LiveAction
A BlueCat Company

LiveWire | Solution brief

Security Insights

Security add-on with packet-level analysis at the network edge for fast and actionable security intelligence

Challenge

Many enterprises operate with fragmented visibility between network and security teams. Furthermore, traditional network detection and response (NDR) solutions are complex, costly, and siloed, leaving blind spots that attackers can exploit.

Solution

Security Insights, an add-on to BlueCat LiveWire accessible through BlueCat LiveNX, delivers faster detection, forensic investigation, and proactive threat hunting. It quickly transforms existing network-edge data into actionable, scalable security intelligence without the blind spots of traditional NDR.

Benefits

- Detect anomalies and respond in minutes, not hours
- Maximize ROI by leveraging existing raw flow data and packet captures
- Reduce complexity with unified visibility across network and security operations

Learn more

Transforming network visibility into actionable security intelligence

Cyber adversaries don't confine themselves to one domain—they move laterally across endpoints, servers, networks, cloud environments, and data centers. Yet, most enterprises still operate with fragmented visibility: the network team sees one slice, the security team sees another, and blind spots remain. This is precisely where attackers thrive.

Enterprises rely on security information and event management (SIEM), security orchestration, automation, and response (SOAR), and extended detection and response (XDR) solutions to secure networks. However, traditional network detection and response (NDR) tools that ingest massive volumes of packet data into centralized cloud-based systems for analysis are often too data-transfer-intensive, expensive, and slow.

At the same time, packet and flow data provide a rich source of security insight. Too often, however, organizations limit this data to performance monitoring, leaving its full forensic and detection potential untapped. Harnessing and analyzing packet and flow telemetry directly at the edge of the network closes visibility gaps, accelerates detection, and avoids the overhead of traditional NDR.

This solution brief explores how Security Insights, an add-on to LiveWire—BlueCat's network packet capture and forensics solution—and accessible through LiveNX—BlueCat's network observability platform—provides network and security teams with actionable, scalable security intelligence without blind spots. This brief explains how Security Insights works and offers specific use-case examples of attack detection scenarios. It also highlights key differentiators from legacy NDR solutions and outlines primary benefits.

Solution overview

Security Insights is a modern alternative to NDR. Where traditional tools are costly, complex, and blind to critical traffic, Security Insights delivers real-time detection of anomalies and suspicious behavior with packet-level analysis that extends to the network's edge.

Analyzing LiveNX and LiveWire flow and packet data without unnecessary data movement to the cloud enables security teams to get actionable intelligence faster. Findings integrate seamlessly into SIEM, SOAR, and XDR platforms, resulting in scalable protection, reduced risk, and improved resiliency without the inefficiencies of NDR.

Whether deployed on a single site or across a global enterprise, Security Insights provides a consistent, scalable foundation for hybrid network defense by acting as an intelligence layer between the network and your security operations stack.

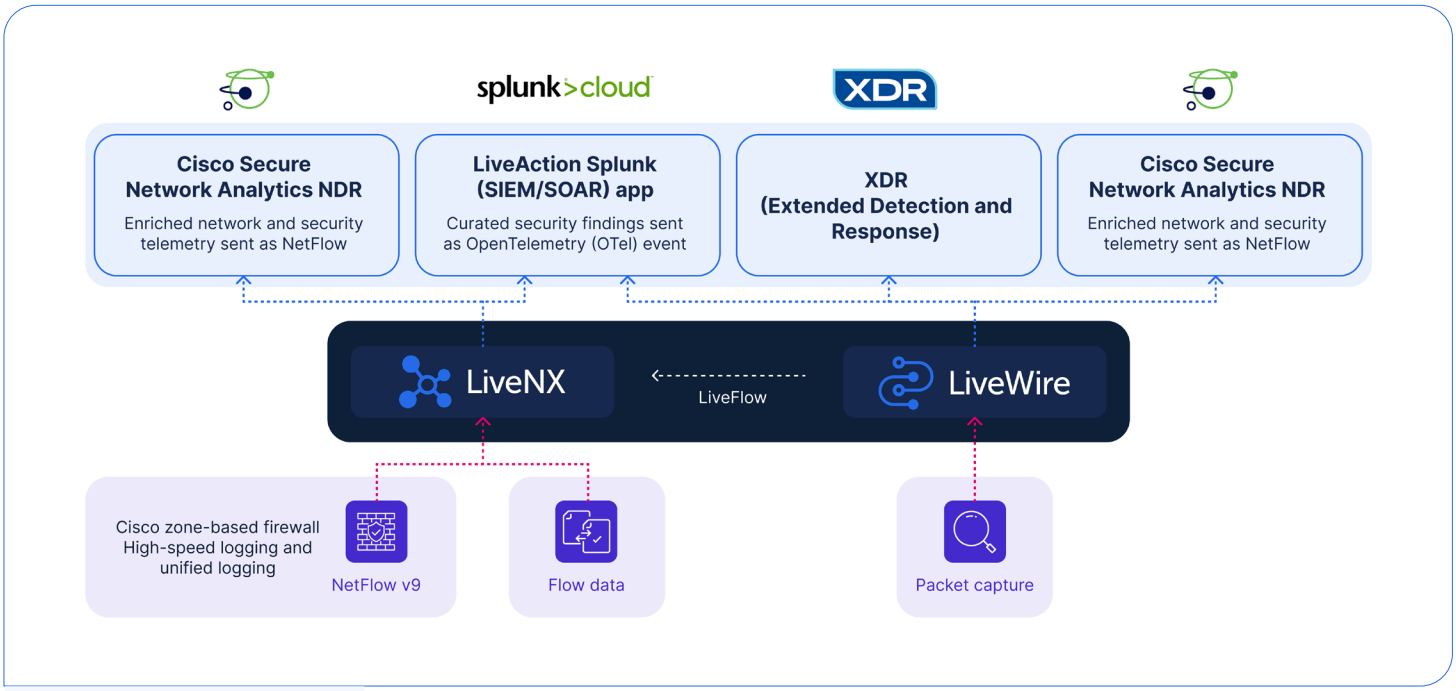

Figure 1. Security Insights architecture

How it works

As a LiveWire add-on accessible through the LiveNX UI, Security Insights operates natively in existing LiveNX and LiveWire environments, transforming network observability into actionable security intelligence. Using the same data that powers performance monitoring, it enables practical network detection without adding tools or complexity. By leveraging flow telemetry from LiveNX and packet-level analysis from LiveWire, Security Insights correlates these findings across all environments—LAN, WAN, SD-WAN, data center, and cloud—giving teams complete visibility into where and how threats emerge.

LiveWire provides deep forensic visibility by performing packet-level capture and analysis at the network edge. It not only captures payloads—including both encrypted and cleartext—but also identifies patterns and reconstructs sessions. This process of capture and analysis is called LiveFlow. These LiveFlow records are then sent to LiveNX, which detects anomalies by aggregating and enriching comprehensive network traffic telemetry. Traffic flow data is collected in LiveNX from NetFlow, IPFIX, sFlow, and Cisco high-speed logging and unified logging.

LiveNX's centralized dashboard then displays these detected threats and traffic anomalies. Security Insights is open and standards-based, allowing for mapping to the Open Worldwide Application Security Project (OWASP) and MITRE ATT&CK frameworks and seamless integration with SIEM, SOAR, and XDR tools for coordinated response. If a detected threat is first seen in a SIEM or another security solution, security and network teams can leverage LiveNX and LiveWire for deeper investigation.

Both LiveWire and LiveNX are required components for Security Insights.

Use cases

This section outlines three real-world detection scenarios that demonstrate the benefits of using Security Insights.

Use case 1: Detecting anomalous Transport Layer Security activity

MITRE ATT&CK ID T1571 – Non-Standard Port

A global logistics company experiences unexpected spikes in encrypted traffic on non-standard ports. Security Insights automatically detects this pattern as "Unexpected Encryption on IANA Reserved Port"—a strong indicator of malicious tunneling activity used to hide command-and-control (C2) communications.

Investigation workflow:

1. Detection (Security Insights)

- Detects encrypted traffic on port 8088, which is not typically used for secure communications.
- Maps detection to MITRE T1571 and flags the event.
- Cross-references with known IANA-reserved ports for validation and automatically alerts the security operations team.

2. Analysis (LiveNX)

- Visualizes affected subnets and identifies systems generating the anomalous traffic.
- Correlates flow records across WAN and SD-WAN links, confirming the pattern is isolated to a single IoT gateway.
- Detects recurring communication intervals—a hallmark of beaconing.

3. Forensics (LiveWire)

- Captures and inspects packets to confirm encrypted payloads.

4. Response

- Security operations team isolates the IoT gateway and blocks all outbound traffic on unauthorized ports.
- Forensic data is exported to the SIEM for post-incident validation and compliance reporting.

Outcome: Early detection prevented malware from establishing C2 persistence, reduced time to detect from hours to minutes, and improved visibility into encrypted traffic without decryption overhead.

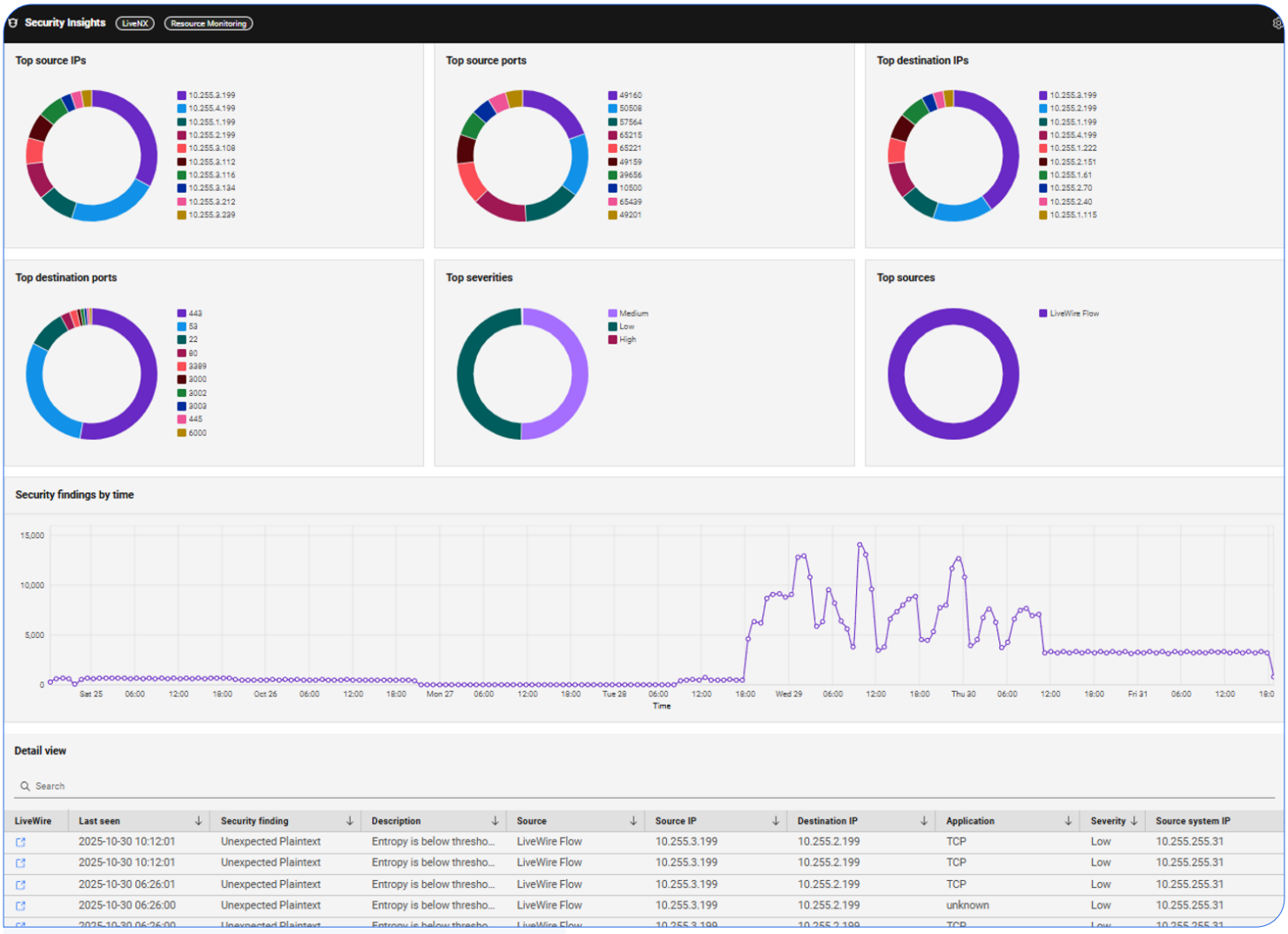

Figure 2. Security Insights summary dashboard and detail view in LiveNX

Use case 2: Proactive threat hunting with threat intel indicators

MITRE ATT&CK ID: T1102 – Web Service

A financial institution's threat intelligence feed reports suspicious domains associated with a recent C2 infrastructure campaign. Using Security Insights, the security team proactively hunts across their hybrid network for any evidence of contact with those domains.

Investigation workflow:

1. Detection (Security Insights)

- Imports threat intelligence indicators of compromise from an external feed and maps them to MITRE T1102.
- Performs a network-wide correlation using flow telemetry to identify outbound communications to suspicious domains.
- Flags multiple endpoints contacting the domain app-sync-storage[.]net, classified as a potential C2 web service.

2. Analysis (LiveNX)

- Analysts pivot into LiveNX to visualize communication frequency and duration by endpoint.
- Correlates DNS queries and flow records to confirm repeated contact from a single subnet within the R&D network.
- Detects unusual data size patterns consistent with exfiltration via HTTPS.

3. Forensics (LiveWire)

- Performs packet capture for the flagged hosts to confirm payload behavior.
- Identifies POST requests containing Base64-encoded data to the suspicious domain.
- Extracts the payload for sandbox analysis to confirm malicious exfiltration.

4. Response

- Sends data to the SOAR to automatically block the compromised domains and associated IP ranges.

Outcome: Stopped stealthy C2 communications before significant business losses occurred.

Use case 3: Forensic investigation of a TLS certificate abuse attack

MITRE ATT&CK ID: T1587.003 – Digital certificates

A large healthcare provider detects irregular SSL certificate behavior across its data centers. Security Insights flags multiple self-signed TLS certificates being used in outbound traffic—a possible sign of malware using forged certificates to bypass inspection controls.

Investigation workflow:

1. Detection (Security Insights)

- Identifies multiple self-signed and untrusted TLS certificates in use on internal outbound connections.
- Maps detection to MITRE T1587.003 and classifies as Unusual Certificate Activity.

2. Analysis (LiveNX)

- Analysts use flow visualization to isolate traffic originating from affected systems.
- Confirms repetitive, short-lived TLS sessions from an IoT medical device subnet to an external IP.
- Detects abnormal TLS handshake intervals and cipher mismatches.

3. Forensics (LiveWire)

- Captures packets for full forensic analysis.
- Confirms that outbound connections contain encrypted commands hidden within TLS payloads.
- Identifies the use of self-signed certificates generated by the malware to establish persistence.

4. Response

- Integrates findings into the SIEM and SOAR for automated certificate revocation and alerting.

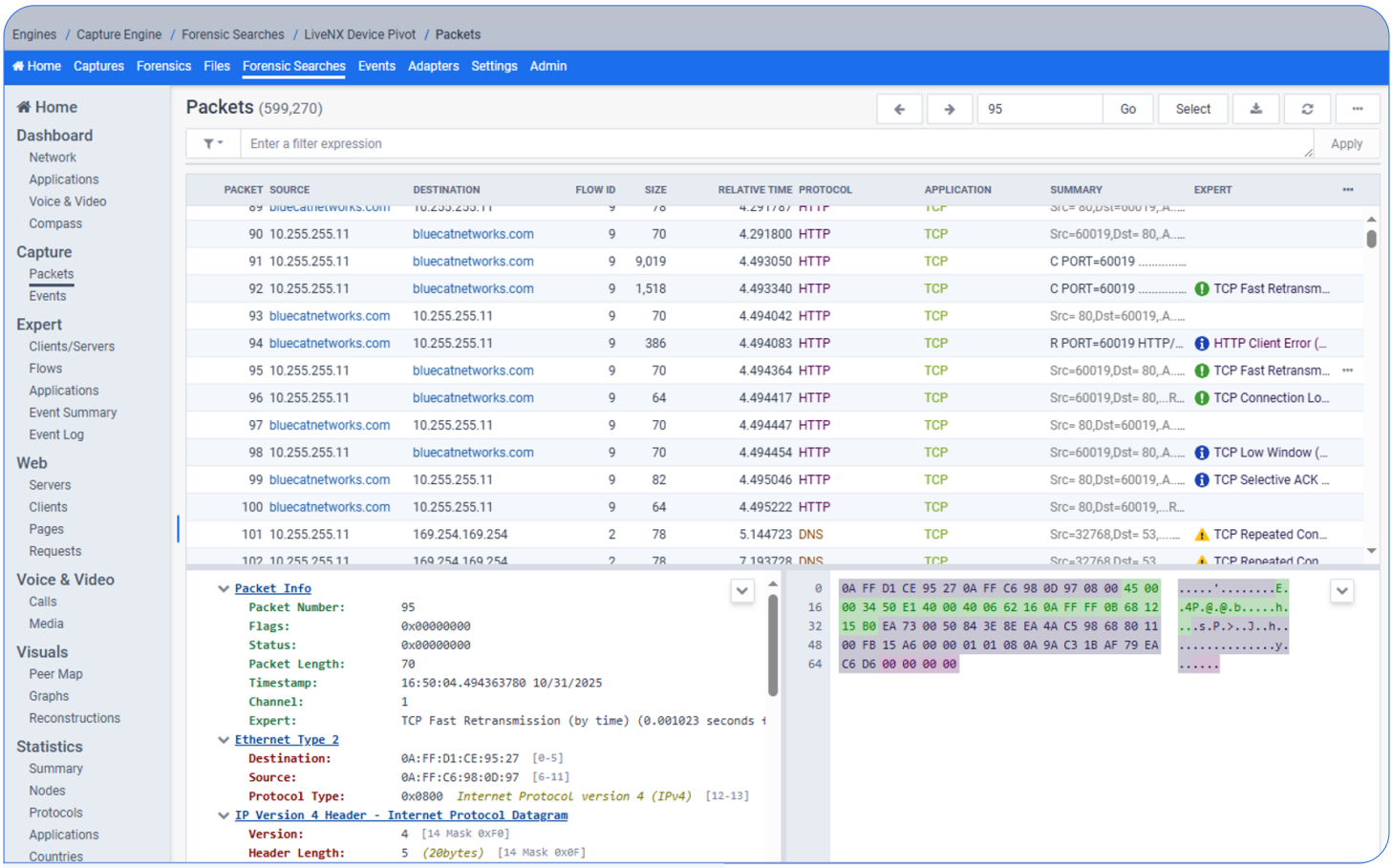

Figure 3. Security Insights individual packet data dashboard used for a forensic search

Outcome: Prevented C2 persistence via forged TLS certificates, enhanced compliance and audit readiness by retaining packet-level evidence, and strengthened certificate governance across the organization.

Key differentiators

Where legacy NDR is centralized, complex, and costly, Security Insights is distributed, efficient, and immediate. It quickly transforms existing LiveNX and LiveWire data into actionable and scalable security intelligence without the blind spots or burdens of traditional NDR.

These four key differentiators set Security Insights apart from NDR solutions:

1. **Unmatched data quality and visibility—without NDR's blind spots**
   Traditional NDR solutions are often constrained by limited data sources or vendor-specific integrations. Security Insights provides unified, high-fidelity visibility across every domain, LAN, WAN, SD-WAN, data center, and cloud, regardless of vendor or architecture. It ingests telemetry from multiple systems and correlates it into a single view. As a result, where NDR tools only see fragments, Security Insights offers end-to-end visibility.

2. **Rich, multi-telemetry ingestion—while NDR depends on partial feeds**
   Traditional NDR solutions often rely on sampled or filtered packet data to reduce ingestion volume, which sacrifices accuracy and context. Security Insights aggregates and enriches comprehensive telemetry, NetFlow, IPFIX, sFlow, and Cisco high-speed logging and unified logging to identify hidden anomalies and patterns across the entire network fabric. This approach gives analysts the complete picture, not just a summary of traffic samples.

3. **Full packet capture and forensic depth—without the cost and delay**
   Most NDR tools move massive packet datasets to a centralized cloud or data lake for analysis, which drives

latency, cost, and compliance concerns. Powered by LiveWire, Security Insights performs forensic-grade packet analysis locally at the network edge. Teams can instantly pivot from flow records to full packet payloads for precise investigations without backhauling data, incurring delays, or the expense of relying on the cloud for analysis.

4. **Edge-first analytics—real-time detection where threats begin**
Traditional NDR architectures analyze data after it's transported and aggregated, introducing delays that attackers exploit. Security Insights shifts this model, generating insights directly at the edge, where many threats originate. By detecting anomalies in real time, it shortens dwell time, reduces operational costs, and ensures sensitive data never leaves controlled environments.

Solution benefits

Security Insights empowers enterprises using LiveNX and LiveWire to modernize threat detection and response with powerful capabilities that simplify operations, accelerate investigations, and strengthen security outcomes across every environment. With Security Insights, network and security teams get these benefits:

- **Faster detection and response**
Cut investigation time from hours to minutes with real-time visibility and actionable insights.
- **Advanced threat hunting**
Leverage raw, unaggregated flow data to uncover hidden threats and accelerate forensics.
- **Unified visibility**
Reduce complexity by bringing network and security data together in a single, correlated view.

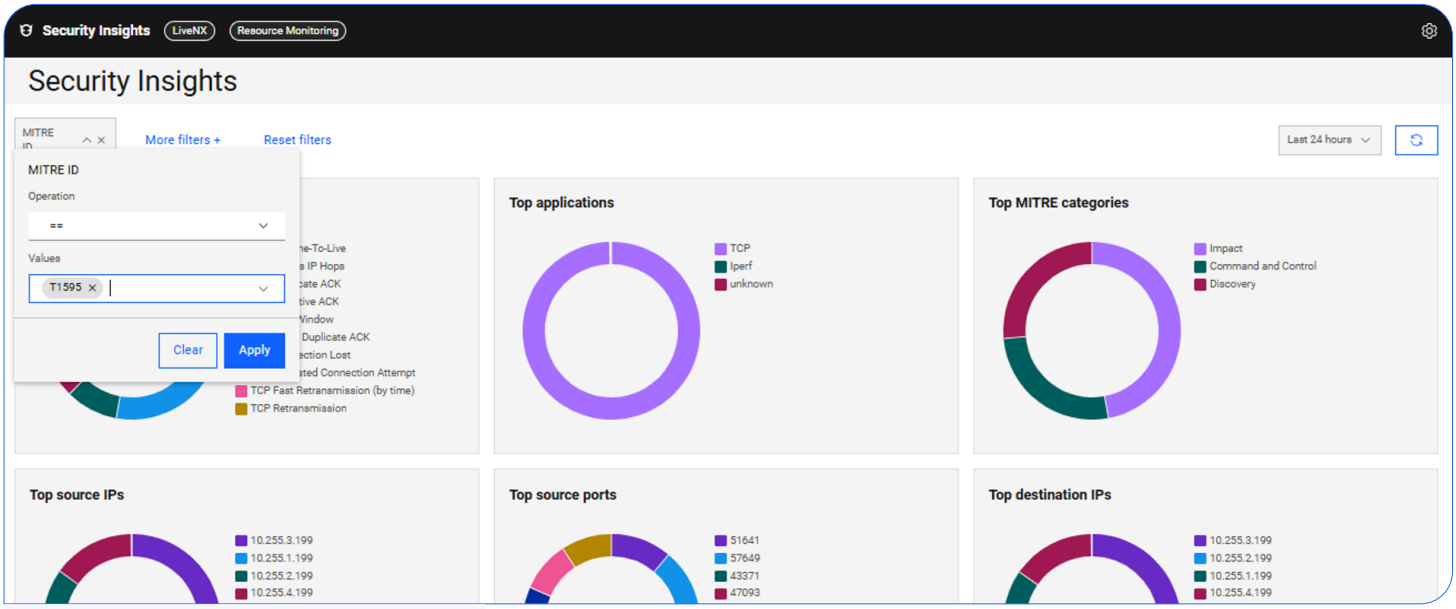

Figure 4. Security Insights filter by MITRE ATT&CK ID

Appendix: Security findings

This appendix provides a list of security findings generated by LiveNX and LiveWire. These findings highlight anomalies, suspicious behaviors, and policy violations detected through flow and packet analysis. While not an exhaustive NDR catalog, they represent high-value insights that accelerate detection, investigation, and response. As LiveNX and LiveWire evolve, this library of findings continues to expand, ensuring network and security teams benefit from richer visibility and stronger outcomes over time.

Security finding	Type	MITRE ATT&CK ID (if applicable)	Component
Anomalous IP hops values	Policy	T1090.003	LiveWire
Cleartext credentials detected	Policy	T1040	LiveWire

Security finding	Type	MITRE ATT&CK ID (if applicable)	Component
Encryption on IANA reserved port	Policy	T1571	LiveWire
Kerberos detected	Policy	T1558	LiveWire
Kerberos RC4 detected	Policy	T1558.003	LiveWire
Malicious IP or domain detected	Indicator of compromise	T1071	LiveWire
Microsoft IP detected	Policy		LiveWire
NTLM protocol detected	Policy	T1557.001	LiveWire
RDP on non-standard port	Policy	T1571	LiveWire
Threat intel indicator	Indicator of compromise	T1102	LiveWire
TLS certificate anomalies detected	Indicator of compromise	TLS	LiveWire
TLS client excessive handshakes	Indicator of compromise	TLS	LiveWire
TLS forbidden version	Policy	T1071.002	LiveWire
TLS long-lived connection	Indicator of compromise	TLS	LiveWire
TLS missing server name indication	Policy	T1587.003	LiveWire
TLS self-signed certificate	Policy	T1587.003	LiveWire
TLS unusual certificate	Policy	T1587.003	LiveWire
Unassigned encryption	Policy		LiveWire
Unauthorized application use	Policy	T1071.002	LiveWire
Unexpected encryption	Policy	T1571	LiveWire
TLS unexpected plaintext	Policy	T1571	LiveWire
TLS weak cipher suite	Policy	T1600	LiveWire
RDP connection after brute force attempt	Policy	T1021	LiveNX
SSH connection after SSH brute force attempt	Policy	T1021	LiveNX
Unauthorized application use	Policy	T1219 or T1071	LiveNX
RDP brute force attempt detected	Policy	T1110	LiveNX
SSH brute force attempt detected	Policy	T1110	LiveNX
New encryption protocol	Policy	T1571	LiveNX
Found RDP on non-standard port	Policy	T1571	LiveNX
New encryption user	Policy	T1573	LiveNX
New encryption service	Policy	T1573	LiveNX
New SSH client version found	Policy	T1573	LiveNX
New SSH server version found	Policy	T1573	LiveNX
New TLS version found	Policy	T1573	LiveNX
Insecure or weak cipher	Policy	T1587.003	LiveWire
New TLS SHA1 found	Policy	T1588	LiveNX
New TLS JA3C found	Policy	T1588.004	LiveNX
New TLS JA3S found	Policy	T1588.004	LiveNX
Lateral movement anomaly <application>	Anomaly	TA0008 (five techniques)	LiveNX
Clique expansion	Anomaly		LiveNX
Interface volumetric anomaly	Anomaly		LiveNX
Application interface volumetric anomaly	Anomaly		LiveNX
DSCP interface volumetric anomaly	Anomaly		LiveNX
Application site volumetric anomaly	Anomaly		LiveNX
Site volumetric anomaly	Anomaly		LiveNX

BlueCat's Intelligent Network Operations (NetOps) solutions provide the analytics and intelligence needed to enable, optimize, and secure the network to achieve business goals. With an Intelligent NetOps suite, organizations can more easily change and modernize the network as business requirements demand.

Headquarters
4100 Younge St. 3rd Floor, Toronto, ON, M2P 2B5
Phone: 1-416-646-8400 I 1-866-895-6931

bluecat.com

Next steps

Learn how you can get packet-level analysis at the network edge for fast and actionable security intelligence.

Contact us