Buyer's Guide 2023: Network Security, Visibility, and Control

The Measurable Benefits of Atomized Visibility and Control Platforms

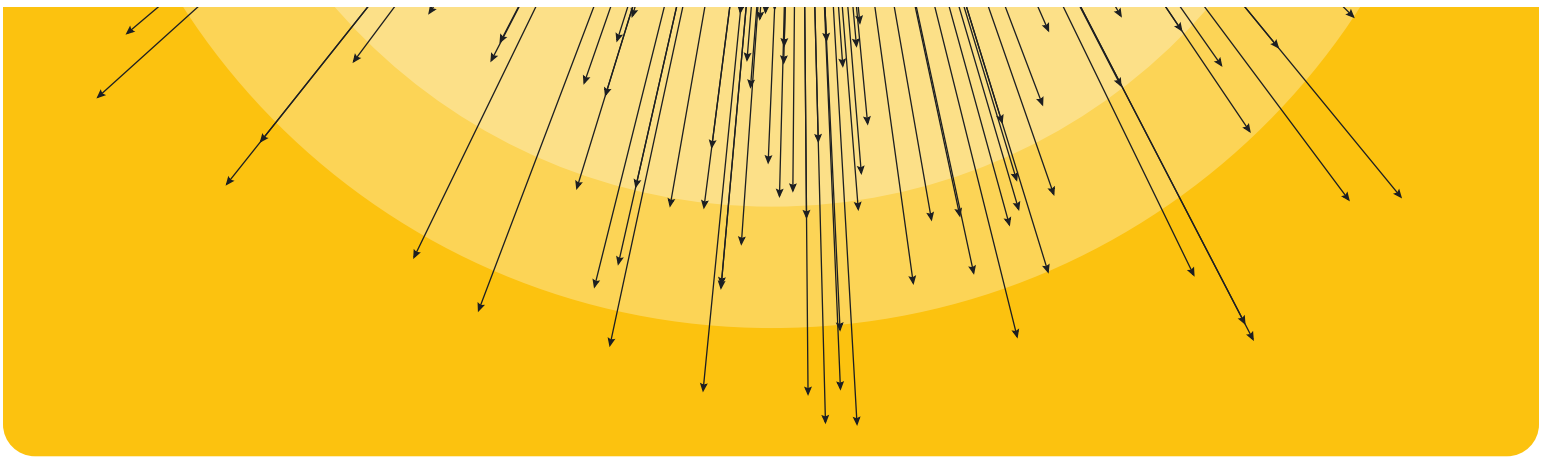


Table of Contents

How to Use This Guide

We live in a multi-cloud world where the Atomized Network is the norm. Enterprise security operations centers (SOC) and cloud operations teams are searching for solutions that can provide scalable, continuous network visibility across the Atomized Network – composites of legacy, on-premises, hybrid, multi-cloud, and edge environments.

If your organization is like many others, you are seeking modern solutions that will address gaps across your newly expanded attack surfaces. Years of "digital transformation" projects, "remote work", hybrid and multi-cloud deployments, and internet of things (IoT) adoption have left organizations with a much larger attack surface and hundreds or thousands of new networks. Modern enterprise networks have become atomized, which means they are Dispersed, Ephemeral, Encrypted, and Diverse (DEED).

There are many vendors and new categories that are causing confusion for buyers. We hear the following often: "Legacy vendors are pushing hardware solutions in the age of the hyperscale cloud," and, "With networks all being encrypted, solutions that are centered on deep packet inspection and decryption just do not make sense or scale to meet today's needs."

This buyer's guide is intended to help you and your organization navigate the market landscape, where we see more than 150 vendors that provide solutions that may meet some of your requirements for network security, visibility, and control. No solution provides all of the capabilities you likely need. And some solutions are too far-forward, which you might consider a "point solution." An example might be a solution that provides "Infrastructure as code posture management for AWS serverless infrastructure." Other solutions you might find in your research are too far behind, like a perimeter-focused next-generation firewall with basic intrusion detection and intrusion prevention capabilities.

The guide is broken into sections that should help you better understand the categories of solutions in the market and the capabilities you should look for in network security, visibility, and control platforms.

- **Section 1** - Brief History of Network Security
  - New security and technology challenges continuously generate new categories and solutions
- **Section 2** - Current Market Overview & Category Descriptions
  - Market landscape of solutions and their benefits and gaps
- **Section 3** - Capability & Feature Lists
  - Simplified list of the core features and considerations for a network security, visibility, and control solution
- **Section 4** - Summary and Recommendations

Market Overview

The cybersecurity technology stack will always be evolving, with new attack types, new assets, better processes, and increased automation. The Atomized Network concept is a great way to conceptualize where we are today—networks are: Dispersed, Ephemeral, Encrypted, and Diverse (DEED). The massive growth of the cloud has the market responding with hundreds of new tools and an array of categories. All of the vendors that have solutions in these categories are vying for attention in the market and your budget.

In the below graphic, we've taken a "network security, visibility, and control" view of the categories that are attempting to modernize the approach in the network security domain. We use a "before, during, after" lens to place the categories along the attack path. Simplified as before an attack happens, during an attack, and after there is a confirmed compromise.

There are new categories like CDR (Cloud Detection and Response) and CNAPP (Cloud Native Application Protection Platform), established categories like EDR (Endpoint Detection and Response), and rapidly growing categories like ASM (Attack Surface Management). While few, if any, organizations have tech stacks that have all of these tools in place today, the vendors in these categories are all actively making big claims and marketing to enterprises.

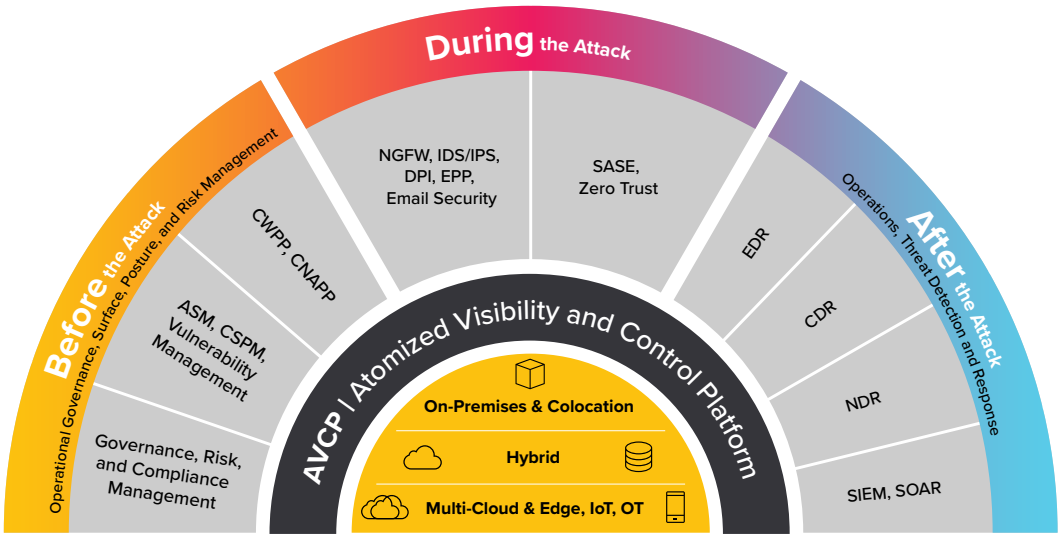


Fig 1. The Ecosystem Categories for Network Security, Visibility, and Control Solutions

From left to right are categories of solutions that provide capabilities for a network security, visibility, and control program that spans before an attack happens, during an attack, and after a compromise. Each of these solutions covers one or more core computing, storage, and network infrastructure and services.

In this buyer's guide, we take a very brief look at the mission of these categories and highlight their benefits and gaps. This is not meant to be exhaustive but to share some important considerations.

Network Security, Visibility, and Control Categories

CSPM

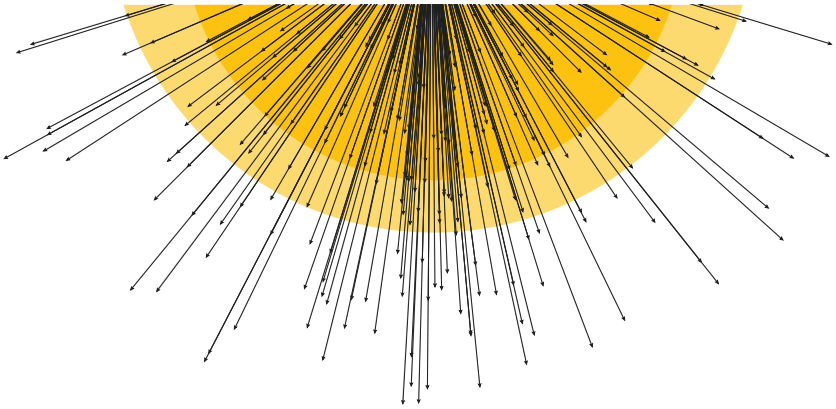
Cloud Security Posture Management (CSPM) is a newer category of solutions that can identify and help remediate cloud misconfigurations. It enables teams to automate some of their cloud security configuration testing and provides compliance assurance in the cloud.

CSPM Benefits:

– Enables a baseline of continuous detection for infrastructure risks, such as excessive access permissions, misconfigurations, exposed APIs, and weak authentication.
– Improves upon the controls that built-in provider tools have while automating various alerts and tasks to enforce policies consistently.
– Helps to keep the focus on optimizing resources based on where there are gaps from legacy systems.
– Helps track changes across clouds for continuous visibility of posture.

CSPM Gaps:

– Not all CSPM platforms are run and ensure the posture is managed in real-time. Attackers can use the time between polling to move swiftly into and laterally across other networks and infrastructure.
– Does not follow or provide support to analysts during an attack. For example, CSPM solutions cannot see lateral movement.
– Does not store traffic flows for forensic / retrospective analysis.
– Does not scale beyond the cloud and requires additional solutions for on-premises, OT, IoT, and hybrid deployments.



ASM

Attack Surface Management (ASM) is a new category of solutions that identifies and manages the risks presented by internet-facing assets and systems. It enables teams to more effectively manage the vulnerabilities of those assets they can detect.

ASM Benefits:

– Provides actionable insights across a wide range of attack surfaces, as many as the platform supports.
– Ensures that asset ownership is easily tracked for the attack surfaces the platform supports.
– Helps identify, prioritize, and evaluate security risks within known assets.

ASM Gaps:

– Discovery of all assets can be challenging for many solutions.
– A high number of false positives are often reported by ASM solutions that do not have the context for custom applications.
– Many teams struggle with the implications of a high number of false positives on risk scoring and tracking remediation.

CWPP

Cloud workload protection platforms (CWPP) are usually agent-based and collect security-relevant data and events and send them to a cloud-based service. CWPP monitors the machines that run the workload and creates alerts about corresponding potential security threats.

CWPP Benefits:

– A “cloud workload first” approach may provide a more complete view of an application’s security posture across single or multiple clouds.
– When configured properly, most CWPP platforms can provide visibility for workload vulnerabilities across single or multiple clouds.

CWPP Gaps:

– Installing and maintaining the necessary agents and virtual appliances slows down deployment, hinders scalability, and may add costs (network, storage, etc.) and impact performance.
– Not all services from all cloud providers are covered by CWPP and may require a mix of solutions. Some users report less than 50% coverage by CWPP platforms.
– CWPP solutions cover only the workload and not the control plane. For gapless insight and protection, CSPM and CNAPP solutions may be required.
– Alert prioritization is hindered by only having visibility into the workload and not the entire cloud environment.

CNAPP

Cloud-native application protection platforms (CNAPP) help secure and protect cloud-native applications. This includes container scanning, CSPM, infrastructure as code scanning, and runtime cloud workloads. CNAPP is a superset of CWPP and CSPM.

CNAPP Benefits:

– Reduced chance of misconfigurations, including access, secrets, and insecure configurations across modern cloud deployments.
– Integration into the CI/CD pipeline, enabling continuous security during new deployments, scaling, and updates.
– Reduced complexity and easier deployments over older, legacy solutions that were not built for the cloud.
– Greater support for scanning proactively than native hyperscale cloud solutions.

CNAPP Gaps:

– Runtime vendors that built CWPP platforms are not all great at integrating seamlessly into the CI/CD platforms and providing value to developers.
– Containers and serverless functions do not require heavy runtime protection.
– The CNAPP market remains fractured, and there is no platform that provides full protection across each cloud and service. We are several years away from mature CNAPP platforms.
– Security testing tools used by the SOC do not integrate with or support runtime protection for workloads; again, the CNAPP platforms are not mature. The teams that purchase and run these platforms are also not always aligned.
– Many of the CNAPP platforms have limited support for Kubernetes.

GRC

Governance, risk management, and compliance (GRC) software enables chief risk officers and CTOs to have a more structured approach to aligning IT infrastructure with business objectives, while at the same time managing risk and meeting regional compliance standards. It assists in supporting an IT risk management process that rolls into an organization's enterprise risk management program and ensures that the activities internally are operated in a way that meets regional laws and regulations.

GRC Benefits:

– Provides a centralized platform for the planning of risk management and compliance management across the organization.
– Better visibility into vulnerability and security controls with easier management of tasks and controls across teams.
– Better reporting for executive leadership.
– Faster audits and reduced risks of compliance issues.

GRC Gaps:

– GRC teams often lack the authority and support from leadership and management teams to fully implement and support the GRC program and the software that drives it. This renders risk and compliance teams and processes ineffective.
– Creating and configuring workflows and assigning cross-departmental ownership and support for the GRC application can be challenging.
– Many manual processes persist for months or years after a GRC deployment.
– Complicated integrations across tech stacks in IT, Security, Cloud, Data Center Operations and Application Development.
– The GRC market is very wide and many organizations need multiple solutions. Common sub-categories and use cases include: corporate governance policies, enterprise risk management, and regulatory and company compliance.

NGFW, NG IDS/IPS

Next-generation firewalls (NGFW) often include next-generation IDS/IPS as the third generation of firewall technology. Other network device filtering functions, such as an application firewall built on in-line deep packet inspection (DPI), are also often included. Some NGFW platforms also include TLS/SSL encrypted traffic inspection, website filtering, QoS/bandwidth management, antivirus inspection, and third-party identity management integration.

NGFW, NG IDS/IPS Benefits:

– NGFWs are good at distinguishing traffic between different applications (from web applications, e.g. Azure hosted inventory systems vs. Salesforce.com) and most of them are faster than earlier generations and can easily be configured to assign different policies depending on the application.
– Easily incorporates information from outside the firewall, such as directory-based policy, blacklists, and white lists.

NGFW, NG IDS/IPS Gaps:

– NGFWs are resource-intensive and becoming more so as encryption across internal networks increases by 5% or more per quarter.
– Configuring and managing NGFWs and IDS/IPS for tens of thousands of devices, services, and endpoints across today's DEED networks can be challenging.
– IDS/IPS are becoming less efficient at the point of attack. There are only milliseconds to detect and prevent an attack with EDR, an IPS, or an NGFW. For example, when a possible remote code execution (RCE) exploit is being transmitted over the network or traversing a device, these platforms have to detect and decide whether or not it will block it in real-time. If it detects and makes the right decision, you're in good shape; otherwise, the attack will be successful.
– Signature-based IDS solutions do not protect against today's modern attack types.

SASE/Zero Trust

A secure access service edge (SASE) provides a wide area network (WAN) and security controls as a cloud computing service directly to the source of the connection (user, endpoint, IoT) rather than a data center. It is often a key part of digital transformation and application modernization initiatives.

Zero Trust security models span all users and devices internally and externally. From devices to data to people, to networks and workloads, Zero Trust implementations require a high level of visibility analytics and automation. The model requires that all devices should not to be trusted by default, even if they are connected to a permissions network such as a corporate network and even if they were previously verified.

SASE/Zero Trust Benefits:

– Continuous monitoring and logging of user activity.
– Easier implementation of segmentation for data and resources, including data security, storage, and transfer.
– Easier implementation of multi-factor authentication and future “passwordless” models.
– Decreased vulnerabilities to insider attacks.

SASE/Zero Trust Gaps:

– Zero Trust and software-as-a-service have accelerated the broad usage of encryption, blinding many of the capabilities of DPI, primarily attack detection and packet analysis capabilities. Workarounds like hardware-assisted decryption can create scalability issues as decryption consumes overhead, increases costs, and hampers performance.
– Zero Trust identity-based access permission models can be bypassed or circumvented.
– Even the most popular Zero Trust networking platforms do not provide the visibility into the traffic-port authentication that most organizations require.
– User and device management becomes far more complex, and the inevitable issue of customers, clients, and third-party vendors that require their own specific policies compounds complexity.
– Remote workers, diversity of devices, and expanded attack surfaces from new cloud applications make implementing and managing Zero Trust very complex.
– Zero Trust implementations often result in an increase in application performance issues.
– Data access, storage, and location management can become very complicated.

NDR

Network detection and response (NDR) solutions are designed to detect cyber threats on corporate networks and provide network visibility and metadata analytics. These tools build models of normal behavior by continuously analyzing network north/south traffic that crosses the enterprise perimeter as well as east/west lateral traffic, and then use these models to identify anomalous or suspicious traffic patterns. Some NDR solutions also incorporate incident response functionality beyond raising alerts. For some, this includes automatically updating firewall rules to block suspicious traffic, quarantining an endpoint, or providing functionality that aids with incident investigation and threat hunting.

NDR Benefits:

– Detects more anomalous network traffic that traditional signature-based solutions like IDS miss.
– Monitors traffic flows across on-premises, hybrid, multi-cloud, IoT, and OT networks if the platform supports it.
– Analyzes network telemetry with store and query or, if the platform supports it, conducts real-time analysis.
– Performs incident investigation from the point of attack to lateral movements across the network, including from on-premises, hybrid, multi-cloud, IoT and OT networks, if the platform supports it.
– Automates responses with the network, EDR, and CDR tools or passes telemetry data to security information and event management (SIEM) and security orchestration and response (SOAR) systems if the platform supports it.

NDR Gaps:

– Most NDR solutions require complex implementations including physical hardware, virtual appliances, agents, traffic mirroring, and flow aggregation tools.
– Most NDRs are point solutions that require additional point solutions to provide visibility across on-premises environments, and some lack capabilities that cover hybrid, multi-cloud, IoT, and OT networks for encrypted or unencrypted traffic.
– Many popular NDR solutions require a second third-party solution to decrypt traffic and manage the privacy implications of decrypted packets.
– Because most NDR implementations do not have complete coverage across all networks, attackers are able to hide in the shadows and have longer dwell time.
– Many NDR solutions have limited threat hunting, forensics, and response capabilities, often leaving those processes to the SIEM and other tools.
– Store and query-based NDR solutions and large implementations of packet decryption have significant compute, storage, and network requirements themselves.

EDR

Endpoint detection and response (EDR), also known as endpoint threat detection and response (ETDR), is a cybersecurity technology that continually monitors an "endpoint" (e.g. mobile phone, laptop, IoT device) to mitigate malicious cyber threats.

EDR Benefits:

– Serves as a last line of defense, providing remote logging and analysis of endpoint behaviors to detect, prioritize, track, and alert on Indicators of Compromise (IOCs).
– Many EDRs are adding capabilities for additional security, like cloud access security brokers (CASB) and data leak prevention (DLP).

EDR Gaps:

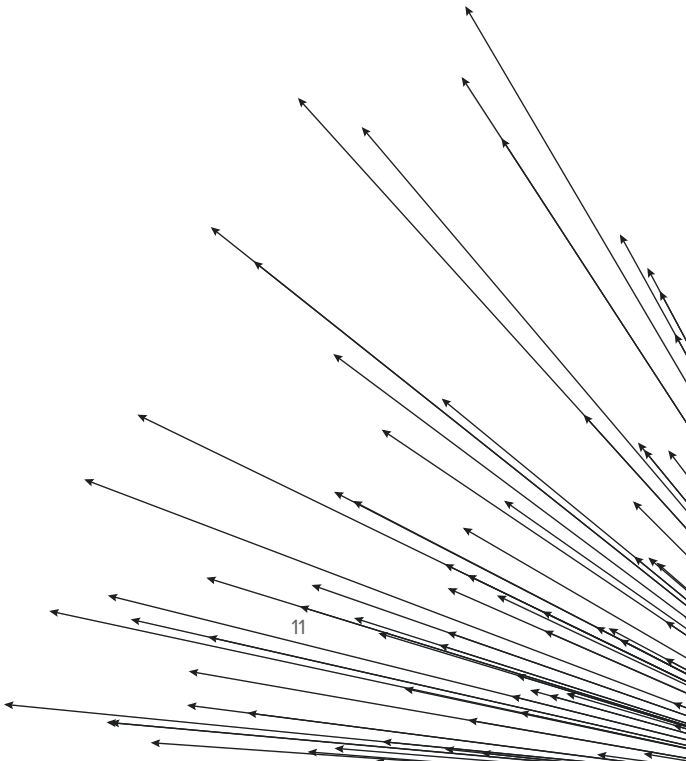
– Agents present issues with updates and performance (CPU/RAM overhead) and can be bypassed by employees and guest users and disabled by attackers.

– Requires constant updates to detection algorithms, signatures, and continuous updates as OSes have their own updates causing conflicts.
– Lack of integration with other endpoint solutions like backup.
– Agentless solutions don't capture local user activity on the remote computer or anything about locally running processes, hardware elements, or other endpoint details of the device itself.
– Encrypted data traffic is difficult to monitor and analyze.
– Unable to gather data about endpoints when those devices are not connected to the corporate network.
– Number of false positives which are triggered due to threat feeds sometimes need to be fine-tuned by the client.
– IoT, operational technology (OT), edge devices, newer hyperscale cloud virtual machines, and other non-standard endpoints are not covered by many EDRs.

CDR

Cloud detection and response (CDR) is a new approach to cloud security that enables security teams to defend cloud applications and infrastructure from account compromise, insider threat, and access misuse, and some even extend into API security. CDR promises to provide consolidated visibility and data-driven analytics to detect, investigate, and mitigate threats in the cloud. This requires that established and new vendors are able to continuously aggregate, normalize and analyze large volumes of data about accounts, privileges, configurations, and activity from SaaS and cloud services to provide insights, situational visibility, and alerts around risks and threats.

CDR Benefits and Gaps: NA. This nascent category has a limited number of providers and adoption, with many organizations adopting and depending on solutions from each of the hyperscale vendors.



Buyer's Guide - Network Security, Visibility, and Control

Capability Considerations:

In this section of the buyer's guide, we take a brief look at many of the key capabilities you will want to consider for the solutions you look for in network security, visibility, and control platforms. This is not meant to be an exhaustive list but is representative of some of the considerations you might find valuable.

Ingestion

There are many ways to capture network traffic and provide a level of visibility required to gain some value and improve network security. Most solutions today require a combination of hardware appliances, virtual appliances, agents, sensors, flow aggregators, traffic mirroring, and other methods. The hyperscale clouds also each have their own unique network traffic visibility mechanisms.

However, as we wrote above, today's networks are dispersed, encrypted, ephemeral and diverse, which is making it more difficult and often impossible for many teams to acquire, ship, install, configure, and manage the infrastructure and software to gain the necessary visibility in the first place.

The Atomized Network makes comprehensive deployment of appliances that provide ingestion impossible. Physical appliances require power, cooling, and spec'ing so they can't move easily to address evolving needs. Coverage is also limited to whatever network's packets can be presented to it, so the ability to monitor traffic using an appliance-based architecture is outstripped as networks disperse into the cloud and ephemeral workload environments.

Zero Trust and software-as-a-service have accelerated the broad usage of encryption, blinding many of the capabilities of DPI, primarily attack detection and packet analysis capabilities. Workarounds like hardware-assisted decryption can create scalability issues as decryption consumes overhead, increases costs, and hampers performance.

Technologies like NGFW, IPS, and NDR are losing potency and becoming at risk of going away because of three evolutionary pressures on DPI technologies delivered on appliances: deployment, encryption, and cost.

The costs of an appliance-based architecture for ingestion are considerable. Physical devices must be shipped to locations when and where capabilities are required. Supporting infrastructure, including packet brokers and decryptors, must be in place. The ongoing lifecycle management of hardware and software, plus configuration and manual updates, limits agility and creates ongoing operational costs.

Here is a list of requirements that you may consider as a way to overcome these ingestion challenges Atomized Networks present.

Requirement	Details
Setup and configure platform without hardware appliances, virtual appliances, agents, or sensors	Leverage NetFlow, sFlow, IPFIX for gapless real-time visibility of all networks
Ingest Network Traffic Flows from On-Premises/Corporate Network	Ingest NetFlow, sFlow, IPFIX from Routers, Switches, Firewalls, Load Balancers – any device that provides flow data
Ingest Network Traffic Flows from On-Premises Virtual Networks	Ingest flow from virtual machines
Ingest Network Traffic Flows from Amazon AWS	Ingest Amazon VPC flow logs and the network interfaces for a VPC including Elastic Load Balancing, Amazon RDS, Amazon Elasticache, Amazon Redshift, Amazon WorkSpaces, NAT Gateways, Transit Gateways, AWS Transit Flow Logs
Ingest Network Traffic Flows from Microsoft Azure	Ingest Microsoft Azure flow logs from Network Security Groups
Ingest Network Traffic Flows from Google Cloud	Ingest GCP VPC flow logs for all network interfaces of the VPC
Ingest Network Traffic Flows from IBM Cloud	Ingest IBM Cloud Flow Logs for VPC
Ingest Network Traffic Flows from Oracle Cloud	Ingest VCN (virtual cloud network) flow logs for OCI (Oracle Cloud Infrastructure
Setup and configure platform without hardware appliances, virtual appliances, agents, or sensors	Leverage NetFlow, sFlow, IPFIX for gapless real-time visibility of all networks

Netography Fusion: Within minutes and without hardware, complicated network taps, and packet inspection agents, your teams can gain visibility from firewalls, routers, switches, load balancers, multiple cloud networks, edge, IoT and OT, and even legacy devices that you've never had visibility to. We can even enable you with visibility where you experience a lack of agent support, encrypted network traffic, or complex global network topographies.

Netography Fusion is device-type and flow-type agnostic and ingests, enriches, and normalizes all flow data in real-time and continuously. Network Security pros are able to see all network traffic and get insights into North-South, East-West, On-Premises to Cloud, and Cloud-to-Cloud traffic all in one modern SaaS portal.

Context

The wide use of tags and labels with a taxonomy built on context (by application, location, security or compliance policy, etc.) continues to enable teams to have better, faster analysis, decision-making, and reporting for the hyperscale, multi-cloud world we live in. With context labels, your visibility and traffic have more context and enable use cases like policy-driven network security and visibility and faster onboarding of new analysts and responders to your teams.

Requirement	Details
Add context from configuration management databases (CMDB) or IT management platforms	Support for CMDBs like ServiceNow
Add context from EDR platforms like CrowdStrike Falcon	Import and sync host and device tags from CrowdStrike Falcon or their API
Add context from other sources of context-management systems via CSV template on S3 bucket	Import your tags/labels manually and/or at an interval from a CSV template stored on an S3 bucket

Netography Fusion: With Netography Fusion's powerful tagging and context labeling, your teams can visualize networks by application, location, compliance groups or any other scheme. The UX/UI is designed by network and security pros for pros and has several unique, time-saving data points that enable analysts to "pivot" quickly, saving time and fatigue. Your analysts will quickly be able to answer questions like: "Who is talking to whom? Over what port? Is it being blocked or not? Where is that data going?"

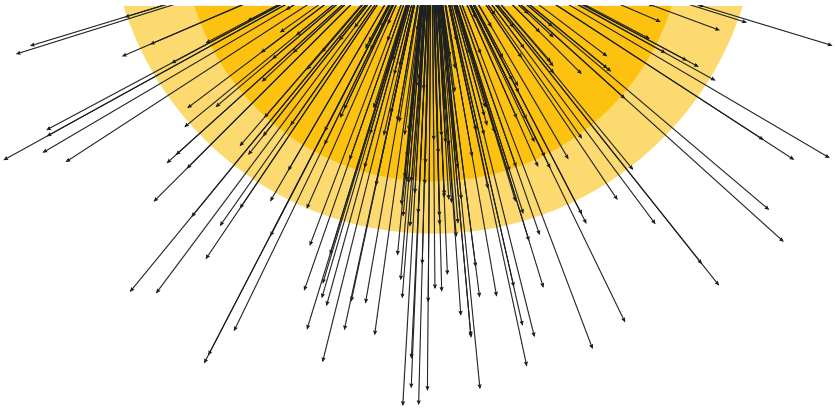
Enrichment

Your team will need network traffic analytics that are enriched with security and business context to provide a complete picture of what's happening so users can pinpoint malicious activity, monitor for compliance, and hunt threats. SOC and cloud operations teams and vendors can use this network traffic data to detect and respond to attacks in real-time. Be sure to consider the integration of the full security stack, which provides the opportunity for an automated, rapid response so that attackers can't leverage their footprint in the network and move laterally.

Requirement	Details
Specify data retention policy and periods	Selectable options for retention: 90/180/365 days
Configurable dashboards	Custom dashboards and UX with optional views (visual aids and lists)
Flexible reporting and exporting	Custom reports and exportable reports as CSV files

Requirement	Details
Enrich network flow data with source autonomous system info	Enriched with routing information for the source network
Enrich network flow data with geographic location	Enriched with location information such as the country, state, city, zip code, latitude/longitude, ISP, area code, and other information
Enrich network flow data with bit rates	Enriched with Bit/s - number of bits that are conveyed or processed per unit of time
Enrich network flow data with packet rate calculations	Enriched with number of packets that are conveyed or processed per unit of time
Enrich network flow data with destination autonomous number	Enriched with routing information for the destination network
Enrich network flow data with DNS lookups	Enriched with DNS Name lookup information
Enrich network flow data with next hop info	Enriched with next-hop information for packets
Enrich network flow data with third-party threat intelligence	Enriched with detections on IP reputation, known malicious IP, third-party services
A UX that provides MITRE Mapping for detected threats	Categorize detection models based on their application to the MITRE ATT&CK techniques
Simple and comprehensive network visualization screens with responsive UX and mouse-over contextual data	Visual maps of hosts and the entities they are talking to, by location, by time, by custom filters

Netography Fusion greatly enriches flow data with context and data points that enable your analysts to see the bigger picture and rapidly analyze suspicious traffic or incidents. Based on Flow type, we automatically add valuable data points such as source autonomous system information, GEO location information, bit rates, packet rates calculations, destination autonomous number, DNS lookups, and next hop information are added to the flow record.



Detection

While endpoint detection and response (EDR) solutions provide coverage for about 60% of all of the devices on most corporate networks, the need to detect intrusions, attacks, malware, ransomware, misconfigurations, and more is needed on all endpoints across your networks. Therefore the importance of network detection has grown as new categories of attacks reveal the consequences of not having gapless protection for all endpoints. Attackers know they have plenty of places to hide as networks, and entire enterprise networks become atomized. Your approach to securing the modern enterprise network must adapt.

Requirement	Details
Support for wide search capabilities	Look for the ability to search enriched network flow records and the ability to create and save custom searches. Analysts, threat hunters, and incident responders need a powerful, flexible, and standard query language, so they can rapidly analyze, investigate, and respond to suspicious traffic or incidents, and also create automated alerts and remediation.
Visibility of lateral movement	Visibility and detection of east-west traffic, and tracking of a lateral move across the network
Detection for scans	Ability to detect fast and slow scanning
Detection for command and control	Detections for connections to known C&C peers
Detection for botnets	Ability to detect many different types of participation in botnet networks from infected hosts
Detection for malware	Ability to detect many different types of malware by modeling traffic from infected hosts
Detection for phishing	Ability to detect traffic sent from or to known phishing sources
Detection for SPAM	Ability to detect traffic sent from or to known Spam sources
Detection for DDoS	Complete detection of DDoS attacks against hosts and networks
Detection for P2P	Ability to detect common P2P services, encrypted or unencrypted
Detection for data exfiltration	Ability to detect large data movement from specific labeled devices

Requirement	Details
Detection for Operational Governance controls, example Social Media usage	Ability to detect and verify, manage and report on compliance with organizational social media policies
Transparent Detections	Detection models should be transparent - black-box decisions are not valuable to analysts and threat hunters
Custom Detections	Ability to create custom detections for your specific deployments and attacks that target your vertical or industry
Alert, or Alert & Remediate on Detection	Set detections to alert (via the integrations below) or auto-remediate with network control and orchestration

Netography Fusion: Detect threats and network issues with the included Netography Detection Models (NDM) or the custom detection models your teams create. Netography's Threat Research Team has created dozens of NDMs to detect botnets, malware, P2P, data exfiltration, ransomware, phishing, SPAM, and DDoS activity. These comprehensive threat and network configuration models are included at no additional charge and are continuously refined, with new NDMs being added frequently as threats evolve. All models are completely open, customizable, and transparent to your analysts.

Alerting

The cornerstone of a successful network security program includes fine-tuned alerting, including human-readable warnings about a possible breach or compromise of a network, a file, a system, an application, a server, or any component that needs the attention and, sometimes, the action of a security analyst. Look for solutions with a low-false positive rate and the ability to fine-tune the alerts, enrich them with valuable information, and send alerts to the SIEM or SOC management platform.

Requirement	Details
Support for a "Chat Ops" implementation via Slack or Microsoft Teams	Ability to send alert/event notifications to Slack or Microsoft Teams
Support for Twilio for a custom alerting implementation	Ability to send alert/event notifications to Twilio
Support for Webhook	Ability to send alert/event notifications to any system that connects via a Webhook

Requirement	Details
Alerts should include enriched flow data	Alerts can be configured to contain enriched data enabling analysts to respond faster and perform fewer pivots or gathering of additional decision support data
Splunk, IBM QRadar, or other SIEM Integration	Enriched events are securely sent to customer Splunk or IBM QRadar
Ability to send alerts via email	Ability to send alert/event notifications to your email recipients, including cc/BCC

Netography Fusion includes customizable and comprehensive support for alerting platforms like PagerDuty, Slack, Teams, Twilio and SIEMs like Splunk and IBM QRadar and more via Webhook functionality.

Response

Responding to a lower number of false positives is key to responding quickly when a real incident is alerted. Analysts and incident responders need accurate intelligence, access, and training to follow playbooks and remediation advice, including performing actions like shutting down or isolating networks and endpoints, terminating harmful processes (or preventing them from executing), deleting files, and more. The goal is to respond to the extent necessary while having as small an impact on business continuity as possible. Many responses can be automated through fine-tuned orchestration models. However, it's important to be able to fine-tune the resolution of network and endpoint responses.

Requirement	Details
Automated or manual network response option: RTBH	Enforce network policy and remediate via RTBH
Automated or manual network response option: Blocklist Manager	Specify a custom blocklist and IP or IP/CIDR addresses in the Whitelist field
Automated or manual network response option: Flowspec	Block IPs at the network level
Automated or manual endpoint response option: CrowdStrike or other EDR	Quarantine host (with limit configuration) including an expiration timeframe
Automated or manual network response option: NS1 DNS or Amazon Route 53 or other DNS provider	Enforcement or remediation of network issues with NS1 DNS or AWS Route 53 DNS orchestration

Netography Fusion's platform enables easy to implement and run incident response and/or remediation with its write once, continuously run everywhere capability or from within your SIEM or SOAR. Remediation is supported by BGP, RTBH, Blocklist Manager, Flowspec, CloudStrike Falcon, API, and DNS orchestration.

Foundational

The final category of requirements to consider for a network security solution is foundational. From securing the solution to securing the transmission of network traffic analytics to supporting additional solutions in your tech stack, many of the core decisions you'll need to consider are outside of network visibility and detections.

Requirement	Details
Ability to secure network data to a central database or cloud	Ability to enable secure transfer of network data
Customization and integration support via APIs	Ability to more deeply integrate and customize your implementation via RESTful APIs including: Forensics – Search for data (alerts/blocks/flows) Analytics – Query statistical and analytical data (alerts/blocks/flows) Configuration – Control service configurations (devices/VPCs/labels/tags) Ability to leverage a living API for testing
Automation support via Infrastructure as Code (IaC) platform	Support for HashiCorp Terraform or similar IaC platform for organizations that are automating infrastructure scale up/down/out and require full support for network security and visibility for ephemeral infrastructure at scale
High-quality, and organized documentation	Access to an easy to use, organized support portal with searchable tutorials on implementing, configuring and using the solution and the integrations Documentation should include API documentation that provides descriptions for every API object, along with descriptions for every JSON property, including value types and ranges. Each endpoint also has code samples in shell, Javascript, Python, Java, Ruby, Golang, or others The Living API provides a working API where one can construct and execute API requests to the API services

Requirement	Details
Engaged and well-trained customer experience professionals	Ideally, you'll be able to speak to the CX team during the purchase process and learn about their process. Look for a program that is tailored to each customer and is use-case driven. A great CX program is staffed by industry experts and has a comprehensive methodology that spans the POV to onboarding, adoption, training, maturing, and a partnership that includes capturing feedback on services and features
Ability to scale	You'll want to deeply understand how you will scale your implementation for your on-premises, hybrid, multi-cloud, and edge networks. You'll need to ensure that you'll get the resolution and retention you need to meet your network security, visibility, and control requirements

Netography Fusion is designed to be seamlessly integrated into your existing technology stack. The platform was architected with the latest scalable technology stacks and is 100% SaaS-based, enabling it to scale to support the massive dispersed, ephemeral, encrypted, and diverse networks of today's enterprise. The platform was built on the same APIs that our customers can leverage. Our customer experience team and Netography Advisory Services philosophy centers around providing enduring value, actionable insights, and deliverables and services that empower and enrich your security program and team members. Our staff of industry experts and program managers ensure that we will meet and exceed your expectations.

Summary and Recommendations

We believe the "Atomized Network" is not just the new normal – it's the driving force for organizations like yours that are seeking a modern platform for network security, visibility, and control.

Legacy solutions and teams that work in isolation using tools built for how the network used to be, no longer provide the ability to protect and defend the Atomized Network.

The Atomized Network is...

– **Dispersed**: We need a solution we can deploy across the entire Atomized Network with threat detection models we write once to protect everywhere, instead of a dispersed set of tools with different logic for detection, operated by siloed network, security, and cloud operations teams.

– **Ephemeral**: We need a solution that can be deployed on demand in seconds or minutes, instead of appliance-based models that take weeks or even months to deploy.
– **Encrypted**: We need a solution that is encryption agnostic, providing an equal set of capabilities to users regardless of the presence of encryption on a network.
– **Diverse**: We must be able to defend the network as one composite system instead of relying on a panoply of diverse cloud and on-premises solutions that are separate and distinct.

New categories and evolving vendors

Many legacy cybersecurity vendors are bringing their legacy approaches to new categories like CWPP, NDR, and CDR. They are proving challenging to implement (appliances, agents, compute, storage, etc.) and impossible to achieve a gapless level of visibility and control. At the same time, new vendors and solutions are addressing single-use cases, or they are focused on one cloud and not another cloud. Meanwhile, SOC, cloud operations, and IT teams are being challenged to scale up and down, support digital transformation and deployments across multiple clouds, and deal with new security challenges with APIs, software supply chain security, and the continuing onslaught of ransomware attacks.

Have a look at the below image, it's the same image from before, with additional notes about the gaps that many teams are experiencing with the different categories. In some cases, solutions like CDR seem already eclipsed by the expanding security capabilities of the hyperscale cloud providers and solutions like Netography Fusion.

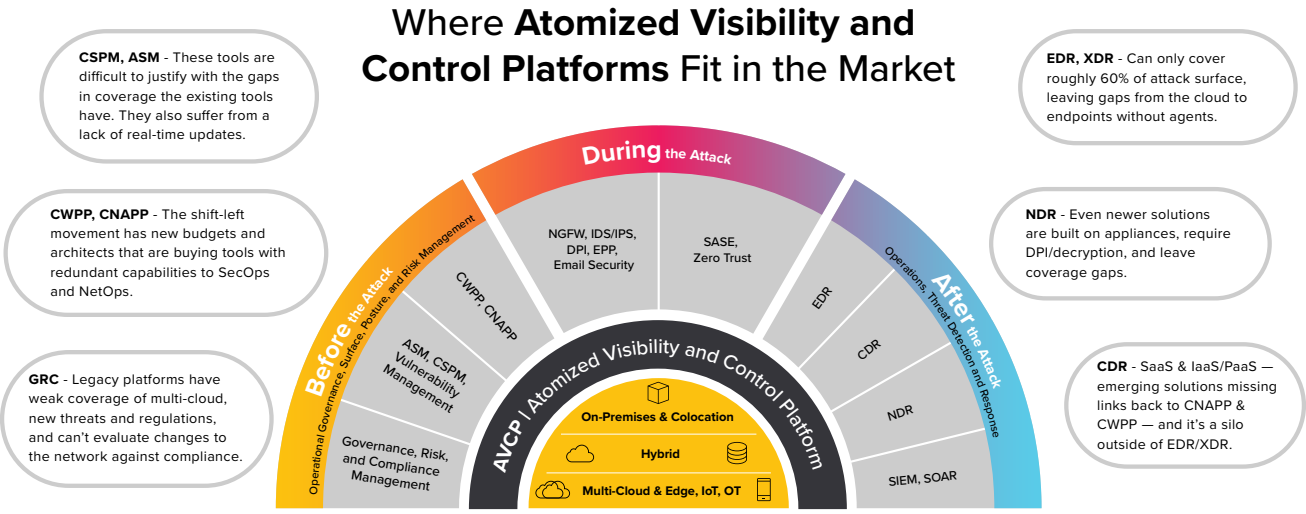


Fig. 2 Overview of Gaps in Today's Network Security Visibility, and Control Solutions

The case for Netography Fusion

We invented Netography Fusion, which we refer to as an Atomized Visibility & Control Platform (AVCP), a cloud-scale, network-centric platform, specifically architected to deliver unified capabilities regardless of the nature and location of what is being defended. At its core, Netography Fusion generates a real-time network event stream with anomaly detection and compliance analysis.

We've achieved this by reconstituting the network security capabilities disrupted by dispersion and encryption with an approach that lives off the land, relying on network flows, metadata, and enterprise context—not packets—to provide complete network visibility, and control. Our SaaS-based universal platform deploys frictionlessly to deliver capabilities immediately when and where they're needed across the Atomized Network. A single portal provides a unified view of all data across the entire ecosystem, enriched with security and business context to provide a complete picture of what's happening so users can pinpoint malicious activity, monitor for compliance, and hunt threats. SOC and cloud operations teams can detect and respond to attacks in real time as they emerge with interoperability across the security stack, which provides the opportunity for rapid response so that attackers can't leverage their footprint in the network.

The industry continues to raise the bar for attackers with aggressive measures to make networks more difficult to hack. Yet history shows us time and again that controls can be abused, vulnerabilities in software can be exploited, and user error invariably happens. Network security will always be important to limit the "blast zone" of a compromise, reduce attacker dwell time, minimize the cost of breaches and downtime, and prevent future intrusions. However, to be effective, it needs to be architected for the Atomized Network.

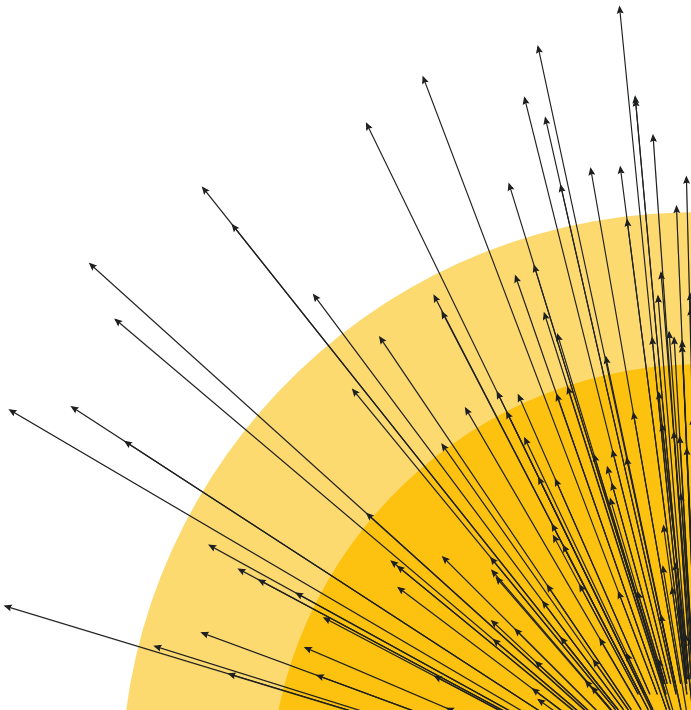
With Netography Fusion, we tell you what you've got, what it's doing, and what's happening to it. We're where you need us when you need us. We are immune to encryption. And we look at your network as a composite of its components, not as a pile of components with separate solutions to figure out what is there. It's the only security product that secures the Atomized Network.

About Netography

Netography® has created the first network-centric platform that reconstitutes capabilities disrupted by the combined impact of encryption and Atomized Networks across the security world. Enterprises have become functionally blind to the composition and activities of their networks, resulting in increased dwell time and more attackers leveraging the gaps between the capabilities of an organization's other tools and the siloed operations teams who operate them.

Netography Fusion® is for enterprise security operations center (SOC) and cloud operations teams that need scalable, continuous network visibility across the Atomized Network – legacy, on-premises, hybrid, multi-cloud, and edge environments. With the Netography Fusion platform, these teams gain visibility and control of network traffic and context across users, applications, data, and devices, to see what they are, what they are doing, and what's happening to them.

Netography is the only company that delivers Security for the Atomized Network®. Based in Annapolis, MD, Netography is backed by some of the world's leading venture firms, including Bessemer Venture Partners, SYN Ventures, a16z, and more. For more information, visit netography.com.



NETOGRAPHY