Remediate Faster With Velociraptor

The Leading Open-Source Digital Forensics and Incident Response (DFIR) Framework

Security practitioners spend countless hours hunting, investigating, and remediating increasingly elusive threats, yet often find themselves one step behind the bad guys. When potential breaches are not addressed and eradicated at their roots, they find the fuel needed to grow and morph into incidents and attacks that can pose significant risk to an organization.

> **Nearly 70% of companies that are breached are likely to get breached again within 12 months.**
>
> CPO

Velociraptor is the world's leading open-source DFIR framework and part of Rapid7's renowned cybersecurity open-source and intelligence community. Providing advanced endpoint monitoring, hunting, digital forensics, and cyber response, Velociraptor empowers users to collect, query, and track any and every aspect of a specific endpoint, groups of endpoints, or even an entire network.

Deep Forensics for Expedited Investigations and Incident Response

Velociraptor's powerful forensics visibility supports investigation use cases across endpoint ecosystems, enabling users to leverage critical functionality in three key areas:

Collection: Quickly deep dive and collect targeted digital forensic evidence simultaneously across all endpoints. With Velociraptor, you can surgically reconstruct attacker activities through digital forensic analysis so you know exactly what was impacted by an attack. See everything and efficiently gather the specific data you need from a single endpoint or across the entire fleet to understand the impact and scope of an incident and inform response actions.

Security Challenges

- Inefficient processes for collecting data on endpoints
- Difficult to continuously and accurately identify specific activity across ecosystem
- Hard to hunt for suspicious activity and identify all affected assets with limited forensics

> **We love Velociraptor, especially how once unleashed, it can quickly find and neutralize an APT (Advanced Persistent Threat). It makes you appreciate just how strong and effective it is. It truly is like the velociraptor in Jurassic Park… aggressive and intelligent.**
>
> Mike Cooley
>
> Vice President and Chief Information Officer
>
> Crown Automotive

Monitoring: Continuously query the endpoint for specific activity in event logs, file modifications, process execution, and more; then send matches to the server for analysis. Interrogate anything on any endpoint, triggering queries with questions specifically related to your environment. Continuous monitoring ensures you will be instantly alerted whenever and wherever any malicious activity matches your specified criteria.

Hunting: Actively search everywhere for suspicious activity using a library of forensic artifacts. Link together multiple digital forensic capabilities for a customized investigation and situational approach to threat hunting. Powerful automation enables holistic hunting for suspicious activity and compromised machines across the network. Leverage proven artifacts and playbooks for threat containment and eradication to respond and recover faster.

Sample Scenario: Critical Vulnerability on the Loose

Moving From Advisory to Detection to Remediation in Minutes

A critical advisory is released regarding a CVE (Common Vulnerability and Exposure) that's highly vulnerable to attack. Millions of systems/machines are at risk. Organizations need to check all their endpoints to determine if and where the vulnerability is present.

In steps Velociraptor to the rescue, launching an "everywhere hunt." With no dependence on logs or telemetry previously sent to cloud storage, Velociraptor queries endpoints for artifacts that indicate the vulnerable software is present. This search can target a single endpoint or an entire fleet of endpoints to quickly identify all affected assets. This same process can be repeated on the affected assets to check for evidence that the vulnerability was exploited. Since most of the processing is done on the endpoint, this all happens lightning fast. Scans take only a few minutes. Crisis averted.

Field tested by our elite Incident Response experts

The Rapid7 Incident Response (IR) team deploys Velociraptor for ***every*** customer engagement. Velociraptor's deep-dive forensic capabilities enable the Rapid7 IR team to fully scope, contain, and eradicate threat actors from environments faster than ever before. With superior visibility, the team is able to execute an advanced hunt in the heat of a developing incident and move quickly to mitigate the threat. Combined with truly unlimited incident response, Rapid7 Managed Threat Complete customers can have confidence that incidents are resolved quickly and that their environment is stronger and more resilient.

Learn More

Interested in learning more about Velociraptor?
Check out the Velociraptor Blog.
Join the discussion in https://www.velocidex.com/discord.
Join the mailing list velociraptor-discuss@googlegroups.com.

> **Velociraptor is a fantastic endpoint detection and response utility. It's beautiful; it's clean; it's super sweet.**
>
> John Hammond
>
> Cybersecurity Researcher/
> Content Creator
>
> Hunt for Hackers With Velociraptor