Cato Unveils First SD-WAN With Revolutionary, Cloud-based Threat Hunting System

Cato leverages zero-footprint data aggregation, machine learning algorithms, and cross-enterprise traffic visibility to pinpoint threats and reduce dwell time

TEL AVIV, ISRAEL, May 23, 2018 /EINPresswire.com/ -- TEL AVIV, Israel, May 23, 2018 - Cato Networks, provider of Cato Cloud, the world's first secure, global SD-WAN as a service, announced today a revolutionary approach for hunting threats on enterprise networks. Cato Cloud serves as the virtual cloud network for hundreds of organizations connecting and securing all branch locations, mobile users, and physical and cloud datacenters. The Cato Threat Hunting System (CTHS), built into the Cato Cloud, leverages rich traffic context and unobscured network and endpoint visibility to accurately pinpoint threats and dramatically reduce dwell time. CTHS represents the first time that threat hunting is done without deploying a dedicated and costly data collection infrastructure within the enterprise.

> As an industry, detecting threats has been significantly hampered by the complexity of collecting granular, relevant data over time and applying the right analytics and people to interpret that data."
>
> *Gur Shatz, co-founder and CTO of Cato Networks*

"As an industry, our ability to detect threats has been significantly hampered by the complexity of collecting granular, relevant data over time and applying the right analytics and people to interpret that data," says Gur Shatz, co-founder and CTO of Cato Networks. "Virtual cloud networks, such as Cato Cloud, enable effortless access to such data, empowering our proprietary software and world-class SOC to hunt for threats on customer networks."

Threat Hunting System at the Core of Cato Cloud

Existing approaches to threat hunting combine end-point and network detection, third-party event logs, SIEM platforms, and managed detection and response services. These approaches are challenged on several fronts. First, sensors have to be deployed to collect raw data. Enterprises must ensure sensors intercept all relevant traffic in branches, datacenters and the cloud. Endpoint sensors complement network sensors, but can't be deployed on all edge devices (i.e. IoT devices). Second, logs fed into SIEM platforms lack the full network context, limiting their value for threat hunting. Finally, most organizations lack the skills and resources to analyze the data and identify persistent threats.

CTHS, built into Cato Cloud, overcomes the cost and complexity of existing approaches to accurately detect threats. CTHS has the following capabilities:

* Full Visibility, No Sensors: Cato Cloud sees all WAN and Internet traffic normally segmented by network firewalls and Network Address Translation (NAT). CTHS has full access to real-time network traffic for every IP, session, and flow initiated from any endpoint to any WAN or Internet resource. Optional SSL decryption further expands available data for threat mining. CTHS uses its deep visibility to determine the client application communicating on the network and identify unknown clients. The raw data needed for this analysis is often unavailable to security analytics platforms, such

as SIEMs, and is impossible to correlate for real-time systems, such as legacy IPS.

* Deep Threat Mining: Data aggregation and machine learning algorithms mine the full network context over time and across multiple enterprise networks. Threat mining identifies suspicious applications and domains using a unique “popularity” indicator modeled on access patterns observed throughout the customer base. Combining client and target contexts yields a remarkably small number of suspicious events for investigation.

* Human Threat Verification: Cato’s world-class Security Operations Center (SOC) validates the events generated by CTHS to ensure customers receive accurate notifications of live threats and affected devices. CTHS output is also used to harden Cato’s prevention layers to detect and stop malicious activities on the network.

* Rapid Threat Containment: For any endpoint, specific enterprise network, or the entire Cato customers base, the SOC can deploy policies to contain any exposed endpoint, both fixed and mobile, in a matter of minutes.

“The network, threat and application data available through the Cato Cloud is an analyst goldmine,” says Elad Menahem, head of security research at Cato Networks. “Using CTHS and its machine learning algorithms trained with data from hundreds of enterprise networks, we’ve been able to focus on the few security events that matter and identify malware infections in minutes."

CTHS creates a deep, threat hunting foundation that powers all Cato security services without which customers would be required to deploy data collection infrastructure or analyze mountains of raw data. At the same time, CTHS adheres to privacy regulatory frameworks such as GDPR. With CTHS and Cato Cloud, enterprises of all sizes continue their journey to streamline and simplify network and security.

Cato Researchers Present CTHS at Infosecurity Europe

Details of CTHS will be presented by Elad Menahem, head of security research, and Avidan Avraham, security researcher, at Cato, at the upcoming Infosecurity Europe show.

The Tech Talk, entitled “Improved C&C Traffic Detection Using Multidimensional Model and Network Timeline Analysis,” will occur on Wednesday, 6th June, at 16:00 – 16:25 in London.

To learn more about CTHS and Cato’s integrated networking and security solution, visit us at InfoSec, stand H60 or online here.

About Cato Networks
Cato Networks provides organizations with a cloud-based and secure global SD-WAN. Cato delivers an integrated networking and security platform that securely connects all enterprise locations, people, and data. Cato Cloud cuts MPLS costs, improves performance between global locations and to cloud applications, eliminates branch appliances, provides secure Internet access everywhere, and seamlessly integrates mobile users and cloud datacenters into the WAN. Based in Tel Aviv, Israel, Cato Networks was founded in 2015 by cybersecurity luminary Shlomo Kramer, co-founder of Check Point Software Technologies and Imperva, and Gur Shatz, co-founder of Incapsula. Visit www.catonetworks.com and Twitter: @CatoNetworks.

SOURCE Cato Networks

Contact (media only):

Dave Greenfield
Cato Networks
press@catonetworks.com