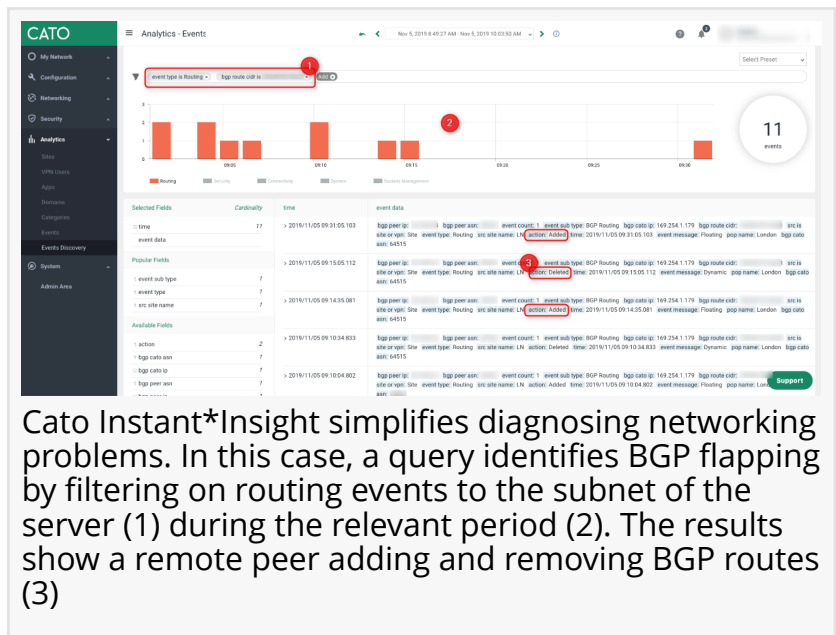# IT MANAGERS ANALYZE 1 MILLION EVENTS IN 1 SECOND AT NO CHARGE WITH CATO INSTANT*INSIGHT

*Cato Instant*Insight leverages the world's first SASE platform for breakthrough network visibility without the challenges of SIEMs and event managers.*

TEL AVIV, ISRAEL, December 10, 2019 /EINPresswire.com/ -- Cato Networks, provider of the world's first SASE platform, introduced today Cato Instant*Insight, the first time SIEM capabilities have been included at no cost in a secure access service edge (SASE) platform. Cato Instant*Insight leverages the convergence of networking and security into Cato SASE platform to eliminate deployment complexity, upfront investment, and the learning curve previously required with traditional event managers, SIEMs, and network analysis tools.

Cato Instant*Insight simplifies diagnosing networking problems. In this case, a query identifies BGP flapping by filtering on routing events to the subnet of the server (1) during the relevant period (2). The results show a remote peer adding and removing BGP routes (3)

"From its founding, Cato realized that converging networking and security into the cloud would simplify all aspects of networking. Cato Instant*Insight attests to that vision. With our SASE platform, we're able to deliver the kind of visibility out-of-the-box that previously required extensive custom integration and development," says Shlomo Kramer, CEO and co-founder of Cato Networks.

> From its founding, Cato realized that converging networking and security into the cloud would simplify all aspects of networking. Cato Instant*Insight attests to that vision."
> *Shlomo Kramer, CEO and co-founder of Cato Networks*

"Cato Instant*Insight let us find the 'needle in the haystack' in minutes," says Lars Norling, Director of IT Operations at ADB Safegate, a provider of airport efficiency and productivity solutions. "We build complex queries to filter through millions of events just by clicking on values on the side of the screen. Especially for smaller IT teams, Instant*Insight is a game changer. It lets them work together like a large NOC or SOC without investing tens if not hundreds of thousands of dollars on custom integration and forensic tools."

"I'm very impressed with Instant*Insight," says Tomy Joseph, Director of IT Infrastructure at Coolsys, a leader in the commercial refrigeration and HVAC industry. "We can use it right away to troubleshoot all sorts of problems, like our VoIP disconnects or security incidents, by mining a massive repository of security and networking data."

SASE ENABLES ADVANCED ROOT CAUSE ANALYSIS WITHOUT THE PAIN OR COST OF A SIEM

For years, IT's fragmented view of the network has hampered problem resolution and prevention. Developing a timeline of events required mastering a range protocols and APIs just to retrieve the necessary data from networking and security appliances. Data interpretation and normalization technologies were needed to store event data in common format for analysis.   Querying and utilizing this information required specialized skills and knowledge. Finally, IT was left having to store and maintain this massive data warehouse. All of which made root cause analysis difficult and impractical for many enterprises.
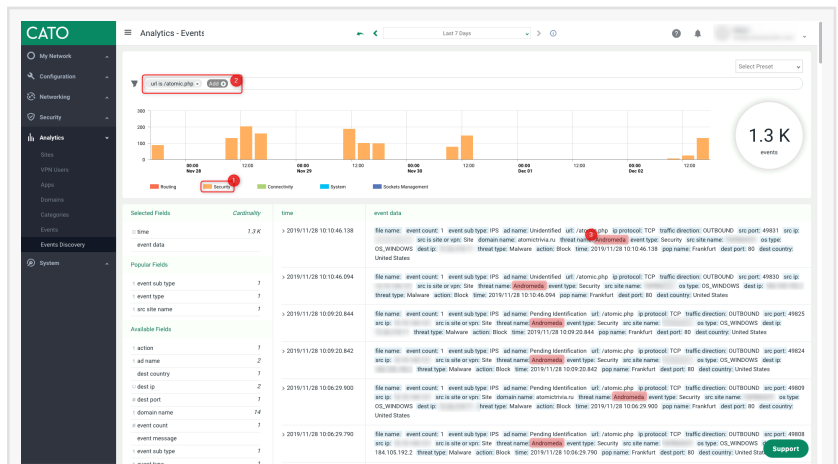
Cato Instant*Insight addresses these problems by organizing the millions of networking and security events tracked by Cato into a single, queryable timeline. IT teams can quickly filter the millions of networking and security events tracked by Cato to arrive at root cause.

Key to Cato Instant*Insight is the Cato's SASE architecture. First defined in Gartner's Hype Cycle for Enterprise Networking, 2019, SASE converges many disparate network and network-security capabilities including SD-WAN, SWG, CASB, SDP/ZTNA, DNS protection, and FWaaS onto a global, cloud-native platform. As such, all networking and security events are already stored in a common data warehouse maintained by Cato.
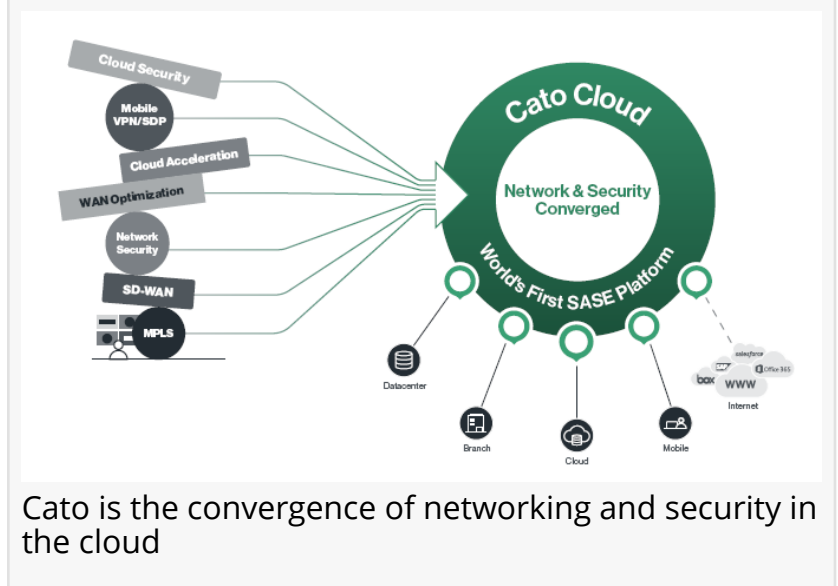

Cato Instant*Insight lets IT easily hunts for threats. Here a query identifies the Andromeda botnet by filtering security events (1) and then looking for traffic to the URI /atomic.php, which is associated with Andromeda (2). The main view (3) displays the raw results.

Cato is the convergence of networking and security in the cloud

More specifically, Cato Instant*Insight revolutionizes the challenges of delivering SIEM capabilities in three ways:
• Automated aggregation consolidates all security and networking events into one massive data warehouse without any effort. No additional agents are needed to extract, or code required to normalize data.
• Faceted search makes Cato Instant*Insight very adaptable and still easy to use. All variables and parameters are presented for easy querying. Network and security professionals simply select the requisite items to construct the necessary queries.
• The network analysis workbench is a built-in interface for data mining. There's no need to purchase an additional data analysis tool to piece together the timeline of networking and security problems. Instant*Insight correlates all events into a single timeline, filtered through this simple interface

PRACTICAL EXAMPLES OF HOW INSTANT*INSIGHT IMPROVE SECURITY AND NETWORKING ANALYSIS

Cato Instant*Insight helps organizations drill down through the millions of events generated across an enterprise network to spot security threats and diagnose network disruptions that were previously shielded by the fragmented visibility of appliances.

Security operations teams, for example, can use Cato Instant*Insight to easily identify the uniform, predictable communications that indicate bot traffic by reviewing entire communication exchanges between clients and suspicious target (see Figure 1). Companies with limited security staff or looking to augment their SOC should consider the Cato Managed Threat Detection and Response (MDR) service.

Networking teams can use Cato Instant*Insight to easily diagnose root cause of intermittent problems, such as periodic loss of connectivity. Normally resolving such issues require extensive event logging, unavailable in most edge routers. Cato Instant*Insight let's network administrators filter through millions of events across their global networks in seconds to uncover the cause of connectivity problems (see Figure 2).

To learn more about Cato Instant*Insight and the rest of the Cato solution, click here or contact us at https://www.catonetworks.com/contact-us

Dave Greenfield
Cato Networks
press@catonetworks.com
email us here

This press release can be viewed online at: http://www.einpresswire.com