

COMPLETE ENDPOINT PROTECTION

CrowdStrike and Kudelski Security

Despite a multitude of anti-virus products available, around 70% of breaches still originate at the endpoint. Security-conscious organizations are now turning toward the light-weight agility of cloud-based endpoint detection and response (EDR) solutions that do more to keep them ahead of the curve – either managed by their own security teams or a modern MSSP.

Protecting the Endpoint

A number of options are available to address the challenge of protecting endpoints from both malware-based and malware-less attacks.

Standard anti-virus technology provides some level of endpoint protection but struggles to detect sophisticated attacks and does not immediately trigger effective incident response.

CrowdStrike, through their cloud-based architecture, provides an endpoint detection, protection and response solution that is easier to deploy. It is compatible with multiple operating systems, centers on behavioral analytics and Indicators of Attack (IoA) to detect and prevent threats.

Kudelski Security enhances the CrowdStrike offering through its Managed Security Services. We extend the capabilities of security teams to deal rapidly and decisively with threats detected on the endpoint, before they disrupt operations. Clients will get 24x7x365 protection, pervasive endpoint visibility and benefit from the rich expertise of our threat hunters and analysts who will perform additional investigations to rapidly confirm threats. If needed, we will activate the agreed response plan to block and contain the attack before critical assets can be compromised. Every alert we send out is contextualized, actionable and with easy-to-follow remediation guidance.

The State Of Endpoint Security



76% of buyers have either changed their AV vendor recently, or plan to do so



40% of organizations use three or more agents to protect against a range of threats



Only **41%** of buyers have upgraded to their vendor's latest product in a timely manner



EDR is now the most desired additive endpoint feature