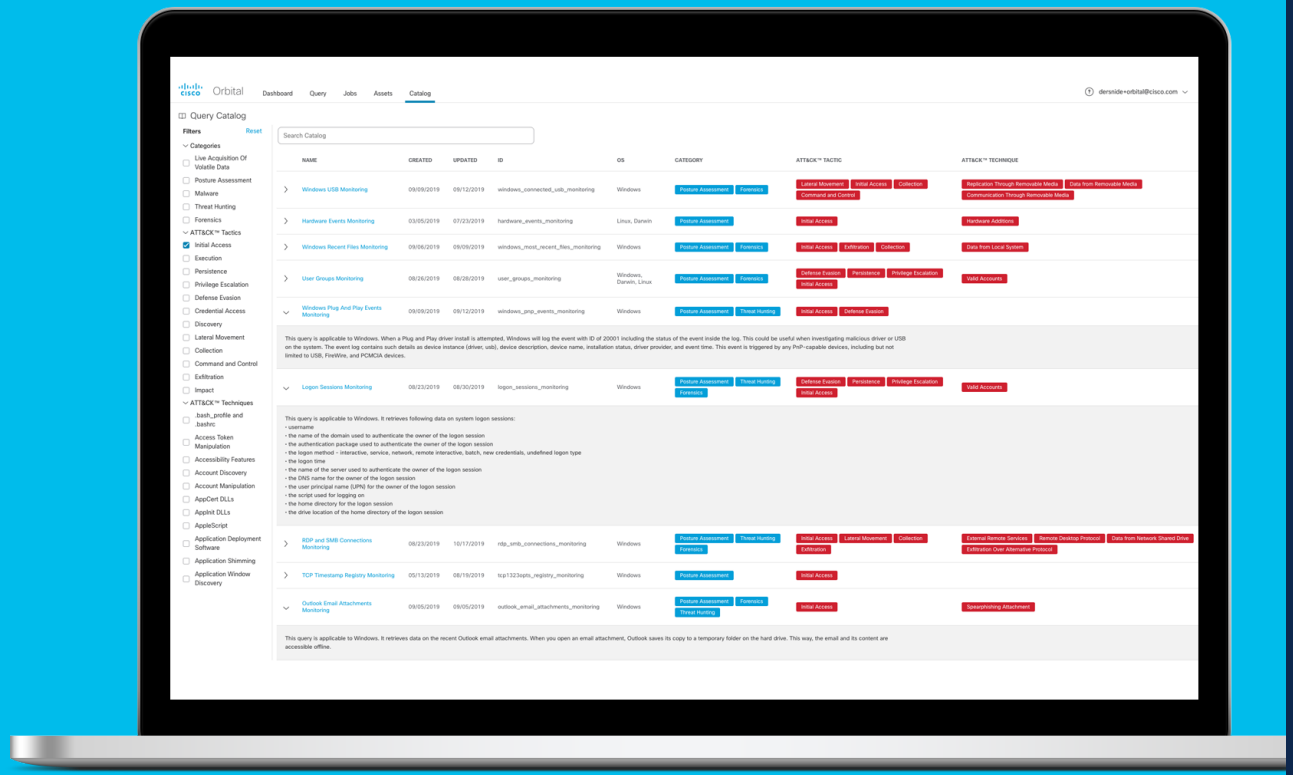
Cisco AMP for Endpoints

Know everything. About every endpoint. Right now.



What is Orbital Advanced Search?

Orbital Advanced Search is a new advanced capability in Cisco AMP for Endpoints designed to make security investigation and threat hunting simple by providing over a hundred pre-canned queries, allowing you to quickly run complex queries on any or all endpoints. This enables you to gain deeper visibility on what happened to any endpoint at any given time by taking a snapshot of its current state. Whether you are doing an investigation as part of incident response, threat hunting, IT operations, or vulnerability and compliance, we get you the answers you need about your endpoints fast.

What challenges can you help address?

Dealing with a data breach can put many strains on your security team – even more so when they are already reeling from talent shortage. Faced with an incident, they now have to spend copious amount of time investigating the problem. With malicious attacks from malware and other perpetrators as the major root cause of a breach, they often find it difficult to address these more evasive threats. But as traditional antivirus falls short in protecting your endpoints, one thing is clear, today's modern malware requires modern defenses. And we can help with that by getting all the information you need from your endpoints, allowing you to stop breaches and attacks fast.

What business value can I gain from this capability?

We help you get the information you need in near real time to investigate and respond to threats quickly and confidently. As a result, we can help shrink the lifecycle of an incident or a data breach that you may be dealing with – mitigating any or further damaging cost of the breach to your business.

How does it work?

Whether you are investigating an incident or hunting for threats we can help you simplify and accelerate these tedious processes in the following ways:

1. **Forensics snapshots.** We can capture a snapshot of data from an endpoint such as running processes, open network ports and a lot more at the time of detection or on demand. You can think about it as a "freeze framing activity" on an endpoint right to the moment when something malicious was seen. This allows you to know exactly what was happening on your endpoint at that point in time.
2. **Live search.** We can run complex queries on your endpoints for threat indicators on demand or on a schedule, capturing the information you need about your endpoints in near real time.
3. **Predefined and customizable queries.** We provide over a hundred predefined queries that you can quickly run as they are or easily customized as needed. These queries are simply organized in a catalog of common use cases and mapped to the Mitre ATT&CK.
4. **Storage options.** The results of your queries can be stored in the cloud or sent to other applications such as Cisco Threat Response for further or future investigations.

What are the common use cases for this capability?

With Orbital Advanced Search, we can help you do the following important tasks better, faster:

- **Threat Hunting.** Search for malicious artifacts in near real-time to accelerate your hunt for threats.
- **Incident Investigation.** Get to the root cause of the incident fast, accelerating remediation.
- **IT Operations.** Simply track disk space, memory, and other IT operations artifacts.
- **Vulnerability and Compliance.** Quickly check the status of Operating Systems for things like versions and patch updates, ensuring your endpoints are in compliance with current policies.

1965868 10/2019