# CROWDSTRIKE & KUDELSKI SECURITY

## Complete Endpoint Protection

Despite a multitude of anti-virus products available, around 70 percent 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 or a modern MSSP.

### Protecting the Endpoint

CrowdStrike, through their cloud-based architecture, provides an endpoint detection, protection and response solution that is easier to deploy. It is compatible with mutliple operating systems, centers on behavorial analytics and Indicator 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 gety 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 it contextualized, actionable and with easy-to-follow remediation.

### The State of Endpoint Security

**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

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

**EDR** is now the most desired additive endpoint feature

CrowdStrike is the leader in cloud-delivered next-generation endpoint protection. CrowdStrike has revolutionized endpoint protection by being the first and only company to unify next-generation antivirus, endpoint detection and response (EDR), IT hygiene, vulnerability assessment and a 24/7 managed hunting service – all delivered via a single lightweight agent.

www.crowdstrike.com

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.

# Kudelski Security

## Next-Generation Managed Security Services

Kudelski Security amplifies the power of the CrowdStrike solution through its advanced Managed Security Services, providing security teams a range of benefits.

- Improve resilience to attack
    - We reduce threat detection time through fusion of security data and contextual intelligence, gathered from a vast range of sources
    - We deliver fast, effective threat analysis and thorough investigation of relevant alerts
    - Daily threat hunting detects hidden activity of an advanced attack, which would otherwise be missed
    - The optional CrowdStrike Data Retention and Investigation Service is designed to leverage the Falcon Data Replicator to pull all agent-collected data and make it searchable for up to a one year (rolling 12 month) period in the Kudelski Security private cloud
- Adopt a streamlined response to incidents with our clear, actionable recommendations
- Gain broad visibility into the state of your security, through our MSS client portal
- Easy-to-understand dashboards and monthly service reporting

# CrowdStrike

## Next-Generation Endpoint Protection

CrowdStrike Falcon modules provide complete endpoint protection through solutions such as application and system discovery, next-generation anti-virus, and continuous endpoint visibility. Falcon enables you to prevent both known and unknown attacks, malware or malware-free, whether your endpoints are connected to the Internet or not.

- Gain real-time endpoint visibility and insight into all applications and processes – authorized or not
- Protect endpoints across all leading platforms, including Windows, OSX, and Linux, data center servers, virutal machines and all major cloud platforms
- Retire legacy antivirus and simplify endpoint security with easily deployable, next-generation endpoint protection technology



Info@kudelskisecurity.com | www.kudelskisecurity.com

KUDELSKI SECURITY