Case Study

Security

IT@Intel: Advancing Intel's Security Posture Through Partnership & Innovation with CrowdStrike

CrowdStrike and the CrowdStrike Falcon® platform are critical to Intel Information Security. As a strategic supplier and innovation partner, CrowdStrike helps advance our mission "to make it safe for Intel to go fast."

Intel IT Authors

Mitch Baskette
Endpoint Security Architect

Ted Mahar
Global Cyber Response Manager

Jac Noel
Security Solutions Architect, Principal Engineer

Elaine Rainbolt
Industry Engagement Manager

Carl Walters
Product Owner Endpoint Security

Executive Summary

The Intel Information Security (InfoSec) team continuously adds to our defense-in-depth capabilities. With a global workforce using over 171,000 client endpoints, the team is constantly looking for ways to prevent, detect, and respond to emerging sophisticated threats. Improving our security posture became even more challenging as the COVID-19 pandemic accelerated edge and hybrid business requirements. Employees now work from anywhere, anytime, and may disconnect from the Intel network for days, weeks, or more. We needed more modern tools to fulfill our mission to "make it safe for Intel to go fast."

To help us achieve our mission, we engaged CrowdStrike and their Crowdstrike Falcon platform approximately three years ago. CrowdStrike's advanced endpoint detection and response (EDR) and cloud-native next-generation antivirus (AV) capabilities met our needs with one lightweight agent that leverages the speed of CrowdStrike's unified platform. Next, they brought additional value with CrowdStrike Falcon Spotlight's vulnerability assessment, the CrowdStrike Falcon Overwatch 24/7 proactive threat hunting service, and the CrowdStrike Falcon Device Control module (see Figure 1).

> We want the technology to work for us. Not us working for the technology. Crowdstrike provides solutions that work.
>
> Brent Conran, Chief Information Security Officer, Intel

The CrowdStrike Falcon platform ingests and correlates data from thousands of customers and millions of endpoints to help reduce Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to continuous threats. As CrowdStrike continues to innovate, we continue to see value. A recent innovation is Advanced Memory Scanning (AMS), based on Intel® Threat Detection Technology (Intel® TDT), a feature of 6th gen and newer Intel® Core™ processors and Intel vPro™ platform processors. AMS can help detect and prevent cyberthreats such as fileless attacks, which can evade other threat indicators by hiding in memory.

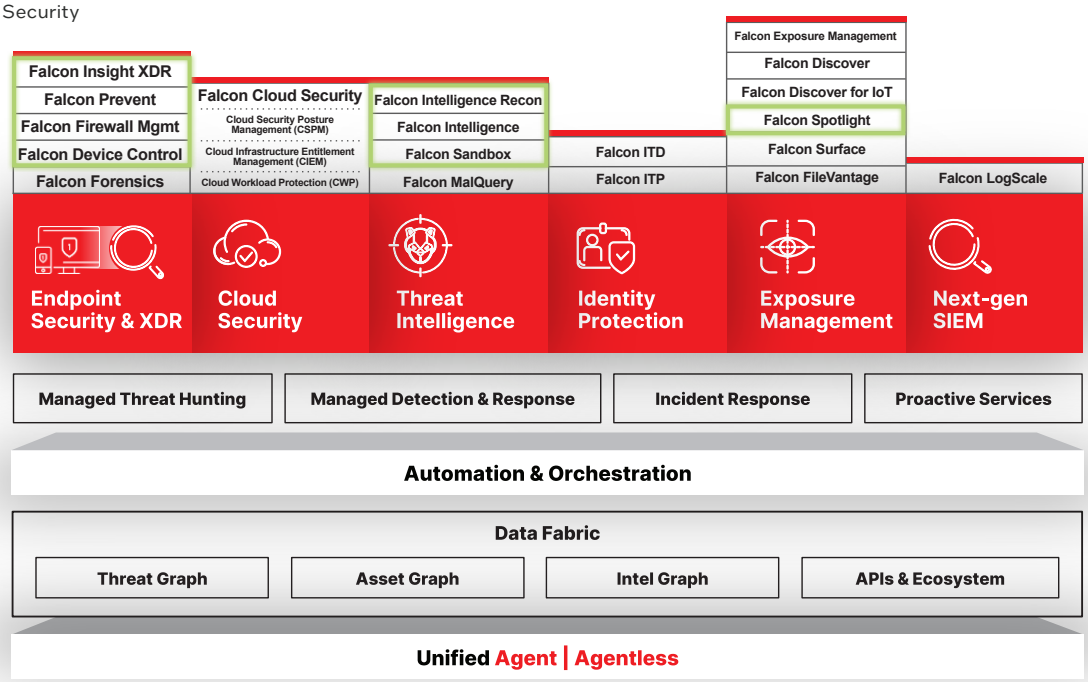

Figure 1. The CrowdStrike Falcon platform is a cloud-native security platform with unified modules and a single light-weight agent. Intel currently licenses the modules outlined in green.

Our Endpoint Security Challenge

Intel needed better cybersecurity capabilities that could scale to support a company with over 171,000 client endpoints. Our legacy host security solution stack had many agents that impacted client performance, creating a poor user experience. The solution also required on-premises resources and had significant scaling challenges. We had to create multiple management clusters: one for the Americas region; one for Europe, Middle East & Africa (EMEA); one for Asia Pacific (APAC); and more clusters for other segments. Beyond that, we had very little orchestration or integration among the clusters. If something happened in the Americas Region, we would have to pivot to investigate all other regions, serially. It was a time-consuming and sub-optimal process.

When the pandemic hit, remote work became the norm for many employees. That meant a typical client endpoint was not connected to Intel's corporate network for days or weeks. Because our legacy EDR/AV capability was on-premise, off-network systems were essentially "dark" to us. As the hybrid work security challenges suddenly emerged, we continued to face rapidly advancing threats from evolving methods of attack and post-exploit activities.

Intel's Endpoint Security Requirements

Intel's endpoint cybersecurity requirements begin with performant capabilities designed to scale. They must work as seamlessly as possible in concert with the rest of Intel's IT infrastructure, applications, and operations.

Intel requires modern, agile security capabilities to support new, hybrid work environments, larger attack surfaces, and data on-premises and in multiple clouds from software as a service (SaaS) suppliers and public cloud service providers (CSPs). Our security capabilities must excel at helping our cybersecurity team prevent the majority of threats (99%), freeing our responders to focus on the most sophisticated 1% of advanced threats as they continue to evolve.

Dual-use Tools Pose a Growing Threat

Dual-use threats include tools and technologies employed for both legitimate and malicious purposes. These threats pose a challenge for cybersecurity because they can evade detection by antivirus software or security policies that only block known malware.

For example, Cobalt Strike is a commercial penetration testing tool that can assess the security of networks and systems. It is used to identify and exploit vulnerabilities and emulate advanced persistent threats (APTs). However, hackers can also use it to launch stealthy attacks, establish covert channels, and execute malicious payloads.

APT attackers have used Cobalt Strike with Dynamic Link Library (DLL) hijacking to connect to a company's VPN. That type of DLL side-loading is an example of a dual-use threat that takes advantage of Windows libraries that are shared by different programs. DLL side-loading occurs when a malicious DLL file is placed in the same directory as a legitimate program, and the program loads it instead of the original DLL file. This way, the hacker can execute their payload without raising suspicion or triggering alerts.

Leveraging the CrowdStrike Falcon platform, administrators can utilize the prevention policies screen to implement dual-use cases where Hardware Enhanced Exploit Detection-based indicators of attack (IOAs) trigger AMS to help uncover stealthy, two-stage attacks such as Cobalt Strike that might deploy a secondary ransomware payload.

Our security capabilities must continue to evolve to get better at prevent and reduce MTTD and MTTR to advanced cyberthreats. They must identify indicators of attack (IOAs) and reactive indicators of compromise (IOCs). Proactive IOAs can prevent and detect threats earlier in the kill chain, sophisticated zero-day exploits, and APTs.

Finally, we want Intel's security vendors to align to our vision and take advantage of the value of frameworks such those from the National Institute of Standards and Technology (NIST) and MITRE. These frameworks help provide a comprehensive way to assess our environment, and the research that goes into them helps us identify vendors that can best help us meet our information security needs.

CrowdStrike's Solution

We were drawn to CrowdStrike as they offered a cloud-native solution with advanced EDR. The CrowdStrike Falcon platform is an always-on solution, and its scalable, cloud-native operation also meant we could get out of the business of running and managing our own clusters. In addition, the CrowdStrike Falcon platform operates with only one lightweight agent on the endpoint.

Our proof of concept successfully demonstrated the CrowdStrike Falcon platform EDR/NGAV capabilities enabled us to quickly identify, contain, and remediate threats. The CrowdStrike Falcon platform uses automated workflows, real-time response actions, and remote forensic capabilities. It provides behavioral analysis, exploit prevention, machine learning, and proactive IOA-based threat prevention. Each IOA focuses on detecting the intent of what an attacker is trying to accomplish, regardless of the malware or exploits used. We also discovered that the CrowdStrike Falcon platform has APIs that could allow us to integrate telemetry data into our cyber data lake which is the heart of our Cyber Intelligence Platform (CIP).

With the spike in employees operating from remote/hybrid work environments, we needed much better visibility into endpoints operating outside the corporate network. The Falcon Spotlight vulnerability management capability gave us a comprehensive view of all our endpoints across all regions, and it combined our telemetry with telemetry from other CrowdStrike customers, all with the speed and agility of the cloud. Falcon Spotlight now helps our InfoSec team prioritize remediation efforts based on risk scores, exploitability, and exposure analysis.

CrowdStrike continues to deliver value with other modules that work using the same lightweight agent. For example, we engaged the CrowdStrike Falcon Overwatch service for 24/7 proactive threat hunting by their expert analysts. Using advanced techniques such as machine learning, behavioral analysis, and human intelligence, Falcon Overwatch helps us detect stealthy adversaries that may evade other security solutions.

We also licensed the CrowdStrike Falcon Device Control feature of Falcon Discover to monitor and control USB devices connected to endpoints. CrowdStrike Falcon Device Control helps prevent data loss, malware infection, and unauthorized access by enforcing granular policies based on device type, vendor ID, serial number, or encryption status.

Security Frameworks Deliver Real Value for Threat Hunting

Security frameworks such as those from NIST and MITRE provide organizations with effective ways to close the skills gap and improve business resiliency against cyberattacks. With the ongoing cybersecurity skills shortage and the increasing frequency and sophistication of cyberattacks, the need for skilled cybersecurity workers is more apparent than ever.

For example, in 2022, the CrowdStrike Falcon platform was tested using the "MITRE ATT&CK Evaluations for Managed Services." The evaluation assesses the ability of a vendor's services to identify a sophisticated adversary with no prior knowledge of the attacker, emulating a real-world scenario. CrowdStrike achieved remarkable results, accurately and conclusively presenting visibility and supporting evidence across 75 of the 76 techniques in the evaluation.

These results demonstrate the combined power of the CrowdStrike Falcon platform and CrowdStrike Falcon Complete, which offers 24/7 protection. By natively integrating global adversary threat intelligence into its CrowdStrike Falcon platform, CrowdStrike enables rapid correlation of intelligence to behavioral telemetry, empowering threat hunters to stay one step ahead of an attacker. This critical context of objectives and tactics, techniques, and procedures (TTPs) provides threat hunters with the necessary tools to identify adversaries and stop breaches quickly and effectively.

> "In related CrowdStrike MITRE ATT&CK® Enterprise Evaluations, the Intel Threat Detection Technology hardware optimizations for Advanced Memory Scanning and Hardware Enhanced Exploit Detection provided a high-fidelity detection assist that helped confirm many CrowdStrike MITRE ATT&CK test detections."
>
> - Farid Hendi, Director of Product Management Crowdstrike

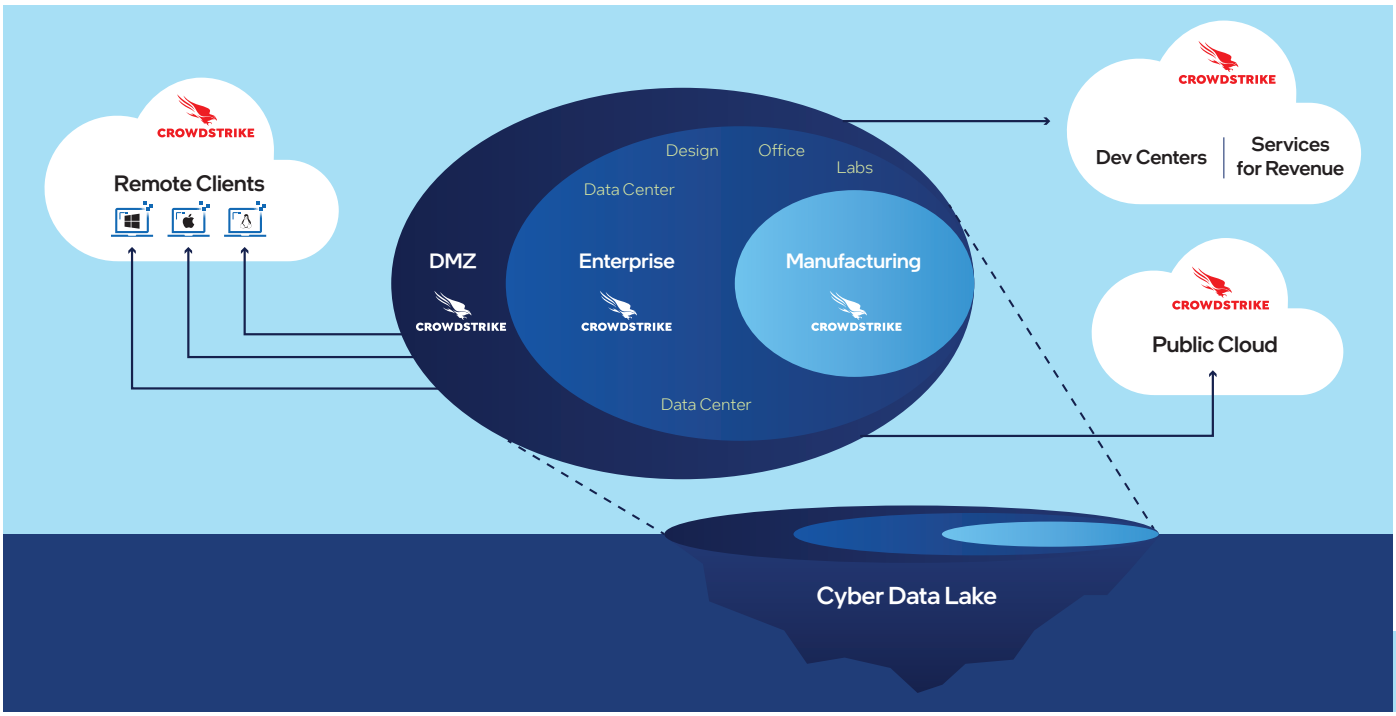

Figure 2. CrowdStrike collects telemetry from our multi-cloud and global on-premise environments then delivers it via Apache Kafka to our cyber data lake.

Deploying the CrowdStrike Falcon Platform

The CrowdStrike Falcon platform is a modular and extensible solution. Intel's security operations, including our Global Cyber Response, Vulnerability Management, Investigations and Forensics, and Threat Intelligence teams utilize the CrowdStrike Falcon platform's capabilities out of the box. The CrowdStrike Falcon agent is a key producer of data. It feeds data into our cyber data lake via Apache Kafka, where the data is filtered and joined with other IT and non-IT data. The combined data becomes even more powerful for security operations and provides value for other Intel teams such as Compliance, Risk Management, and Identity and Access management.

Our CIP receives the CrowdStrike telemetry via Kafka. This enables the InfoSec team to leverage CrowdStrike's industry-leading intelligence to provide proper security context. With its cloud-scale, near-real-time threat intelligence and seamless integration into our CIP, the CrowdStrike Falcon Platform continues to demonstrate tremendous value. We now see CrowdStrike as more than a strategic supplier. CrowdStrike is a key innovation and collaboration partner in our fight against cyber adversaries.

AMS: A New Threat Detection Capability

Attackers continue to evolve methods for exploit/initial access and post-exploit malicious activities. To gain initial access, attackers often co-opt legitimate code, re-using instructions already loaded in memory. According to Crowdstrike's 2023 Global Threat Report, 71% of endpoint cyberattacks in 2022 were malware-free. Such vulnerabilities open the door to APTs, ransomware, and prevalent dual-use tools like Cobalt Strike. These fileless attacks and APTs can evade modern attack indicators by hiding in memory.

71% of endpoint cyberattacks in 2022 were malware-free

To solve that problem, CrowdStrike and Intel co-engineered a new, advanced memory scanning (AMS) capability based on Intel TDT. This hardware-accelerated solution brings an important additional layer of defense against IOA. Through each stage of attack — initial access, execution, and even lateral movement — malicious actors can leave traces of their behaviors. With AMS, the Falcon sensor offloads the performance-intensive memory scans from the CPU to the Intel® Integrated GPU on 6th gen Intel® Core™ processors and newer. This allows the sensor to get ahead of the curve on fileless malware and other sophisticated attacks that may be hiding in memory.

Intel IT has enabled the CrowdStrike Falcon platform's AMS capability across our entire client fleet. AMS scans have been running and we have seen no consequential impact on system performance. In addition, CrowdStrike designed a fallback feature for Intel® Core™ processor-based systems older than 6th gen, enabling the AMS capability to run on the CPU in a performant manner.

Conclusion

Intel IT was challenged with the efficacy and management of our legacy EDR/AV solutions. These solutions required many agents and clusters of on-premises EDR data processing and storage. By the end of 2019, we determined that CrowdStrike, with its cloud native CrowdStrike Falcon platform and lightweight agent, met our needs for improved EDR and NGAV capabilities.

When the pandemic hit, employee laptops and mobile devices were often off the corporate network for days or weeks. CrowdStrike helped us solve this problem with their CrowdStrike Falcon Spotlight vulnerability assessment capability – again using the same lightweight agent together with the speed and scale of their cloud platform.

The CrowdStrike Falcon Platform continues to help Intel advance its security posture through other capabilities such as CrowdStrike Falcon Device Control, CrowdStrike Falcon Overwatch, and threat intelligence and reconnaissance capabilities. These all combine to help Intel reduce our MTTD and MTTR to sophisticated threats.

CrowdStrike and Intel continue to collaborate on innovative hardware-based security capabilities. AMS based on Intel TDT, is just one example of how Intel and CrowdStrike have partnered to deliver more effective security solutions for our customers.

Minimum Endpoint Requirements

Advanced Memory Scanning (AMS) requirements:

- Falcon sensor 6.45 or later with Memory Scanning enabled via prevention policy
- Windows 10 or newer
- 6th gen or newer Intel® Core™ processor-based PC platform

Hardware-Enhanced Exploit Detection (HEED) requirements:

- Falcon sensor 6.51 or later with Hardware-Enhanced Exploit Detection enabled via prevention policy
- Windows 10 or newer
- 6th gen or newer Intel® Core™ processor-based PC platform

For More Information

- Learn more about Intel IT best practices at https://intel.com/IT
- IT@Intel: Building a Modern, Scalable Cyber Intelligence Platform with Apache Kafka
  Our Apache Kafka data pipeline ingests tens of terabytes per day, providing in-stream processing for faster threat detection and response.
- Advanced Persistent Threats: Hunting the One Percent
  IT@Intel continues to evaluate new ways to reduce the signal-to-noise ratio and increase our ability to detect, isolate, and destroy APTs.
- Detect Threats Earlier with Hardware-assisted Security
  Intel and CrowdStrike collaborated to bring together our world-class technologies and expertise to co-engineer advanced threat detection and response capabilities.
- CrowdStrike | MITRE ATT&CK® Evaluations
  CrowdStrike Falcon® Complete managed detection and response (MDR) achieved the highest detection coverage in the 2022 MITRE Engenuity ATT&CK® Evaluations for Security Service Providers.