

VARONIS + CROWDSTRIKE

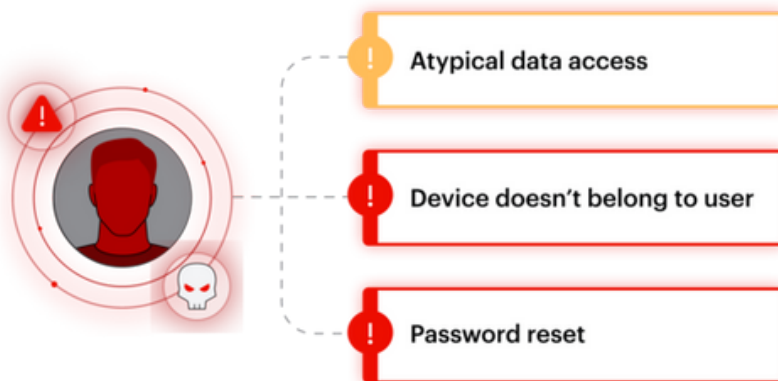
End-to-end threat detection and response.

CHALLENGE

Sensitive data threats come from every part of the perimeter. Organizations often struggle to protect sensitive data due to fragmented security systems, leading to alert fatigue, labor-intensive manual investigations, and delayed response times. Threat actors exploit these gaps in visibility and communication between security tools to evade detection and compromise larger amounts of data.

SOLUTION

Varonis' integration for CrowdStrike Endpoint Security provides Varonis Managed Data Detection and Response (MDDR) analysts with a real-time feed of your EDR alerts and related telemetry directly within our platform. This additional telemetry enhances our incident responders' and forensic analysts' ability to detect a broader range of threats earlier in the kill chain, allowing them to conduct end-to-end investigations with minimal involvement from customers or third parties.



KEY BENEFITS

- Detect more threats earlier on the kill chain.
- Get swift and conclusive investigations.
- Maximize your CrowdStrike Endpoint Security investment.

“We can rest easy knowing Varonis is handling our data. If they identify a critical risk, they escalate the matter, address it quickly, and give us confidence during the incident management process.”

AARON KALIST

Cybersecurity Administrator,
Keeley Companies

[Read the full case study here](#)



Detect more threats earlier on the kill chain.

Varonis MDDR analysts use CrowdStrike Endpoint Security alerts to proactively identify and stop a wide range of threats. This approach ensures that potential threats are mitigated before they can cause significant damage, enhancing your overall security posture.



Get swift and conclusive investigations.

Varonis consolidates telemetry from various sources —data, cloud, identity, network, and endpoint—into a single view for swift and conclusive forensics. This all-encompassing approach enables our analysts to quickly understand the full scope of an incident, significantly reducing the time and effort needed for investigations.



Maximize your CrowdStrike investment.

By correlating CrowdStrike Endpoint Security alerts with Varonis' unique data-centric alerts, MDDR analysts can identify threats that might go unnoticed with EDR telemetry alone. This integration maximizes the value of your existing EDR investments, providing a more robust and effective security solution.

TRY VARONIS FOR FREE.

See how our cloud-native solution covers all your data security needs.
Get started today at varonis.com/trial.