Managed Detection and Response (MDR) for Private Equity and Venture Capital

PONDURANCE

How to protect your investments and portfolio



Cyberattacks are certainly not a new threat in any digital industry, but recent trends reported by the Wall Street Journal indicate that hackers are turning their sights to midmarket companies and the private equity and venture capital firms that back them as prime targets. Ransomware groups have begun to see these portfolio businesses as lucrative sources of payouts because they know how much money is at stake for their targets. Also, attacks on smaller organizations tend to stay out of the news and cybersecurity has traditionally not been a high priority in the due diligence of funding deals. By scanning the newswire for deal announcements and targeting companies who just received funding, these bad actors see not only a vulnerable target in the new portfolio company but also an avenue of attack on the investment firm's entire portfolio. While these trends are alarming, there are steps a firm can take to drastically mitigate these risks.

A strong cybersecurity posture with MDR services as a cornerstone can ensure your portfolio is protected.

WHAT STEPS CAN I TAKE TO PROTECT MY PORTFOLIO?

Because the threat landscape is considerably broader now, with remote workers logging into company systems from multiple devices and scattered networks, PE and VC firms must assess how well potential portfolio companies are handling cybersecurity. For instance, are they regularly training employees on how to watch for phishing scams or malware? Are employees taking proper precautions to ensure the safety of their passwords?

While it is difficult to thoroughly assess each potential investment for effective cybersecurity posturing, there are some key areas you can probe to determine an acceptable minimum level of security.

For each potential investment, you should understand:

- Are there risk assessment protocols in place?
- Do they have a program in place to scan for and manage security vulnerabilities?
- Do they train employees to recognize and avoid potential phishing and malware attacks?
- Do they have the ability to detect, investigate and respond to cyber threats?
- Do they have incident response playbooks?
- Do they regularly utilize any security reporting or analytics?

By establishing minimum requirements for all your businesses, you can ensure your potential investments are not easy targets for cybercriminals.

HOW CAN I ENSURE MY OWN FIRM IS SECURE?

Apart from asking yourself the same questions you would ask a potential portfolio company you plan to invest in, there are services available to help you if you aren't sure of the answers you get when you look internally at your own cybersecurity practices.

For an investment firm to stay competitive and protected with so much complexity in its security landscape, MDR services can be particularly valuable. Unlike cybersecurity software tools or even traditional managed security services, MDR delivers comprehensive Security Operations Center (SOC) services from a team of analysts to provide active detection of malicious activity in your network and assist in rapid incident response to eliminate those threats with targeted remediation actions.

Most importantly, MDR ensures you have a team of experts behind you 24/7, ready to quickly respond to any security events that may occur. Our MDR team stands ready to partner with both you and your firm to protect your business.

THE PONDURANCE DIFFERENCE

24/7 U.S.-based SOCs – Our SOCs never take a day off. Pondurance MDR services are powered by analysts, threat hunters and incident responders who utilize our advanced cloud-native platform technology to provide you with continuous cyber risk reduction.

360-degree visibility – Pondurance provides extended detection and response (XDR) across fully managed and monitored solutions for:

Networks – Network traffic analysis sensors
Endpoints – Endpoint detection and response
Logs – SIEM-as-a-service platform
Cloud infrastructures – Including AWS, GCP and Azure

Rapid response and close collaboration – Closed-loop incident response helps you reduce the time it takes to respond to emerging cyber threats.

Integrates with your existing infrastructure and controls – No need to rip out your existing security investments. Pondurance integrates with your cloud and traditional security controls.

pondurance.com

Contact us at PE-VC@pondurance.com to learn more.

Copyright © 2022 Pondurance