

Challenges



- Security Control failures is the #1 concern around cybersecurity for executives (Gartner 2021)
- An average customers make use of less than 25% of the security features and controls available to them and even fewer cross optimize security controls across their cyber security tools (Discern research)
- CISOs are looking to build dashboards that show the value of the investments they have made in market leading security platforms like the CrowdStrike Falcon Platform
- CISOs struggle to understand how mature their program really is and map to standards like MITRE

Solution



- Discern benchmarks the customer's deployment of the Falcon Platform and map its security controls to MITRE and other standards
- Discern provides suggestions and recommendations for hardening configurations of different security platforms for the customer
- Discern carries out closed loop policy automation to harden a customers security defenses
- Discern cross optimizes CrowdStrike Falcon controls with other major security platforms
- Discern acts as the policy brain for our customers and deliver policy as code

How does it work?



- Discern leverages CrowdStrike APIs to assess customers controls and identify white spaces
- Discern ingests CrowdStrike events to inform policies in other major security tools
- Discern ingests CrowdStrike events to build dashboards for the CISO on the progress of their security program, benchmarking successes and outcomes for additional reporting
- Discern ingests other security platform data and then uses the Falcon platform to further fortify customers

Use-Cases and outcomes



- Ensure full coverage security by driving the adoption of key CrowdStrike Falcon features, such as enabling real-time visibility, additional prevention policies, and device controls, including for high-risk devices and users.
- Help CrowdStrike customers assess their controls vs standards like MITRE and show progress over time
- Leverage the Falcon Platform's rich security data to change risk settings on other tools like Netskope, Mimecast etc.
- Become a policy suggestion engine to optimize existing security controls
- Automatically map and visualize Security controls vs. top standards including CIS, NIST, MITRE etc.

About Discern Security



Discern Security is the first AI based configuration management and recommendation engine. We help our customer get visibility into their security controls and harden them using AI.

About CrowdStrike



CrowdStrike Inc., a global cybersecurity leaders, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The Crowd Strike Falcon platform's single lightweight agent architecture leverages cloud-scale artificial intelligence and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph, CrowdStrike Falcon correlates over two trillion endpoint-related events per week in real time from across the globe, fueling one of the works most advanced platforms for security.

