

HOW ADS STAYS PROTECTED FROM CRITICAL VULNERABILITIES

SUMMARY

Atlantic Data Security (ADS), a Check Point Elite Partner, experienced firsthand the efficacy of Veriti's proactive security measures when a critical VPN vulnerability (CVE-2024-24919) was automatically blocked before it could cause harm.

CHALLENGE

ADS faced a significant challenge with a newly surfaced vulnerability affecting Virtual Private Networks (VPNs). The Check Point vulnerability identified as CVE-2024-24919 compromised the confidentiality, integrity, and availability of VPN connections, potentially allowing attackers to intercept, manipulate, or disrupt secure communications. While ADS was diligently working with their customers to implement a mitigation plan, their own systems remained unpatched due to the immediate demands of customer protection.

SOLUTION

ADS utilized Veriti for their internal firewall management and had implemented its automatic Indicator of Compromise (IOC) feature to streamline the remediation of daily threats. During the emergence of CVE-2024-24919, Veriti's proactive exposure assessment and safe remediation capabilities were crucial.

Despite ADS not having patched their systems yet, Veriti automatically blocked an exploitation attempt related to CVE-2024-24919.

RESULTS

The impact of Veriti's protection was significant. Within a week, Veriti completed 20,308 remediation actions, saving ADS approximately 848 labor days and \$508,500 in cost savings. With an MTTR (Mean Time to Repair) of just 4 hours, the efficiency of Veriti's automated systems was clear.

ADS's confidence in Veriti's capabilities was further affirmed by the sheer volume of attacks blocked—1.4 million—demonstrating the system's robust defense against diverse threats. By mitigating CVE-2024-24919 proactively, Veriti not only protected ADS but also provided a compelling success story for ADS to share with their customers, driving further adoption of Veriti's solutions.

Veriti's proactive exposure assessment and safe remediation have proven to be invaluable for Atlantic Data Security. By automatically blocking critical vulnerabilities like CVE-2024-24919 before they could be exploited, Veriti has ensured proactive protection and operational efficiency.

"Veriti gives us peace of mind that we are protected even when we have not patched yet. This is what security tools are supposed to do. Protect you from yourself."

Scott Perzan, Director of IT and Security Services Technology at ADS



**LEADING CYBERSECURITY CONSULTANCY
AND SOLUTION PROVIDER**

CHALLENGE

New Vulnerability:

CVE-2024-24919, a critical Check Point vulnerability, compromised VPN confidentiality, integrity, and availability.

Immediate Customer Protection:

ADS was focused on helping customers mitigate the vulnerability, delaying their own system patching.

Threat Exposure:

Unpatched systems increased the risk of exploitation.

REALIZED VALUE OF 1 WEEK FROM CONTINUOUS EXPOSURE ASSESSMENT AND SAFE REMEDiation

20,308

remediation actions completed within a week

848 DAYS

of labor saved

\$508,500

Cost Savings

4 HOURS

Mean Time to Repair (MTTR) reduced

1.4 MILLION

attacks blocked.