Healthcare Sector

Safety and Soundness

83 percent of surveyed healthcare organizations said they've seen an increase in cyberattacks over the past year

66 percent of surveyed healthcare organizations said cyberattacks have become more sophisticated over the past year

45 percent of attacks motivation was destruction of data

The Situation

Healthcare organizations are increasingly being targeted by cyberattacks due to the gold mine of personal data they possess. The potential damaging effects these attacks can have is substantial. Cyber attackers now have the ability to access, steal and sell patient information on the dark web. Beyond that, they have the ability to shut down a hospital's access to critical systems and patient records, making effective patient care virtually impossible. With increased adoption of medical and IoT devices, the surface area for healthcare attacks is becoming even larger. The problem has been further compounded by limited cybersecurity staffing and stagnant cybersecurity budgets in the industry.

VMware Carbon Black offers healthcare organizations the tools they need to keep their systems safe and compliant, by using a single agent and an easy to use console. It is lightweight, and easy to deploy on tens of thousands or even hundreds of thousands of endpoints.

Increase Endpoint Visibility

With the growing sophistication of attacks, CISOs need to look at any connected asset as a potential target. This includes electronic medical-record systems, medical devices, payment processing systems, and more. VMware Carbon Black's EPP empowers you to accelerate investigations and respond confidently to threats. Easy to digest attack chain visualizations—powered by real-time endpoint data—make it simple to see what has happened, and is happening, on your machines.

LEARN MORE

To set up a personalized demo or try it free in your organization, visit *CarbonBlack.com/trial*

For more information or to purchase VMware Carbon Black Products please call: (855) 525-2489 in the US, (44) 118 908 2374 in EMEA

For more information, email *Contact@CarbonBlack.com* or visit *CarbonBlack.com*

Establish Protection from Emerging Attacks

With the potential attack surface growing and evolving quickly, you need to stop as much as possible. This means leveraging a variety of technologies from whitelisting to streaming analytics to behavioral prevention. VMware Carbon Black's EPP collects and centralizes massive amounts of data in real time and analyzes attackers' behavior patterns to detect and stop never-seen-before attacks. Leveraging the power of the cloud, it analyzes more than 500B events per day across millions of global endpoints, helping you stay ahead of emerging attacks.

Run Automated Compliance and Vulnerability Assessments

With the risk of attack ever present, it's important to audit systems regularly and establish remediation steps across all your security infrastructure. VMware Carbon Black's EPP allows you to query your endpoints, in real time, and at scale. This eases the burden of managing complexity for teams by making it simple to find vulnerabilities and to achieve (and prove) compliance—streamlining security operations and saving teams time.

Work with Healthcare-Focused MDRs

There are a variety of managed detection & response service providers out there who specialize in the unique challenges faced by healthcare organizations. When resources are short, these shops can quickly improve your security posture and Carbon Black has a large number of partners in this space.

Application Whitelisting

To block unauthorized activities that could potentially initiate a harmful attack, Carbon Black offers application whitelisting, or application control, to strengthen perimeter security. Whitelisting identifies known files, applications, or processes and allows them to execute. Conversely, unknown activities are blocked or restricted, which prevents them from opening up and spreading within a system or environment in an attack mode.

vmware® Carbon Black