The Future-Ready SOC: Using XDR to Achieve Unified Visibility and Control

CIOs and CISOs of globally distributed enterprises face an enormous challenge: how to scale operations to meet the pace of escalating threats while IT and security team members are distributed and rely on a web of disconnected and disparate tools to do their work.

The technology and procedural silos that exist between IT and security operations center (SOC) team members have impeded an enterprise's ability to effectively mitigate risk. Until and unless this chasm is crossed, SOC teams and their IT counterparts will never achieve their goals. An overwhelmed, distributed workforce and increasing attacker dwell times have raised the stakes for the CIO and CISO. Reducing mean time to resolution (MTTR) is a critical goal because the faster an incident is detected, investigated and resolved, the more likely it will result in a good business outcome. Two critical success factors hold the key to preparing for the future-ready SOC: automation and the cloud.

By unifying detection and response activities across IT and security domains and devices, VMware Carbon Black Cloud™ delivers the essential foundation for XDR (Extended Detection and Response) and takes it even further. VMware Carbon Black Cloud uniquely acts as XDR-ready infrastructure and offers native support for automated, cross-domain, XDR-enabled controls that deliver built-in, context-centric, unified security.