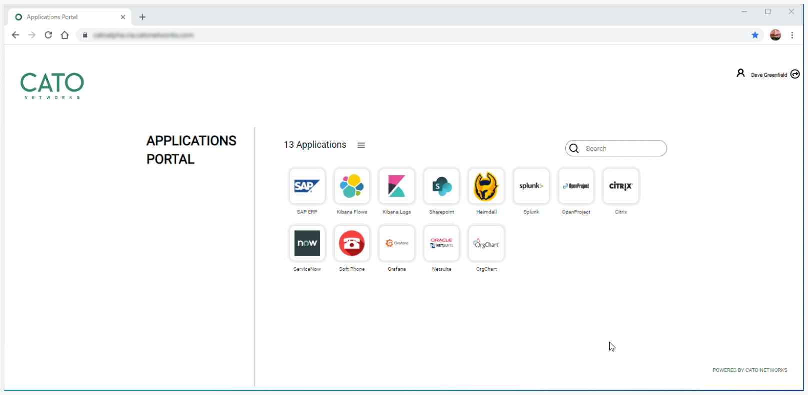
EIN PRESSWIRE

CATO LAUNCHES INSTANT ACCESS; THE FIRST SASE-BASED CLIENTLESS ACCESS SERVICE FOR DELIVERING WORK-FROM-HOME AT SCALE

Newest Enhancement to Cato SDP Demonstrates the Power of SASE, Enabling Enterprises To Deliver Secure, Fast, Remote Access Worldwide at the Flip-of-a-Switch.



Cato SDP with Instant Access simplifies secure remote access

TEL AVIV, ISRAEL, March 19, 2020 /EINPresswire.com/ -- Cato Networks,provider of theworld's first SASE platform, introduced today Cato SDP with Instant Access to help IT leaders rapidly deliver work-from-home solutions at scale worldwide. Instant Access adds a new clientless access option and application portal to Cato SDP, the first software-defined perimeter (SDP) solution to leverage a true secure access service edge (SASE) architecture, delivering shorter rollout times, unlimited scalability, continuous threat prevention, and optimized performance worldwide.

> We found ourselves having to rapidly increase our capacity to support a larger than normal remote workforce and successfully rolled out 150+ Cato VPN clients within 24 hours. It was a huge success."
>
> *Kent Wade, Director of IT and Cybersecurity at Westmoreland Mining LLC*

"With the global health crisis, enterprises are looking to deploy work-from-home capabilities at scale. Cato has seen remote access adoption more than double since the outbreak of COVID-19. The enhancements to Cato SDP will further help IT leaders to quickly deliver secure remote access at scale to their employees across the globe," says Shlomo Kramer, CEO and co-founder of Cato Networks.

CATO SDP WITH INSTANT ACCESS DELIVERS OPTIMIZED REMOTE ACCESS WORLDWIDE IN MINUTES

As work-from-home becomes the norm, remote access has become an even more critical part of IT infrastructure. Legacy VPN servers suffer from scalability limitations, which impact the expansion of work-from-home access to all employees, and performance problems for distant remote users. VPN also introduces security risks as malicious users are a mere password away from sensitive business-critical resources.

Cato SDP addresses those challenges. With Instant Access, users can only access authorized applications. They simply click a URL, authenticate once through single sign-on (SSO), and gain access to their portal of authorized applications. For those requiring full access to both Web and legacy applications, Cato continues to offer its Cato Client as part of Cato SDP.

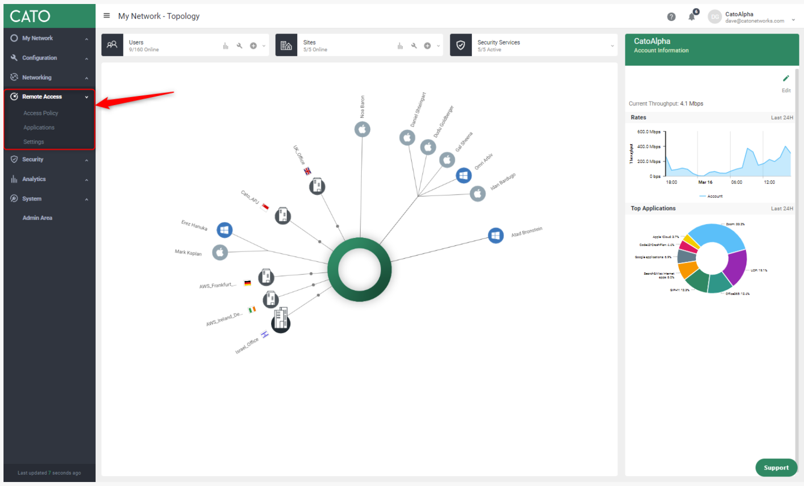
CATO SDP LEVERAGES THE POWER OF SASE TO TRANSFORM REMOTE ACCESS

By leveraging Cato's global SASE platform, Cato SDP with Instant Access solves the critical scaling,

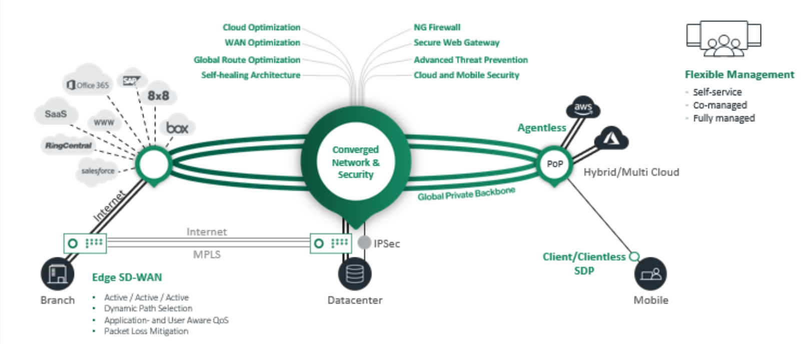
performance, security, and management limitations that have hampered legacy mobile access solutions. Specifically, Cato SDP delivers:
* Rapid Deployment – Cato SDP deploys instantly, requiring no additional software on the mobile device or SDP connector software or SDP gateway hardware in the datacenter. As the enterprise network, Cato already controls application flows, allowing Cato customers to publish applications with just a few clicks at their Cato management consoles.

* Unlimited Scalability– Cato's SASE cloud-native and globally distributed architecture supports an unlimited number of users across the globe. Users can easily move from the office to their homes, or work on the road, with their access being consistently secure and always optimized.

* Optimal Global Performance – Cato SDP sends remote traffic across Cato's optimized, global private backbone not the unpredictable public Internet. Remote users are first-class citizens on the corporate network.



The Cato management console is a single-pane-of-glass for managing remote access and the rest of the enterprise network.



Cato. The Network for Whatever is Next

* Secure Access – Multi-factor authentication is part of the SASE platform and is provided with Cato SDP. Restricting access to approved applications and eliminating network credentials simplifies not only the user experience but also removes the risk of attackers or advanced malware accessing unauthorized network resources.

* Continuous Threat Prevention – Cato's cloud-based network security stack continuously protects remote workers against network-based threats. Cato's security stack includes NGFW, SWG, IPS, advanced anti-malware, and Managed Threat Detection and Response (MDR) service.

* Single-Pane-of-Glass Management – Cato SDP is configured, maintained, and managed through the same portal as the rest of Cato's networking and security services making configuration and management very simple.

ENTERPRISES RELY ON CATO SDP FOR REMOTE ACCESS DURING GLOBAL HEALTH CRISIS
Many are already benefiting from the power of Cato SDP. Here's what several enterprises had to say:

ASM Assembly Systems
"Cato has helped us respond to the COVID-19 outbreak significantly faster than would otherwise have been possible. We had been using a firewall as our VPN server but when our users shifted to working from home, we saw the CPU load jump to 79% as concurrent VPN usage more than tripled. We expect to hit over 90% when our VPN usage quintuples by end of the week," says Ian Bleazard, IT Director of Infrastructure and Analytics in the SMT segment of ASM Assembly Systems, a leading global supplier to the electronics business.

“With Cato, we can equip all employees with a very scalable remote solution and instead of connecting to a VPN server, they can just connect straight into the Cato Cloud and be able to source all our global applications.□□We are also able to issue those licenses and manage the remote users from the same dashboard we use for our global offices. Having one console for everything makes the whole management process much simpler, and very much helped us stay on top of these unique circumstances.”

Geosyntec Consultants
“Our company is dispersed across the globe with over 80 office locations, many of them are on the Cato network. We utilize a few different VPN technologies. With the COVID-19 pandemic on the rise, many of our users began to work remotely. Our VPN traffic spiked, in some cases hitting the limits of our VPN servers,” says Edo Nakdimon, Senior IT Manager, at Geosyntec Consultants, an environmental engineering firm.

“Instead of purchasing more VPN server licenses, we equipped remote users with Cato access. In a matter of 30 minutes, we configured the Cato mobile solution with single-sign-on (SSO) based on our Azure AD. Cato provided us a scalable remote access solution that extends our QoS and network policies in our SD-WAN to our remote users and reduced the network overhead and bottlenecks for remote users as they connected directly to Cato, eliminating unnecessary hops across the public Internet core. The easily deployed SSO and web filtering integration provided us an additional layer of security for our VPN users. The Cato mobile access solution is simple to deploy, yet robust. It improved our employee’s ability to securely and productively work remotely.

Westmoreland Mining
“We found ourselves having to rapidly increase our capacity to support a larger than normal remote workforce and successfully rolled out 150+ Cato VPN clients within 24 hours. It was a huge success,” says Kent Wade, Director of IT and Cybersecurity at Westmoreland Mining LLC, a coal supplier.

To learn more, visit us at www.catonetworks.com

Dave Greenfield
Cato Networks
press@catonetworks.com
email us here
Visit us on social media:
Twitter

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

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases.