

PROCUREMENT OFFICER'S DETERMINATION  
Intergovernmental Cooperative Purchasing  
COMAR 21.05.09.04

Department/Procurement Agency: Department of General Services

Contract Term: Three Years

Amount: Estimated \$19,400,000

Category: Information Technology

Contract Type: Fixed Price

Name and address of selected Contractor: To be determined by issuing a request for quotation to the identified resellers under the Carahsoft Technology Corporation's OMNIA Contract Number R191902 resellers.

**Scope Description:**

Purchase the following CrowdStrike products/services:

- Crowstrike Falcon Complete with the following modules
  - Falcon Complete with Threat Graph Standard on Gov Cloud  
CS.FCSD.GOV.SOLN.T11.36M - 80,000 endpoints
  - Falcon Complete with Server Threat Graph Standard on Gov Cloud  
CS.FCSD.HPS.GOV.SOLN.T8.36M - 5,000 servers
  - Falcon for Mobile with Threat Graph Standard on Gov Cloud  
CS.FALMOBST.GOV.SOLN.36M - 15,000 mobile devices
  - Elite Support  
RR.HOS.ENT.ETLE.36M
  - Identity Threat Protection Complete Bundle  
CS.ITPC.GOV.SOLN.36M - 150,000 active identities
  - Falcon FileVantage - File Integrity Monitoring  
CS.FILEVANTAGE.SOLN.36M - 100,000 endpoints
  - Falcon Device Control - Visibility across USB device usage  
CS.DEVICE.SOLN.T13.36M - 80,000 endpoints
  - Falcon X Premium - Threat intelligence reporting and research  
CS.FALXPRESOLN.T14.36M - 100,000 endpoints
  - Falcon MalQuery - Malware Search Engine  
RR.IPM.ENT.5.36M
- University LMS Subscription New Customer Access Pass  
RR.PSO.ENT.NCAP.36M - 60 credits
- CrowdStrike University Training Credit  
NR.PSO.ENT.CRE.12M - 900 credit
- CrowdStrike Falcon Certification Program Exam Voucher  
NR.PSO.ENT.CPEV.12M - 300 credits

The 24/7/365 Security Operations Center (SOC) within the Office of Security Management (OSM) currently monitors approximately 30,000 endpoints through disparate Endpoint Detection and Response

(EDR) solutions and Antivirus products. The plan is to increase this to 100,000 endpoints over the next year. One of the thematic findings in the Statewide security assessments, which are now legislatively required to be performed by all units of State government at least every two years with results reported on, was a lack of consistently implemented, managed, and monitored endpoint protection tools, including EDR solutions. This lack of consistency across agencies creates a substantial risk for the State as a whole. By consolidating into a single platform and centralizing the management and oversight of EDR, the State can achieve economies of scale and improve security. The OSM expects many other units of State government to use this shared, consolidated platform. The CrowdStrike services include the capabilities itemized below the deployment which will allow OSM to achieve additional improvements in security:

- Security Analysts - 24x7x365, US-based, CJIS-cleared security analysts, focused on identifying real threats and adjusting tool settings to eliminate false positives.
- File Integrity Monitoring (FIM) - Detects unauthorized changes to critical system files. Modifying system files is a common tactic used in ransomware and other cybercrime.
- Identity Threat Protection - Get visibility into the active directory to identify shadow administrators, stale accounts, shared credentials, and other attack paths. Protect against and detect identity-based threats in real time without requiring the ingestion of log files. Improve AD hygiene with continuous monitoring for credential weakness, access deviations, and password compromises.
- USB device control - Reduces the likelihood of unauthorized USB storage devices being used to steal data or introduce unauthorized software into the environment.

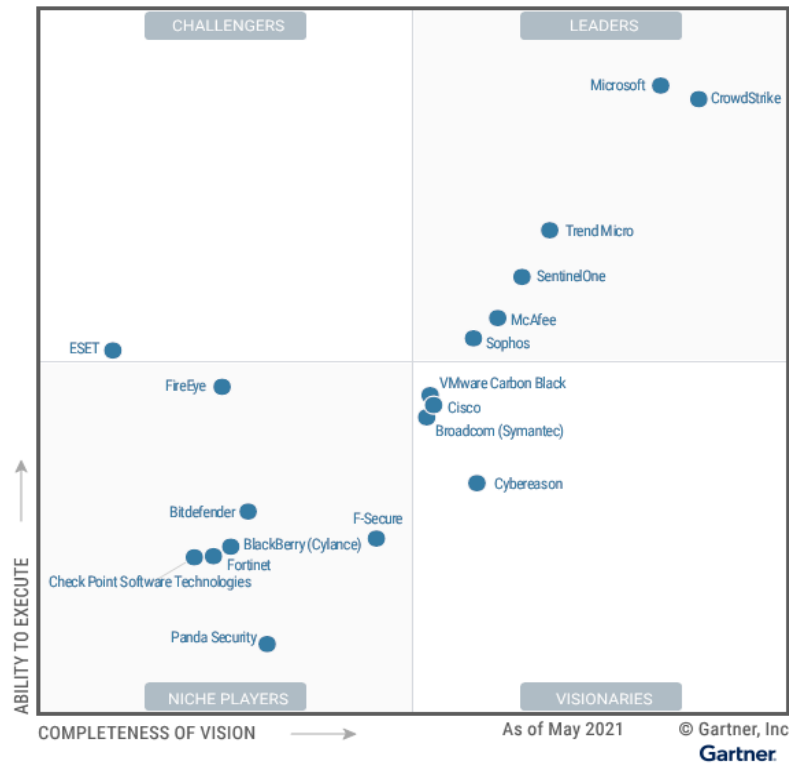
Additionally, for environments where the solution is deployed, CrowdStrike includes full forensic response services if a substantive cybersecurity incident occurs.

### **Basis for Selection:**

DoIT OSM's evaluation of EDR/EPP products focused on solutions identified by Gartner as Leaders in the "Magic Quadrant" against a list of functional and non-functional requirements based on the operational needs of the State enterprise. Among these requirements are:

- Endpoint Protection Platform (EPP)
- Endpoint Detection and Response (EDR)
- File Integrity Monitoring (FIM)
- Device control for USB hardware

The magic quadrant, in the upper-right corner below, identifies the vendors that provide a holistic vision for the market problem and have demonstrated the ability to provide a service aligned with that vision.



After an initial capability assessment, the OSM team determined that the only two solutions that could potentially provide the requisite functionality were CrowdStrike and Microsoft. The principal limitations that excluded other vendors were:

- Lack of integration with existing cybersecurity infrastructure (e.g., bi-directional Threat Intelligence Platform integration, File Integrity Monitoring).
- The product only offers a single-tenant environment.
- The solution did not offer co-managed capabilities.

This evaluation, between November 2021 and July 2022, included independent research, a series of product demonstrations and meetings with each vendor, and limited access to the platforms to evaluate capabilities and ease of use. Evaluation criteria and required features were developed by the OSM based on the current and projected future needs of the team and to satisfy the reporting requirements being developed to support the Maryland Chief Information Security Officer. This evaluation was supported by an independent third-party review, conducted by RSMUS, on the approach and methodology that supported the conclusions of the internal evaluation.

The most significant limitations of the Microsoft solution for our use case are:

- **Complexity** – Microsoft lacks a consolidated solution to meet our needs, requiring the use of several tools (e.g., SCCM, Sentinel, AzureAD, InTune, and Defender ATP) to achieve the same objectives across a smaller number of assets. Specifically, Microsoft is disruptive to business processes during update, impact business operations with load, and relies on OEM for non-Microsoft OS support
- **Flexibility** -The multi-tenancy capabilities of the toolset did not provide all capabilities and granular support when compared to the other solution, including:
  - Self-service provisioning for new tenants visible and managed by the parent

- The parent tenant has the ability to customize the modules/features available for each child
- True parent/child policy relationship allows for streamlined policy propagation across all tenants
- Role-based access for child tenants allows for flexibility in policy management to affect only their endpoints
- Child tenant data and policies are restricted to that tenant but can be viewed and managed by the parent
- **Protection** – The evaluation identified several areas of concern around functional deficiencies based on license types (e.g., capability differences between operating systems that would severely inhibit response capabilities, such as an inability to conduct live response on many versions of Windows that are still in use across the State). The complexity of this problem is exacerbated by the number of feature differences between operating systems and versions, creating inconsistencies in the protective and response capabilities.
- **Platform** - The evaluation identified a lack of feature-parity across OSs, primarily due to the requirement to use multiple tools for functionality beyond the pure EPP/EDR features.
- **Pricing** – Because agencies across the State have different Microsoft licenses, the cost to deploy a consistent toolset would require the purchase of unneeded licenses to gain consistency across the environment.

CrowdStrike’s Falcon platform includes an EDR product focusing on detection and response capabilities to identify and remediate advanced threats and file-based malware prevention, exploiting static and behavioral ML to protect against known threats. Additionally, CrowdStrike’s continued investment in additional features has introduced advanced firewall management and mobile device protection options. CrowdStrike Falcon provides all core EPP capabilities in a single agent, with low resource utilization and a storefront for add-on third-party solutions. An easy-to-use management console and simplified deployment experience add to the high rating for market understanding and innovation. CrowdStrike has a strong reputation in the market as the single solution for endpoint security for organizations looking to consolidate their EPP and EDR agents/solutions. Falcon X threat intelligence and Threat Graph cloud-based data analytics can detect advanced threats and analyze user and device data to spot anomalous activity. CrowdStrike has a customer base that attackers highly target. As a result, it has consistently adapted early to shifts in attack techniques. It achieved positive results in the MITRE Phase 2 evaluations with consistent identification of tactics and techniques.

The CrowdStrike Falcon Complete solution, with the modules described above, provides the following capabilities that are critical for protecting our environments:

- Full feature sets across a wide variety of platforms, including:
  - Mobile devices (iPhone and Android)
  - Windows
  - Linux
  - Mac
- Integration with our core security platforms, including:
  - ServiceNow
  - Splunk
  - Anomali
  - Recorded Future
  - Palo Alto networks
- Incident Response capabilities in the event that an incident occurs.
- Protection of IT assets and centralized logging, even when assets are not connected to the State’s network.

Within the State's DoIT Enterprise environment, the transition to CrowdStrike would result in some level of cost recovery, by eliminating the need to deploy several enterprise tools, including:

- Lookout
- Tanium Threat
- McAfee Antivirus

Additionally, for agencies not currently using the DoIT Enterprise security services, such as MDH, the need for products in the following categories would be eliminated:

- Antivirus Solutions
- Mobile Device AV
- EPP/EDR
- Device Control software

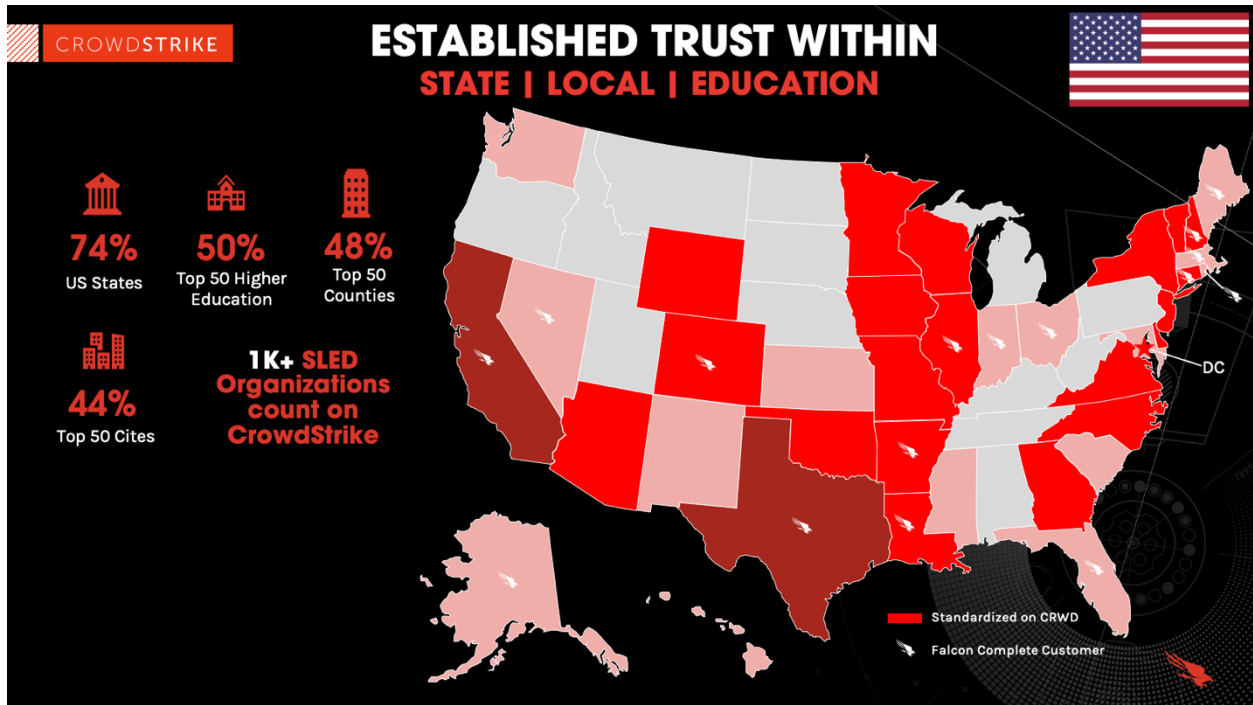
Due to the complexity of a cost comparison, and the potential cost of a major breach, a comprehensive analysis of the cost recovery from this initiative has not been performed. DOITsteam of cybersecurity experts believe that the costs transferred from other products to this platform for agencies with all of these capabilities, combined with the risk-inferred costs associated with agencies that do not have these capabilities would result in a net cost saving for the State. This centralization of cybersecurity capabilities aligns with the legislation passed earlier this year.

Lastly, the implementation and centralized management of the solution capabilities is quickly becoming a mandatory requirement for cybersecurity insurance carriers and impacts other financial instruments, such as bond ratings. Maryland's Cybersecurity team agrees with a report from Moody's indicating that the NIST cybersecurity framework (NIST CSF) is an appropriate mechanism to measure cybersecurity risk and adopting these measures in Maryland is an appropriate risk mitigation practice. By continuing the investment in cybersecurity, the State is better positioned to maintain its AAA bond rating, which has a significant financial impact on the State.

### **Pricing Comparison:**

As stated in our Basis for Selection we have conducted our evaluation on cost as well. With Microsoft's complex bundles and additional costs highlighted earlier the ongoing costs to support their multiple platforms and the need to support additional vendor platforms to achieve our goals are not cost-effective for the State.

The CrowdStrike Falcon Complete offering is a managed detection and response (MDR) service that combines the effectiveness of the cloud-native Falcon endpoint protection platform with the efficiency of a dedicated team of security professionals, hence eliminating "soft" costs and providing DoIT greater value. This is crucial in defending against current and future threats which demands diligent monitoring by skilled staff, equipped to investigate and remediate threats at scale. It allows us to deploy a comprehensive security program that is sufficiently staffed 24/7/365 by security experts and offers us a [Breach Warranty](#), helping Maryland maintain its AAA bond rating. CrowdStrike Falcon Complete is a proven, turnkey solution that delivers a comprehensive, mature endpoint security program and measurable outcomes that Microsoft simply cannot provide.



The use of this procurement method will reduce the time period between need determination and delivery of the solution; will ensure an expedient time to value for the State of Maryland; and reduce the administrative burden on DGS. OMNIA Partners is the nation’s largest and most experienced cooperative purchasing organization for the public sector. Additionally, all contracts available through OMNIA Partners are competitively solicited and publicly awarded by a lead agency, using a competitive solicitation process consistent with applicable procurement laws and regulations. In accordance with COMAR 21.05.09.04, it is determined that this ICPA will provide cost benefits to the State, will promote administration efficiencies, and promote intergovernmental cooperation. The ICPA in the best interest of the State and is not intended to evade the purpose of Division II of the State Finance Procurement Article.

Determination By:

*Susan Howells*

\_\_\_\_\_

DoIT, Procurement Officer

Date: October 3, 2022

Approved by:

*Michael Leaky*

\_\_\_\_\_

DoIT, Secretary (or designee)

Date: Oct 3, 2022

Approved by:

*M. Z...*

\_\_\_\_\_

DGS Chief Procurement Officer

Date: Oct 4, 2022






# POD ICPA - Crowdstrike Falcon 10.3.22 Final

Final Audit Report

2022-10-03

Created:	2022-10-03
By:	maria fisher (maria.fisher2@maryland.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAIEfhpRxENCpt6Bi7J9RfhC5L7pW0_v24

## "POD ICPA - Crowdstrike Falcon 10.3.22 Final" History

-  Document created by maria fisher (maria.fisher2@maryland.gov)  
2022-10-03 - 12:30:10 PM GMT
-  Document emailed to Michael Leahy (michael.leahy@maryland.gov) for signature  
2022-10-03 - 12:31:07 PM GMT
-  Email viewed by Michael Leahy (michael.leahy@maryland.gov)  
2022-10-03 - 12:47:21 PM GMT
-  Document e-signed by Michael Leahy (michael.leahy@maryland.gov)  
Signature Date: 2022-10-03 - 12:48:21 PM GMT - Time Source: server
-  Agreement completed.  
2022-10-03 - 12:48:21 PM GMT