vmware Carbon Black

Carbon Black XDR

EDR made better. XDR made easy.

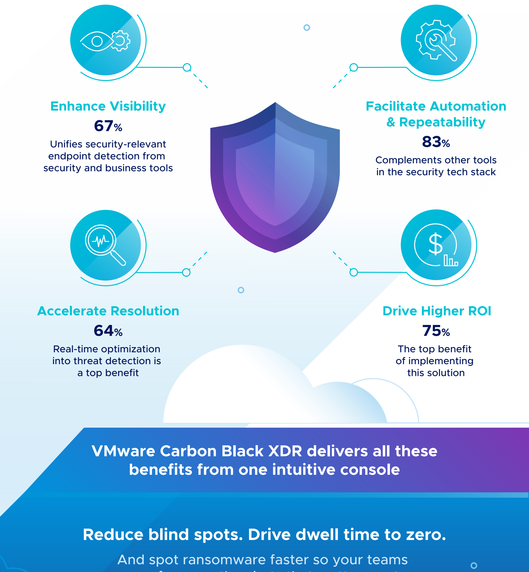
Get the comprehensive visibility you need to combat modern threats.

IT professionals report an increase in ransomware attacks by **48%**[1]

The average time required to contain an incident is **85 days**[2]

With only **12%** of incidents contained within 30 days[3]

78% of IT leaders lack confidence in their company's security tools and saw room for improvement.[4]



VMware Carbon Black XDR

Accelerate threat detection and response with automated correlation of telemetry across endpoints, networks, workloads, and users

According to security professionals who've adopted an XDR solution[5]:

Enhance Visibility

67%

Unifies security-relevant endpoint detection from security and business tools

Facilitate Automation & Repeatability

83%

Complements other tools in the security tech stack

Accelerate Resolution

64%

Real-time optimization into threat detection is a top benefit

Drive Higher ROI

75%

The top benefit of implementing this solution

VMware Carbon Black XDR delivers all these benefits from one intuitive console

Reduce blind spots. Drive dwell time to zero.

And spot ransomware faster so your teams can focus on the alerts that matter most

Catch Sophisticated Threats

Reduce Alert Fatigue

Track Threats Across Many Systems

Visualize Threats in Context

Reduce Operational Complexity

Deploy with Ease

[1] 2023 Thales Data Threat Report

[2] Ponemon Institute, "2022 Ponemon Institute Cost of Insider Threats Global Report," April 2022.

[3] Ibid.

[4] 2021 Insight Report.

[5] Forrester Consulting study commissioned by VMware, "Evolving Security Operations Capabilities: Insights into the XDR Paradigm Shift," December 2022.

To learn more about **VMware Carbon Black XDR**, visit: carbonblack.vmware.com/carbon-black-xdr-activity-path

vmware Carbon Black