

Coronet releases SecureCloud 4.0: A cybersecurity suite optimized for the Hybrid Workspace

Enabling lean IT organizations to effortlessly secure the new reality without spending millions of dollars.

New York, NY August 4th 2020 – Coronet, the fastest growing cyber security platform providing enterprise grade all-in-one security as a service to companies of any size, announced today a new version of its' flagship platform, SecureCloud.

SecureCloud 4.0: Optimized for the Hybrid workspace

SecureCloud 4.0 was optimized to address the new security challenges organizations face as the hybrid workspace becomes the norm. "As users now work from home, the office, on their own devices, on corporate devices, or any combination of the above, organizations are faced with a massive increase in attack surface, yet shrinking budgets and teams" said Guy Moskowitz, Coronet's CEO and co-founder. "The traditional separation of home and work environments is no longer relevant and trying to use traditional security measures such as firewalls and VPNs makes no operational, or financial sense."

Using a zero-trust architecture, SecureCloud 4.0 assumes risks at the user, device, network, email, cloud applications, and access levels, and as such monitors and through powerful AI engines, mitigates risks with no need for human intervention.

Hybrid Workspace introduced a demonstrable increase in attacks

Based on threat data from the 4 million users Coronet currently protects, Coronet saw an increase of 28% in phishing attempts, 17% data leakage, 13% in bots attacks, and a whopping 622% increase in access attempts from unsafe devices. "After the move to work from home, we saw a 400% jump in access from Windows 7, an unpatched, and potentially risky OS, to organizational data" Said Moskowitz. "This was the reason we decided to extend our endpoint protection capabilities to Windows 7 despite its sunset by Microsoft, so we can protect our customers from a potential security nightmare"

The first virtual firewall between the home and office environments

Because Coronet monitors and protects both endpoints as well as email and cloud services in one cohesive platform, SecureCloud 4.0 identifies risks and mitigates them across domains. "If we see that a personal device was infected with malware, we are in the unique position to disable access from that device to corporate data, creating the first virtual firewall between the home and office environments, all while leaving the user's home environment untouched" Said Doron Milchtaich, Coronet's co-founder and CTO. "This ensures no threats leak from the home environment into the organization's environment, eliminating the biggest risk the hybrid workspace poses"

"For a buck or two more than most organizations pay for anti-malware per user, Coronet provides a full security suite protecting endpoints, email, cloud, DLP, access control, and UBA all delivered through a single pane of glass. It was designed from the ground up to thrive in lean-IT organizations, as our AI engines do 93% of the event chasing and mitigation a human once had to do." Summarized Moskowitz.

SecureCloud 4.0 is currently being used by select Coronet customers and will be automatically updated to all Coronet customers in the third week of August.

About Coronet

Coronet protects over four million users and organizations of every size against email threats, data leakage, malware and ransomware, regulatory compliance risks, and cloud app risks. Designed for the hybrid workspace, Coronet's platform uses AI to detect and mitigate threats, eliminating the need for a security team to chase down security events. Provided as a subscription service, with nothing to install on premises, Coronet brings comprehensive, enterprise grade cyber defense through a single pane of glass at an affordable price, eliminating the complexity and laborious nature of traditional security platforms.

To learn more about Coronet, visit us at www.coro.net or follow @coronetnetworks on social media.

Contact:

Abigail Wilson
abigail@coro.net