zscaler / vmware Carbon Black

PARTNER BRIEF

Zscaler and VMware Carbon Black Cloud

Cloud-native security across users, devices, and applications

Traditional endpoint and network security leaves you vulnerable

Today's security and IT teams too often find themselves navigating complex systems of patchwork point solutions deployed to secure different aspects of their environment. The disconnect created by disparate endpoint and network security products adds complexity and makes it difficult to get a full picture of the organization's security posture. This inhibits the ability to coordinate across IT teams to rapidly identify, investigate, and remediate threats, and ensure zero trust application access, especially as organizations increasingly move to support remote workers and BYOD. Legacy security products were never designed to support cloud applications or protect distributed workforces against today's emerging threats—such as file-less and living-off-the-land attacks—and ultimately increase risk.

USE CASES

- Actionable intelligence sharing
- Zero-day threat detection and response
- Posture-driven, zero trust conditional access

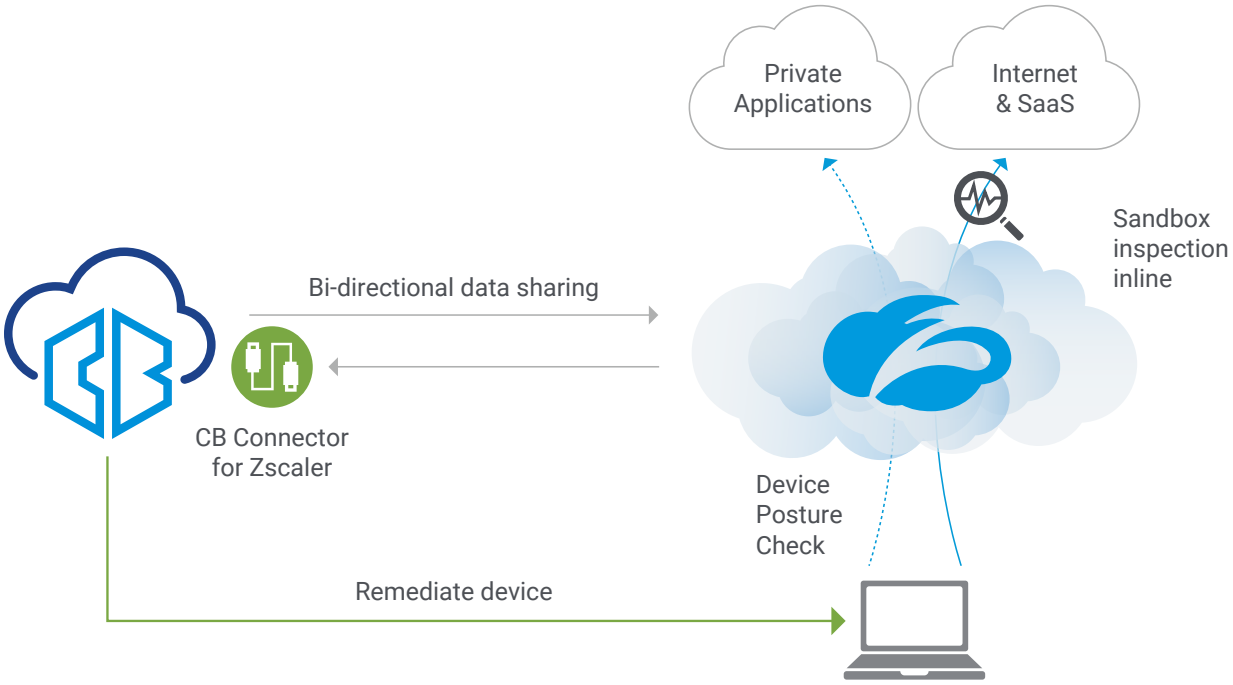
Integrate intelligence to stop zero-day threats and enable zero trust application access

Modernizing security and IT tools provides organizations with increased confidence in their security program and the ability to adapt to maintain productivity despite the increasing sophistication and volume of attacks. Cloud-native platforms reduce overall complexity by providing deeper integrations across systems and increased flexibility for deployment and updates.

By sharing threat intelligence and correlating insights across platforms, VMware Carbon Black and Zscaler™ combine to provide modern, integrated security solutions that deliver end-to-end visibility and protection across users, devices, and applications, including cloud, web, and private applications.

Carbon Black's flexible prevention policies and endpoint response actions combined with Zscaler's advanced threat protection, sandboxing, secure private applications access capabilities, and visibility into files and corporate assets provide an endpoint-to-cloud solution that identifies risk across any environment. This joint solution also prevents those risks from impacting endpoints, enables zero trust conditional access to internal applications, and automatically responds in real time to any activity found to be malicious.

> Together, VMware Carbon Black and Zscaler stop zero-day threats from impacting endpoints and enable true zero trust conditional access to internal applications.



Critical Capabilities

Zscaler Internet Access™ and Zscaler Private Access™ integrate with VMware Carbon Black Cloud Endpoint Standard and VMware Carbon Black Cloud Enterprise EDR to deliver three critical capabilities:

Actionable intelligence sharing

Sharing threat intelligence between Zscaler Internet Access and VMware Carbon Black enables more rapid identification of threats and coordinated endpoint prevention policies to protect devices against emerging threats. The joint solution provides visibility and context to proactively harden your environment and enable a flexible and customized response to threats, including adding to threat feed, triggering policy, isolating endpoints, terminating offending processes, and creating webhooks for policy handling.

Zero-day malware detection and response

Integrating the advanced threat prevention capabilities of Zscaler Internet Access and the VMware Carbon Black Cloud enables organizations to identify and stop zero-day threats before they impact endpoint devices and critical assets. The integrated solution automatically links threats identified in Zscaler Advanced Cloud Sandbox to impacted endpoints and leverages Carbon Black endpoint response capabilities to expedite remediation and mitigate threats.

Posture-driven, zero trust, conditional access

Together, Zscaler and Carbon Black strengthen security by ensuring devices are protected by Carbon Black before allowing zero trust access to business-critical internal applications through Zscaler Private Access. This approach ensures only authenticated users and managed devices are connected only to authorized applications. It works by extending access control policies to include key device security and health indicators to prevent unauthorized or compromised devices from accessing corporate applications, ultimately providing a true zero trust approach to application security.

KEY BENEFITS

Minimized attack surface

- Align and connect security policies and workflows to reduce overall risk
- Identify and stop zero-day attacks before they reach endpoints
- Coordinate security policies across endpoints and cloud apps to reduce the time it takes to identify and mitigate threats

Actionable intelligence and accelerated response

- Leverage intelligence sharing to harden environment and customize response
- Increase visibility into activities of roaming users
- Automatically link identified threats to impacted endpoints

Faster investigation and response

- Accelerate incident resolution through coordination of detection and response capabilities
- Rapidly assess impact of threats across entire endpoint environment
- Enable automatic remediation of endpoints to contain threats

Secure application access

- Enable posture-driven conditional access to better protect business-critical apps
- Prevent unauthorized or compromised devices from accessing corporate applications
- Ensure authorized users are only connected to authorized applications

Reduced cost and complexity

- No infrastructure or security hardware to buy, deploy, or manage
- Cross-platform integration enables faster deployment and automated updates
- Cloud-native security enables flexible deployment options and elastic scalability

About Zscaler
Zscaler enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a multitenant, distributed cloud security platform that protects thousands of customers from cyberattacks and data loss. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

About VMware Carbon Black
VMware software powers the world's complex digital infrastructure. The company's cloud, app modernization, networking, security, and digital workspace offerings help customers deliver any application on any cloud across any device. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact. For more information, please visit **vmware.com**.

zscaler™ / vmware® Carbon Black

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com