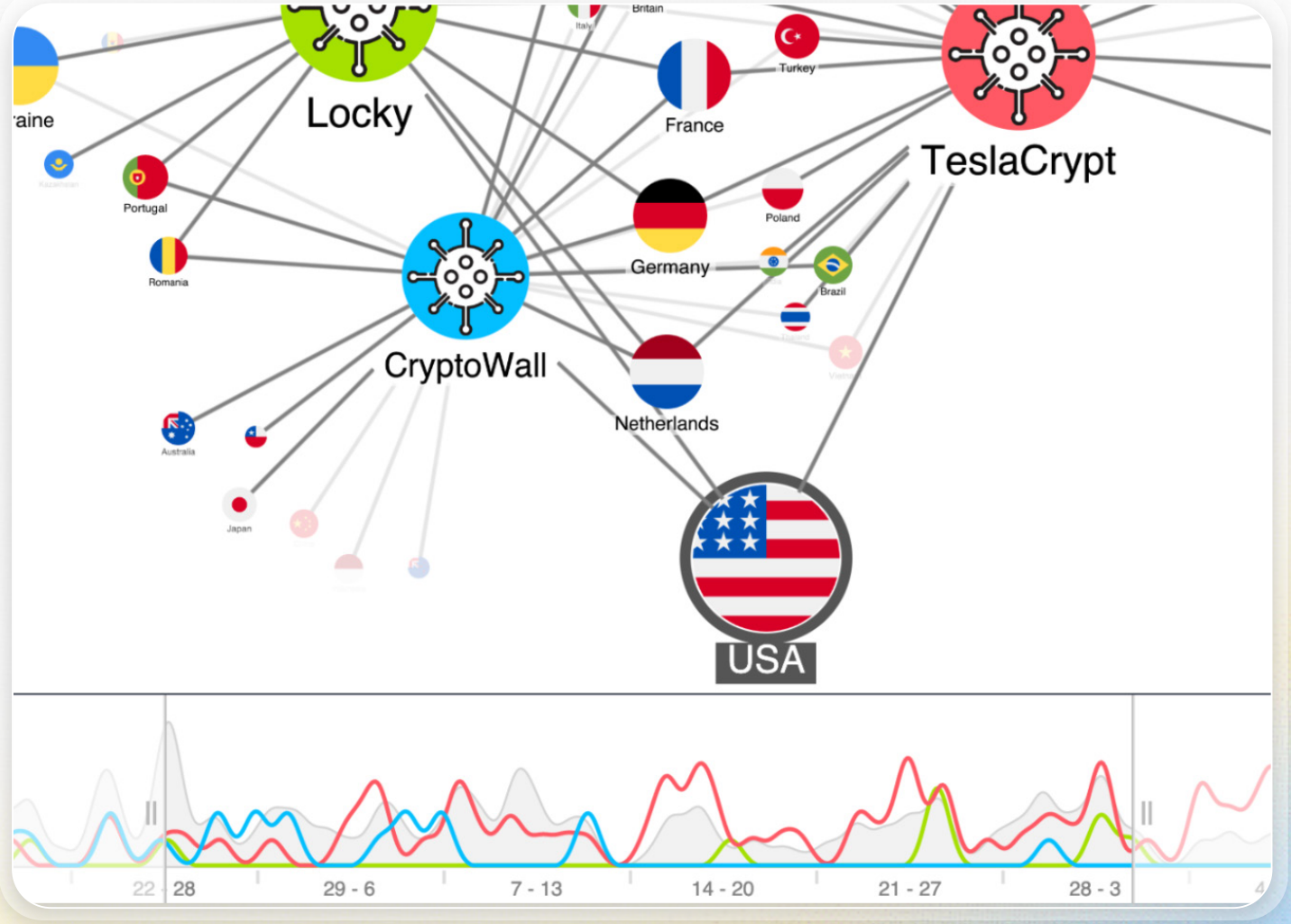


Finding anomalies and patterns

Automated alerts catch known threats. But sophisticated attacks often announce themselves through subtler signals - unusual patterns of behaviour, unexpected connections, activity that falls outside the norm but doesn't trigger a rule. Finding those signals in large, complex datasets requires a different kind of analysis.

Graph visualization excels here. By representing the source and distribution of attacks as a connected network, analysts can move fluidly between a high-level view of the threat landscape and specific clusters of activity - combining nodes by geography, attack type or time period to surface patterns that would be invisible in tabular data. The most connected nodes, the most active sources, the most targeted victims all emerge naturally from the visual structure rather than having to be calculated and reported separately.

Timeline visualization adds the temporal dimension: daily and weekly patterns of network activity reveal who was accessing which systems and when, making it straightforward to spot access outside core hours, correlate suspicious behaviour with known threat events, or identify the moment a compromised credential was first used. Together, graph and timeline visualization give analysts a fast, flexible way to move from a broad anomaly scan to a specific, evidenced finding - without getting lost in the volume.



Geospatial visualization

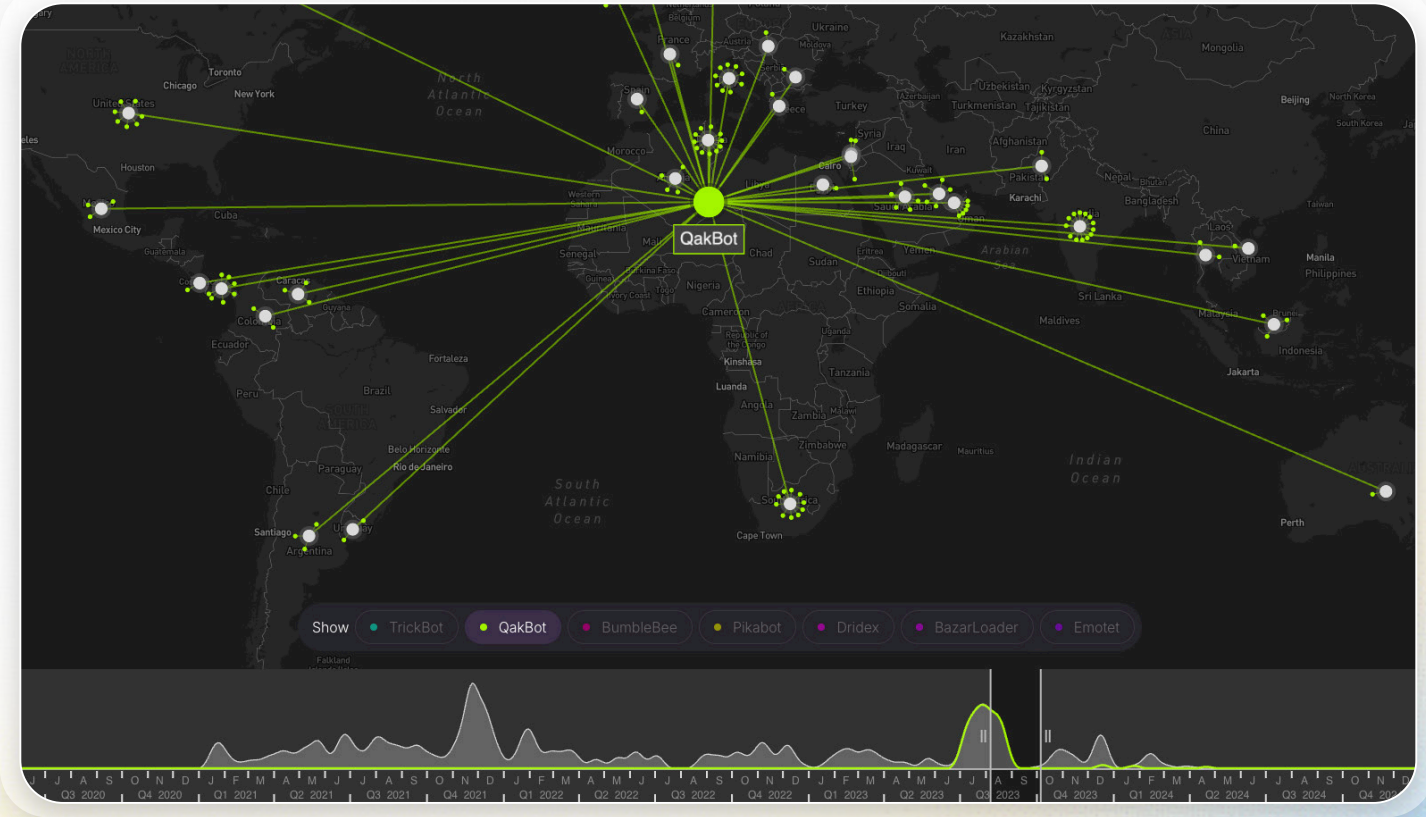
Many of the most significant cyber threats have a geographic dimension that flat network diagrams can't capture. The origin of a DDoS attack, the spread of malware across territories, the geopolitical patterns behind coordinated campaigns - these only become legible when the data is placed in spatial context.

MapWeave, our geospatial visualization SDK, brings that dimension to cyber investigations. By combining network link analysis with map-based visualization, analysts can track how threats propagate across regions in real time - seeing which assets are affected, where they are and how the attack is spreading. Edge bundling and node clustering keep even densely-connected global networks readable, so analysts aren't trading clarity for coverage.

For threats like botnet-driven DDoS attacks - where hundreds of Command & Control servers across multiple countries coordinate simultaneously - geospatial visualization moves the investigation from reactive to spatial: identifying geographic concentrations, spotting unusual traffic patterns across borders, and building a clearer picture of the infrastructure behind the attack.

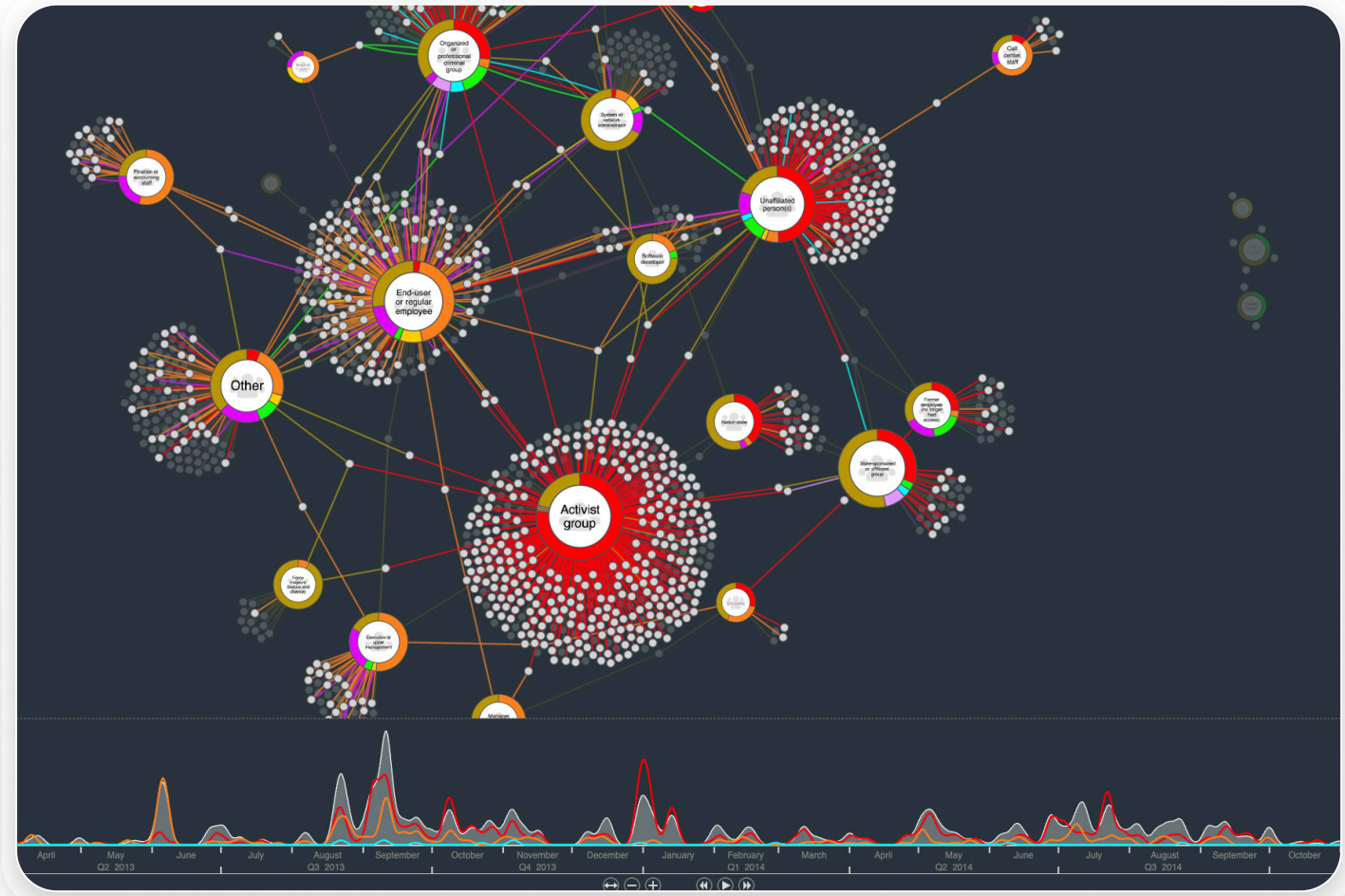
MapWeave works seamlessly alongside KeyLines, ReGraph and KronoGraph, so analysts can move fluidly between a geographic overview and a detailed network or timeline investigation without switching tools.

[See it in action in our interactive DDoS attack demo]



Understanding data breaches

Data breaches rarely have a single cause. They involve multiple actors, multiple attack vectors, and multiple victims - often unfolding over months. Understanding them fully means seeing all of those dimensions together, not in isolation.



Graph visualization is purpose-built for this kind of analysis. By representing attackers, victims and attack vectors as a connected network - with time overlaid via a timeline or time bar - analysts can move fluidly between the high-level pattern and the specific incident. Which attack vectors are most prevalent? Which attacker groups favor which methods? Which victims were most frequently targeted, and why?

This connected view turns breach data from a list of incidents into an intelligence asset — one that reveals structural patterns, informs future defenses, and makes it significantly easier to communicate risk to stakeholders.

[Explore our Data Breaches demo]

Seeing the full picture

Cybersecurity is a data problem that never stands still. The threats are growing in volume and sophistication, the environments analysts must protect are more complex and distributed than ever, and the cost of missing the right signal continues to rise.

Data visualization doesn't solve that challenge, but it changes the odds. When analysts can see their network as a connected graph, trace the chronology of an attack on a timeline, and place threats in geographic context on a map, what would take hours of log-trawling becomes immediately legible. Patterns, anomalies and relationships emerge from the data naturally - and faster.

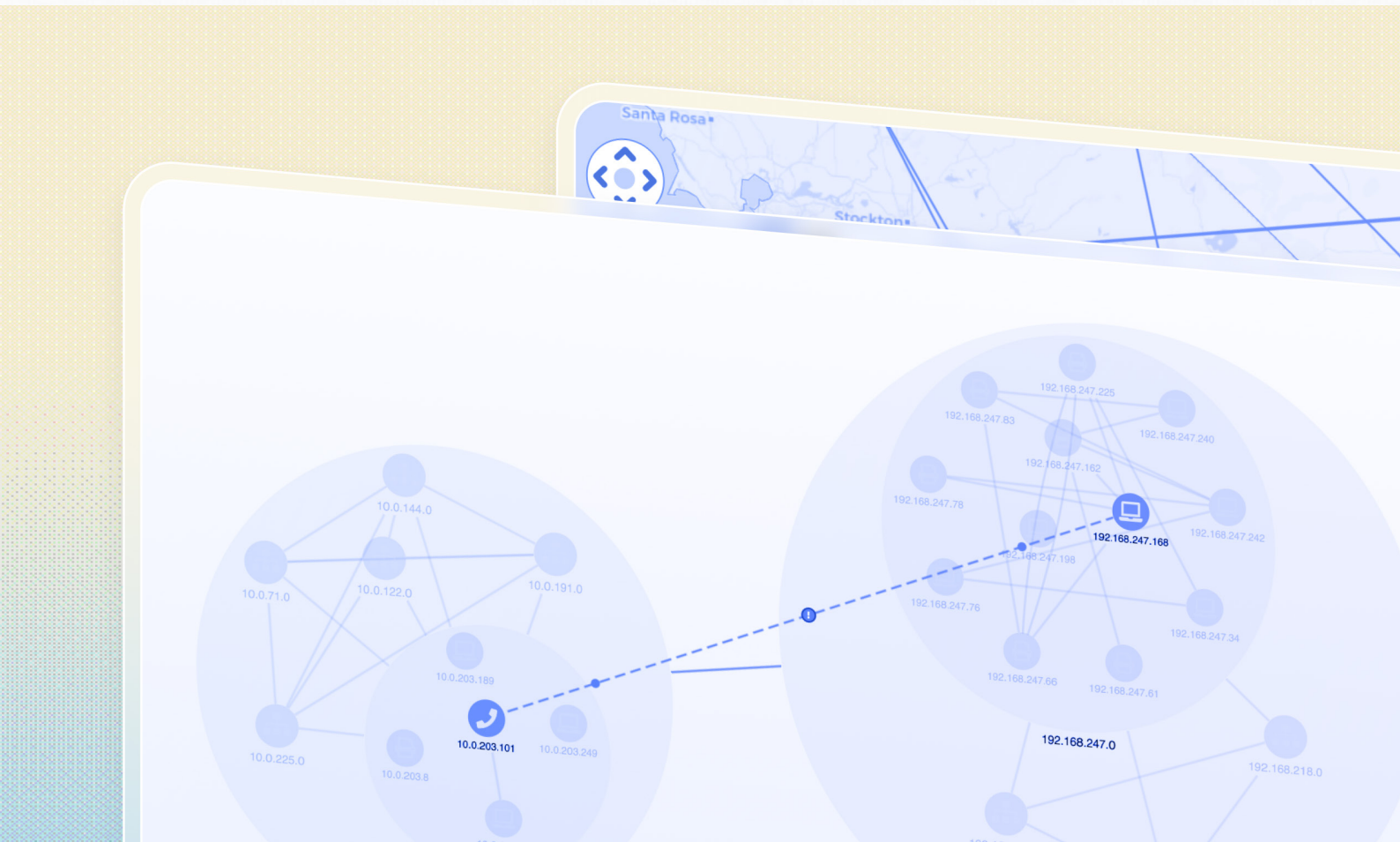
Our graph, timeline and geospatial visualization toolkits are built specifically for this. Together, they give security teams three things:

Clarity: complex, interconnected threat data rendered as intuitive visual structures that analysts can explore without getting lost.

Speed: from alert to root cause, from anomaly to evidenced finding, visualization compresses the time it takes to understand what's happening and act on it.

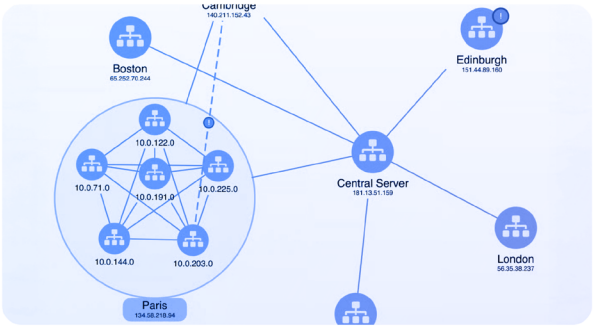
Confidence: a shared visual record that makes it easier to communicate findings, coordinate response, and brief stakeholders who aren't in the data every day.

Whether you're mapping cloud infrastructure, reconstructing an attack's kill chain, or tracking the geographic spread of a botnet, the right visualization makes the difference between data you have and intelligence you can use.



Get started

Sign up to start a trial of our toolkits: cambridge-intelligence.com/try



Graph visualization

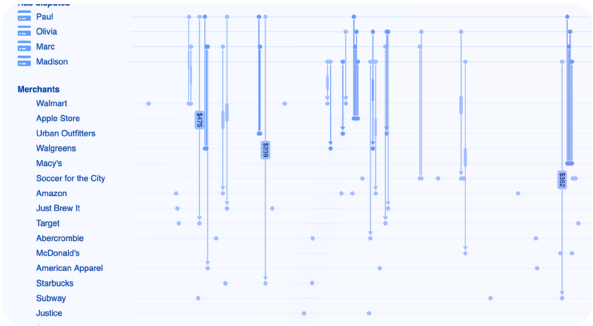
Powered by KeyLines and ReGraph

Reveal patterns, behaviors and connections in complex networks.

Geospatial visualization

Powered by MapWeave

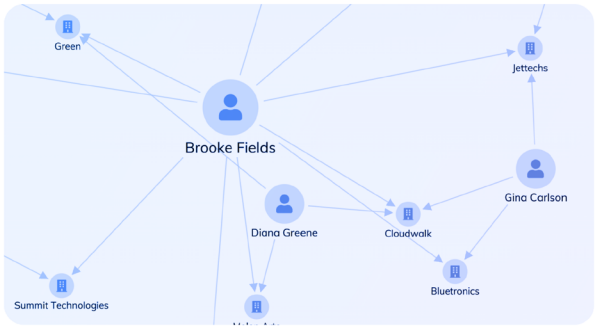
Uncover hidden connections by exploring how people, events and assets move across locations.



Timeline visualization

Powered by KronoGraph

Investigate event data at scale. Explore evolving relationships between unfolding events.



Multi-modal visualization

Powered by All our SDKs

Combine graph, timeline and geospatial views into one coherent analytical experience.

Cambridge Intelligence

Phone (UK): +44 (0)1223 362000
Email: info@cambridge-intelligence.com

Cambridge Intelligence Ltd
6-8 Hills Road, Cambridge, Cambridgeshire CB2 1JP, UK