Cato Fortifies Cloud-native Security Services with New Threat Prevention and Detection Engines

CATO BOOSTS NETWORK PROTECTION WITH NEW ZERO-FOOTPRINT MANAGED THREAT DETECTION AND RESPONSE (MDR) SERVICE & SENTINELONE ZERO-DAY THREAT PREVENTION INTEGRATION

TEL AVIV, ISRAEL, February 26, 2019 /EINPresswire.com/ -- Cato Networks, the cloud-native carrier, announced today two additions to Cato Security Services. Cato Managed Threat Detection and Response (MDR) offloads the resource-intensive and skill-dependent process of detecting compromised endpoints onto Cato. A new partnership with SentinelOne, the leading provider of autonomous endpoint protection solutions, brings zero-day threat prevention to Cato's cloud-based network protection. The two introductions boost the stopping power of Cato's security services, providing CISOs with seamless, comprehensive detection and prevention against a wide range of threats.

In addition to instant alerts, Cato MDR includes a monthly audit report of all incidents.

"Stopping advanced threats and reducing the time to eliminate existing ones are essential for enterprise security. With SentinelOne's industry-leading, AI-powered threat prevention technology and Cato MDR, we extend the easily deployable, multi-layer security built into our cloud-native carrier platform," says Shlomo Kramer, CEO and co-founder of Cato Networks.

CATO: ZERO-FOOTPRINT THREAT PREVENTION AND DETECTION

Despite the heavy investment in threat prevention tools, attackers continue to penetrate enterprises of all sizes. Detecting network-resident threats still takes too long with dwell time on average exceeding 100 days. Reducing that window has required significant investment in dedicated and complex security and data analysis tools along with hiring hard-to-find, skilled security staff to operate them.

With today's announcements, Cato changes that paradigm. Cato's security services already included next-generation firewall (NGFW), intrusion prevention system (IPS), URL filtering (URLF), and anti-malware. With Cato MDR and SentinelOne zero-day, next-generation threat prevention, Cato now brings enterprises complete detection and protection against advanced threats without the complexity of additional hardware, software agents, or the need to access highly specialized security expertise.

> Cato MDR has already discovered several pieces of malware missed by our antivirus system and we removed them more quickly because of Cato."
>
> *Andrew Thomson, director of IT systems and services at BioIVT*

SQUASH MALWARE DWELL TIME WITH CATO MDR

Cato MDR is a fully managed service that offloads the detection of compromised endpoints onto Cato's security operation center (SOC) team. Cato MDR includes:

- AUTOMATED THREAT HUNTING —- machine learning algorithms look for anomalies across billions of flows in Cato's data warehouse and correlate them with threat intelligence sources and complex heuristics. This process produces a small number of suspicious events for further analysis.
- EXPERT THREAT VERIFICATION — Cato security researchers review flagged endpoints and assess the validity and severity of the risk, only alerting on actual threats. Cato relieves customers from handling the flood of false-positives that suck precious IT resources.
- THREAT CONTAINMENT — Verified live threats can be contained automatically by blocking C&C domains and IP addresses, or disconnecting compromised machines or users from the network.
- GUIDED REMEDIATION — The Cato SOC advises on the risk's threat level, recommended remediation, and follows up until the threat is eliminated.

"Cato MDR has already discovered several pieces of malware missed by our antivirus system and we removed them more quickly because of Cato," says Andrew Thomson, director of IT systems and services at BioIVT, a provider of biological products to life sciences and pharmaceutical companies. BioIVT relies on Cato to connect and secure its global network.

"We thought updating our security architecture was going to require running around to different vendors, piecing together a solution, and going through all of the deployment and management pains. So, when we found out that Cato not only delivered a global network but also built-in security services and now MDR, we were extremely excited. It was a huge help."

ZERO-DAY THREAT PREVENTION WITH SENTINELONE

Cato is also announcing next-gen threat prevention capabilities from SentinelOne. The company's industry-leading, AI-based, endpoint protection solution identifies threats without signatures, making SentinelOne particularly effective at stopping zero-day malware.

Cato uniquely implemented the SentinelOne threat prevention engine as a network-level defense. SentinelOne will run in Cato's PoPs globally, analyzing files in transit from the Internet or other Cato-connected resources, such as sites and mobile users. As such, Cato prevents zero-day malware from ever reaching targeted endpoints or moving laterally across the WAN.

"Cato's network-based implementation of SentinelOne's Nexus SDK will accelerate the deployment of next-gen threat prevention capabilities across customer networks of all sizes," says Tomer Weingarten, CEO and Co-Founder, SentinelOne. "In today's hyper-connected world, security is a core and inseparable tenant of networking. Partnering with Cato provides a robust, network-based, threat prevention solution that's seamless, smart, and easy to deliver across the globe."

CATO DELIVERS COMPREHENSIVE SECURITY EVERYWHERE

With addition of Cato MDR and zero-day threat prevention, Cato rounds out its cloud-native security service offering, providing complete, network-based attack protection worldwide. Sites, mobile users, cloud resources — once connected to Cato are protected from Internet-borne

threats. Just switch it on — no additional hardware, software, or IT grunt work is needed.

Cato MDR is currently available as a Cato managed security service. SentinelOne's technology will be offered as a premium Cato security feature in early Q2, 2019.

For more information about Cato Security Services click here.

ABOUT CATO NETWORKS

Cato Networks, the cloud-native carrier, connects enterprise locations, users and cloud resources into a global, secure, and optimized cloud-based network with built-in SD-WAN, network security, and WAN optimization. Unlike legacy telcos, Cato is agile, affordable, simple to deploy, and quick to adapt to changing business needs. Using Cato, customers can cut MPLS costs, improve performance between global locations and to cloud applications, eliminate branch appliances, provide secure Internet access everywhere, and seamlessly extend the WAN to mobile users and cloud resources. Visit www.catonetworks.com and Twitter: @CatoNetworks.

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