Data Sheet

CrowdStrike and Cado Security: Accelerated Forensics and Incident Response

Augment incident investigations with forensic-level context

Key Benefits

Respond Faster

Automate the end-to-end incident response process — from data collection and processing to analysis — accelerating response times.

Add Depth to Your Investigation

Gain immediate access to forensic evidence and key incident details using CrowdStrike Falcon® Real Time Response (RTR), including root cause and scope.

Simplify Forensic Analysis

Eliminate tedious investigative tasks and get the answers you need without using complex scripting and queries.

Get Comprehensive Coverage

Perform forensic investigations across your entire environment, whether on-premises, in the cloud or in a hybrid environment.

Challenges

Once you've identified malicious activity, the clock starts ticking. The business needs answers fast, and in many cases, you need to perform a deep-dive investigation leveraging forensic data to understand the true root cause and scope of an incident and mitigate damage. However, gaining access and collecting all of the data and forensic insights you need to effectively understand what happened can be an extremely time-consuming manual process.

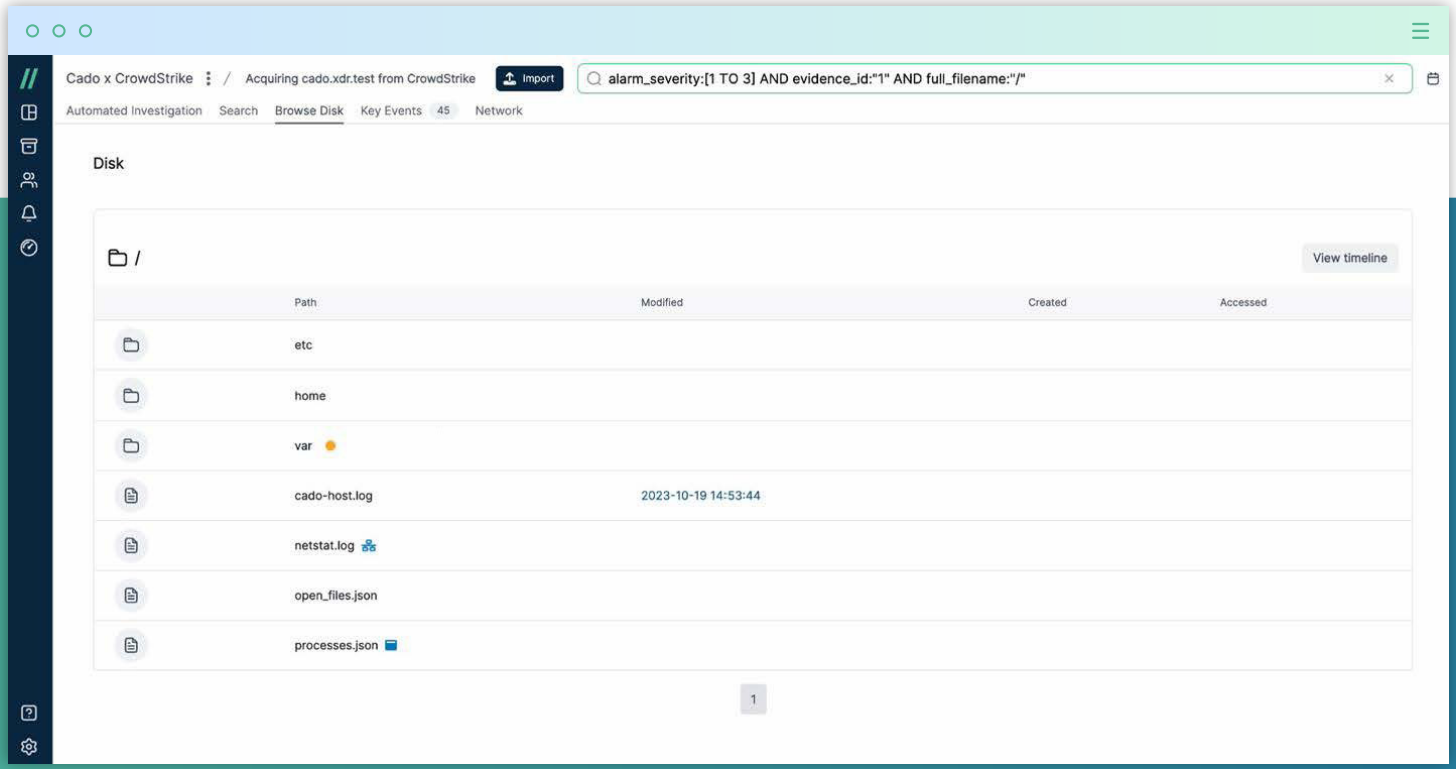
Solution

Powered by data from the CrowdStrike Falcon® platform, Cado Security automates forensic data collection and analysis for impacted systems, empowering security teams to rapidly perform in-depth forensic investigations and minimize time to respond. When it comes to attack containment, time is of the essence. Augment your real-time threat detection platform with forensic-level detail and context from CrowdStrike and Cado Security to identify root cause, understand the impact of incidents and respond faster.

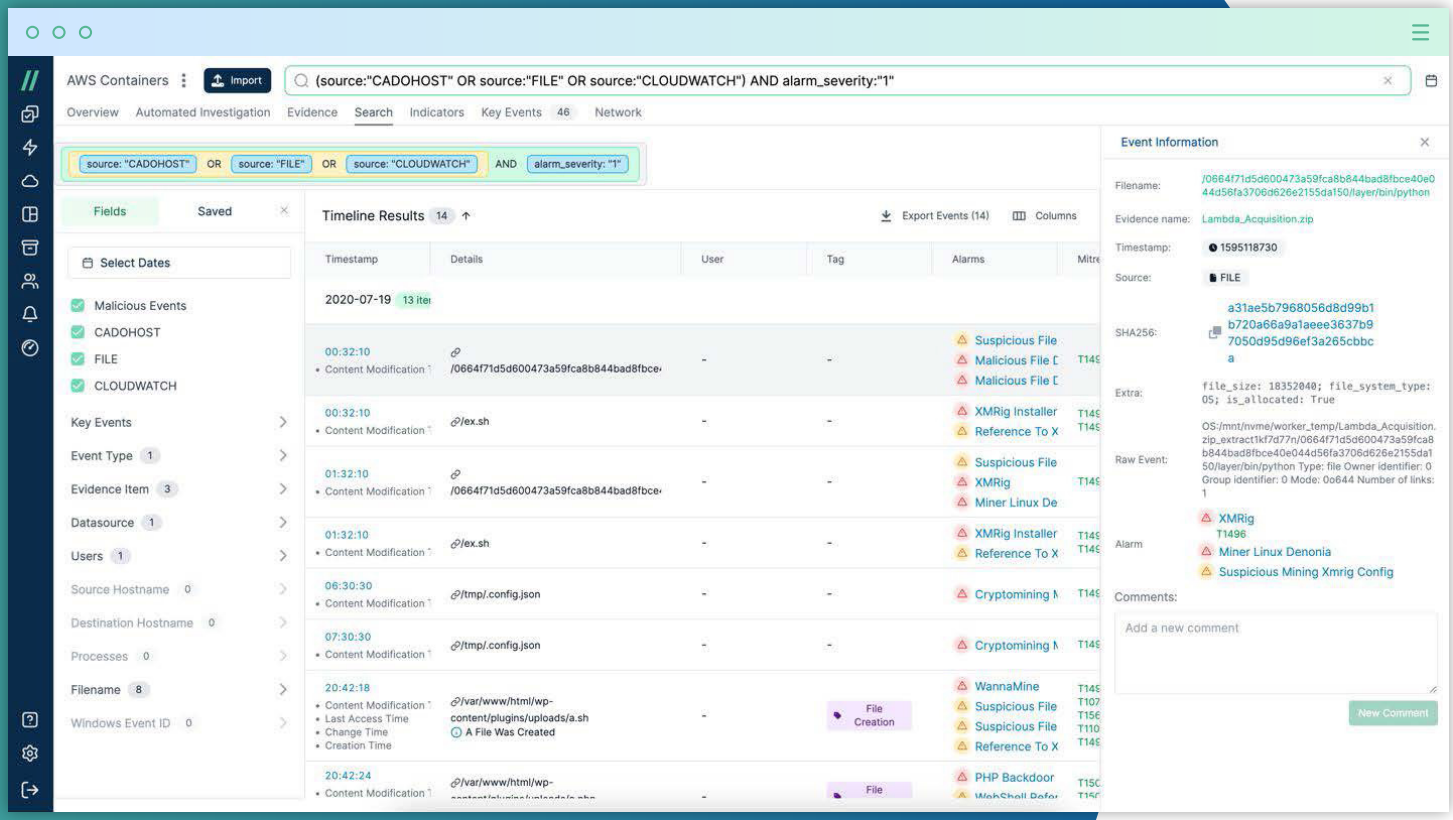
Technical Solution

By leveraging the scale, speed and automation of the cloud, the Cado platform enables security teams to get to the root cause of incidents and respond faster. Once malicious activity is detected by the Falcon platform, Cado leverages Falcon RTR capabilities to automatically collect and analyze forensic data from the organization's impacted systems, enabling security teams to rapidly perform root cause analysis and identify scope and impact for accelerated incident response. This package of collected forensic and contextual data includes:

- All system logs, including application and authentication logs
- Master File Table to understand what files were where in the system
- Configuration files and registry to show how the system was set up
- Volatile data at the time of capture, including data about running processes and memory of running processes
- Web histories to understand which web URLs were accessed
- Active network connections



The Cado platform enriches collected data from the Falcon platform using machine learning and threat intelligence to automatically present key malicious events and affected assets so analysts can rapidly understand incident scope and impact. Cado delivers a complete timeline of events and advanced search capabilities, allowing security teams to easily pivot their investigation and dive as deep into the dataset as required.



The Cado platform does not use a running agent — instead, Cado deploys a dissolvable agent to rapidly collect essential data about what has occurred across the systems of interest. This could be in the event of an incident or for threat hunting purposes. This unique approach also means security teams can gain deep visibility even on machines where the CrowdStrike Falcon agent is not actively running or where an incident occurred before the Falcon agent was deployed.

"The integration between CrowdStrike and Cado Security empowers security teams with the comprehensive capabilities required to quickly identify, analyze and address incidents, setting a new standard for speed and effectiveness."

— Chris Doman, CTO & Co-Founder of Cado Security

Key Capabilities

Automated Forensic Data Capture
Get immediate access to forensic evidence and key incident details across systems of interest.

Broad Coverage
Seamlessly investigate incidents that span cloud, container and on-premises environments.

Expanded Threat Hunting
Incorporate forensic-level detail into your threat hunting practice.

Real-Time and Historical Context
Gain visibility into everything that has occurred on a system since it was installed.

CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

CADO

Cado Security is the provider of the first cloud forensics and incident response platform. By leveraging the scale and speed of the cloud, the Cado platform automates forensic-level data capture and processing across cloud, container and serverless environments. Only Cado empowers security teams to respond at cloud speed. Backed by Eurazeo, Blossom Capital and Ten Eleven Ventures, Cado Security has offices in the United States and United Kingdom. For more information, please visit www.cadosecurity.com or follow us on Twitter @cadosecurity.