McAfee MVISION Insights

The first endpoint to extended detection and response (XDR) security capability to help you get ahead of adversaries

The evolution and pace of cyberthreats are a constant menace and stress point for organizations. Enterprises have reacted by increasing security budgets amid a shortage of security expertise, but they still can't keep up with modern adversaries who are constantly updating their arsenal of tools, tactics, and techniques. The current options are siloed intelligence requiring human and manual intervention. These may address immediate threats, but the increasing numbers and nuances of cyberattacks are bombarding security teams into a seemingly constant reactive posture. A threat intelligence platform (TIP) can offer a large data lake of threats, but this requires manual integration and analyst cycles, producing limited actionability and remediation. Vulnerability management can advise on existing vulnerabilities and their severity but offers limited threat insight into how your security posture can or cannot defend against real-world current threats.

The solution is McAfee® MVISION Insights, with real-time intelligence that empowers proactive action. Comprehensive intelligence that has been distilled and analyzed by artificial intelligence and humans can provide prioritization into which threats and campaigns are most likely to target your organization. MVISION Insights predicts exactly how a threat would impact your overall security, as well as exactly prescribe what you need to do to optimize your security stance.

Key Benefits

- **Risk intelligence gathered from one billion sensors:** Proactively identify threat projects outside your perimeter from a trusted source. Prioritize threat projects according to industry verticals, geography, threat actors, and your enterprise security posture.
- **Identify threat campaigns prior to an attack and prioritize your risk level from a single console:** Gain actionable intelligence on a threat and how your endpoint security posture will stack up against it, including remediation recommendations.
- **Reduce mean time to detection and resolution:** Streamline workflows to accelerate additional safeguards. Assess your current endpoint and cloud security posture with required actionable changes and speed response time from months to hours.

Connect With Us

Transform Your Security So You Can Be More Proactive

MVISION Insights offers capabilities built into the McAfee® management platform experience that uniquely align with and streamline risk and threat operations to preemptively improve defensive countermeasures and accelerate response times while using fewer resources. Risk intelligence gathered and refined from one billion sensors assessed by proven advanced threat researchers empowers your enterprise with the insight it needs to prioritize defenses. Detection, remediation, preemptive accelerated response times, and significant risk reduction can be realized from one console.

Reactive cyberdefense strategies play their role as a critical cyberdefense component but are limited to playing catch-up and fighting fires. Adversaries are using next-generation tools to devise campaigns designed to attack traditional defenses, testing reactive security products to see what techniques will breach their shields. Organizations need to address the entire attack lifecycle before and after they are hit.

Gain Complete Attack Lifecycle Coverage

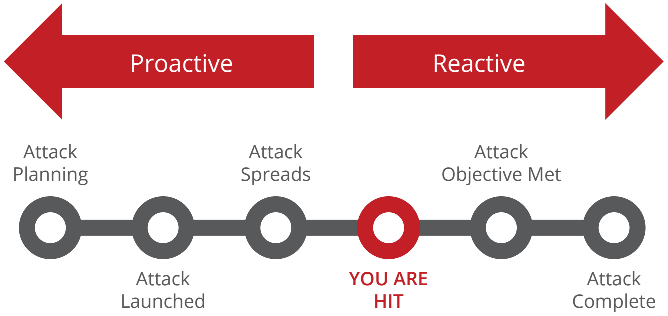


Figure 1. A typical attack lifecycle.

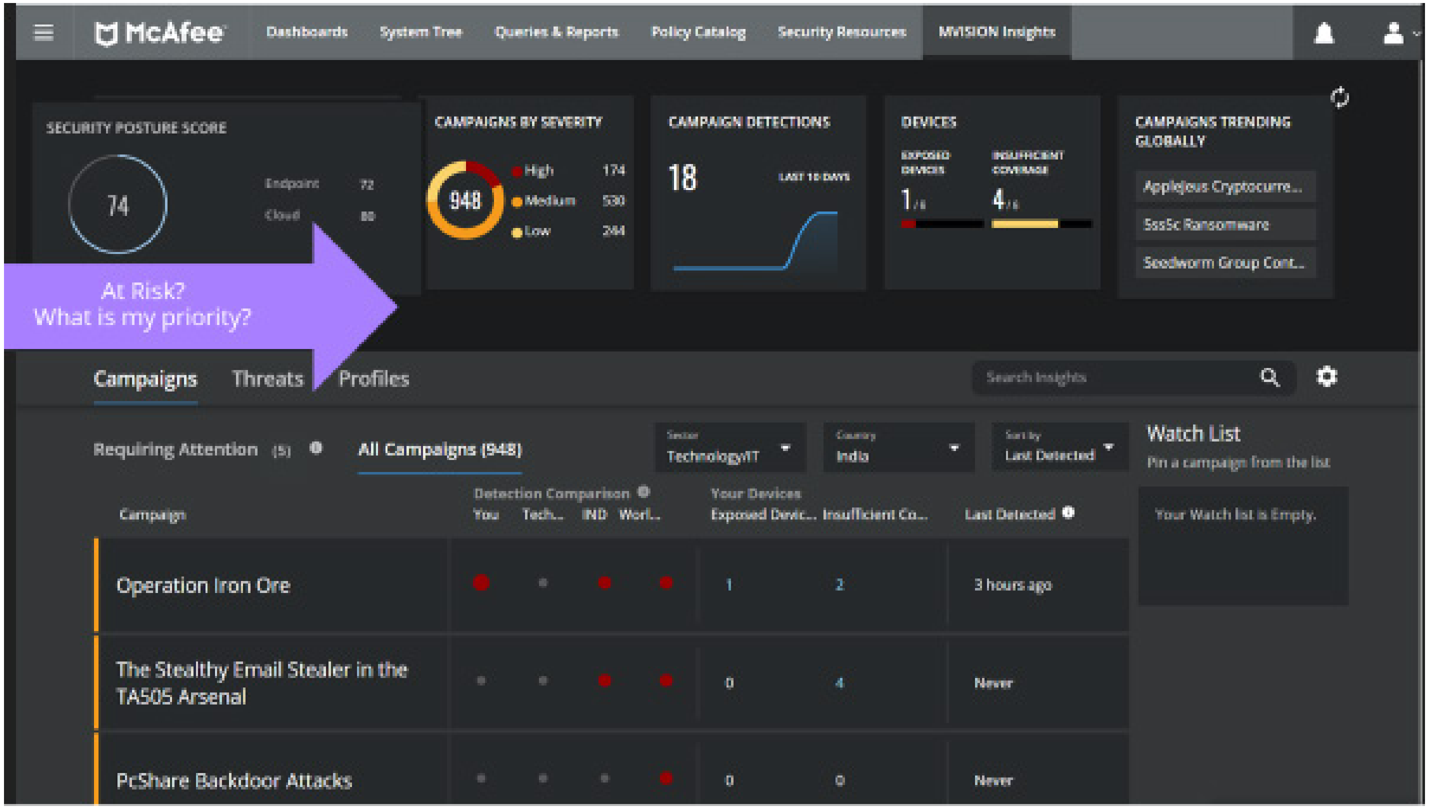
At the end of the day, intelligence and actionable insights give you the best possible cybersecurity stance against the most likely threats and boost confidence in your defenses. Here's how McAfee MVISION Insights accomplishes this:

- **Automatically identify global threats you had been blind to:** MVISION Insights leverages a massive reservoir of security intelligence from more than one billion sensors with optimized threat analysis with human machine teaming. Machine learning detects never before seen threats that human analysts would unlikely to discover due to lack of visualizing and processing. The human interface match and outmatch the wits and ingenuity of the human attackers on the other side of that code with intuition and expertise.
- **Increase situational awareness and focus on what matters:** You know precisely how your defenses stack up before threats hit. MVISION Insights proactively tracks and prioritizes local and global threats that are predicted to hit your enterprise.
- **Machine learning analysis:** This capability allows you to determine how your specific comprehensive security posture derived from endpoint and cloud vantage points would perform and then provides preemptive prescribed protection actions that you can implement quickly and easily to block those attacks.

MVISION Insights Provides Answers to Endpoint and Beyond Risk-Related Questions

- Are you at risk? What is your level of exposure?
- How do you prioritize the attacks that might hit your organization? How do you learn about them? What is your research process?
- How do you know the threats that have not hit your organization but are likely?
- Even if you had a TIP, how would you prioritize all the attacks within the TIP database?
- How do you know about threats that have hit your peers?
- How prevalent is this in your industry and region?
- Is there a particular threat actor targeting my organization?
- How does your current security posture sustain this threat?
- What is your confidence in the complete threat landscape and why?

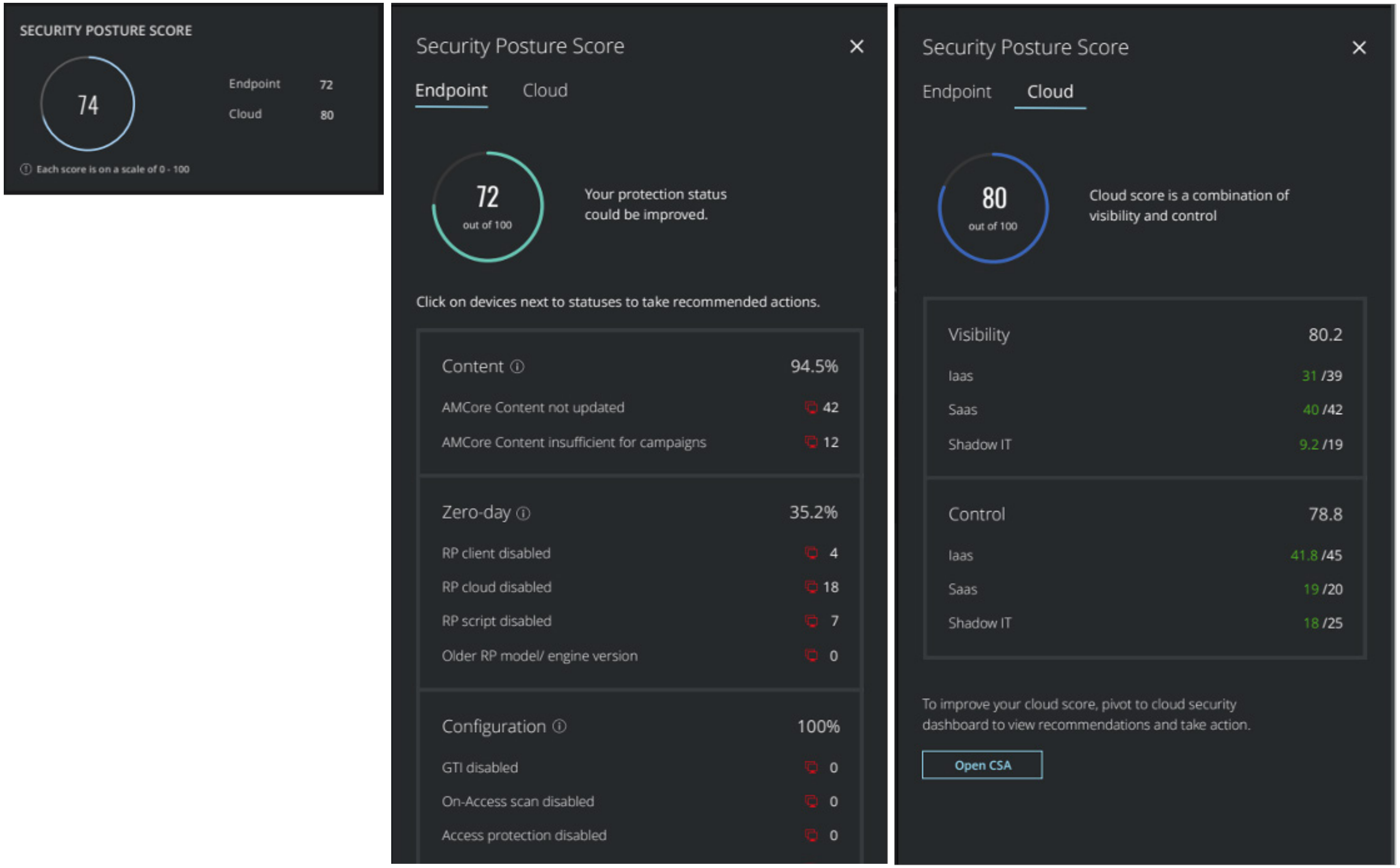
MVISION Insights Dashboard Drives Proactive Security



Campaign	Detection Comparison				Your Devices		Last Detected
	You	Tech...	IND	Worl...	Exposed Devic...	Insufficient Co...	
Operation Iron Ore	●	·	●	●	1	2	3 hours ago
The Stealthy Email Stealer in the TA505 Arsenal	·	·	●	●	0	4	Never
PcShare Backdoor Attacks	·	·	·	●	0	0	Never

Figure 2. MVISION Insights dashboard.

Advance With a Comprehensive Security Posture



SECURITY POSTURE SCORE

74

Endpoint	72
Cloud	80

ⓘ Each score is on a scale of 0 - 100

Security Posture Score ✕

72 out of 100

Your protection status could be improved.

Click on devices next to statuses to take recommended actions.

Content ⓘ	94.5%
AMCore Content not updated	42
AMCore Content insufficient for campaigns	12
Zero-day ⓘ	35.2%
RP client disabled	4
RP cloud disabled	18
RP script disabled	7
Older RP model/ engine version	0
Configuration ⓘ	100%
GTI disabled	0
On-Access scan disabled	0
Access protection disabled	0

Security Posture Score ✕

80 out of 100

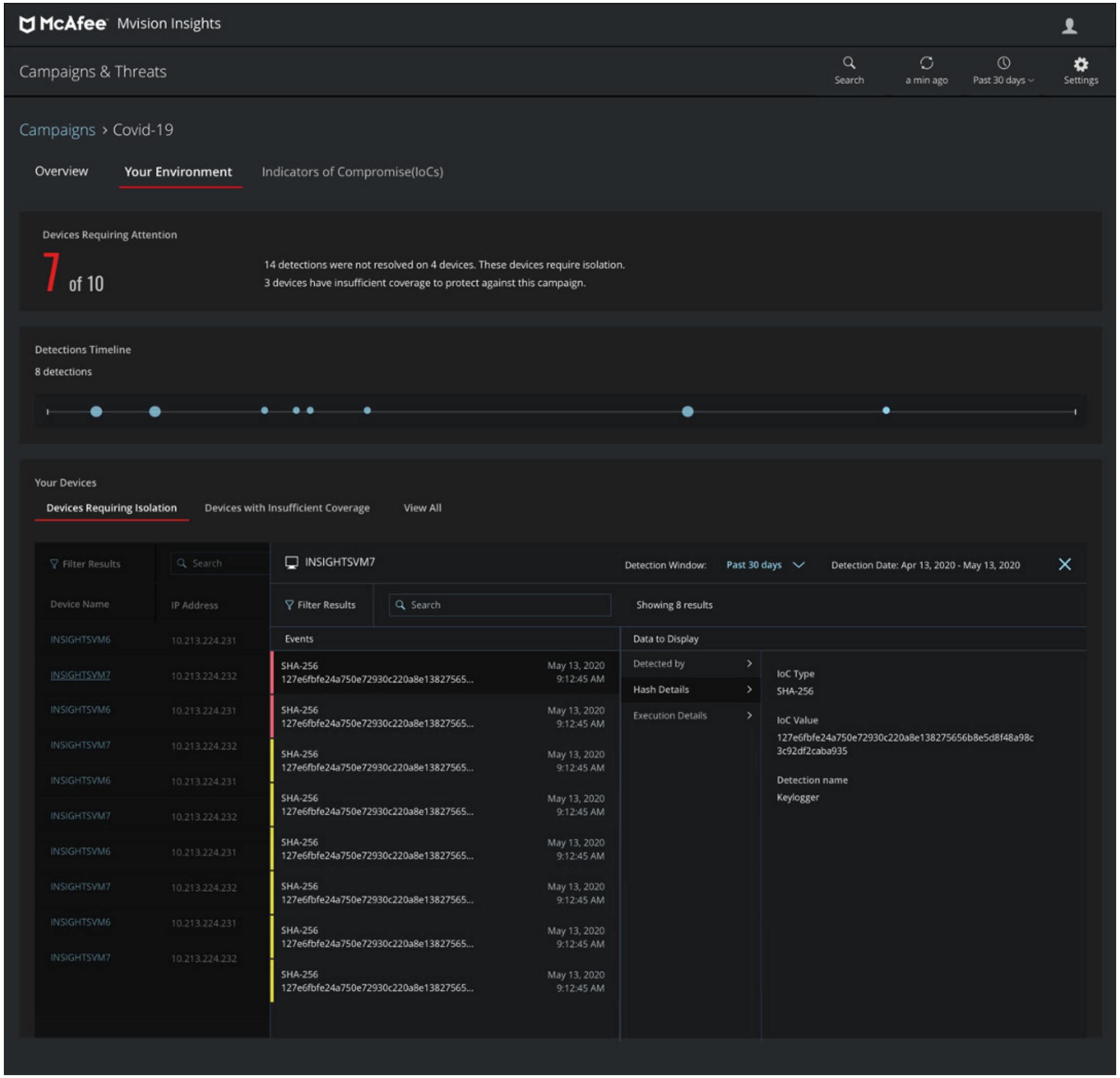
Cloud score is a combination of visibility and control

Visibility	80.2
Iaas	31 /39
Saas	40 /42
Shadow IT	9.2 /19
Control	78.8
Iaas	41.8 /45
Saas	19 /20
Shadow IT	18 /25

To improve your cloud score, pivot to cloud security dashboard to view recommendations and take action.

Figure 3. At-a-glance unified and actionable security posture scoring.

Reach Actionable Risk Assessments



Devices Requiring Attention

7 of 10

14 detections were not resolved on 4 devices. These devices require isolation.
3 devices have insufficient coverage to protect against this campaign.

8 detections

Device Name	IP Address
INSIGHTSVM6	10.213.224.231
INSIGHTSVM7	10.213.224.232
INSIGHTSVM6	10.213.224.231
INSIGHTSVM7	10.213.224.232
INSIGHTSVM6	10.213.224.231
INSIGHTSVM7	10.213.224.232
INSIGHTSVM6	10.213.224.231
INSIGHTSVM7	10.213.224.232
INSIGHTSVM6	10.213.224.231
INSIGHTSVM7	10.213.224.232

INSIGHTSVM7

Detection Window: Past 30 days

Detection Date: Apr 13, 2020 - May 13, 2020

Showing 8 results

Events	
SHA-256 127e6fbfe24a750e72930c220a8e13827565...	May 13, 2020 9:12:45 AM
SHA-256 127e6fbfe24a750e72930c220a8e13827565...	May 13, 2020 9:12:45 AM
SHA-256 127e6fbfe24a750e72930c220a8e13827565...	May 13, 2020 9:12:45 AM
SHA-256 127e6fbfe24a750e72930c220a8e13827565...	May 13, 2020 9:12:45 AM
SHA-256 127e6fbfe24a750e72930c220a8e13827565...	May 13, 2020 9:12:45 AM
SHA-256 127e6fbfe24a750e72930c220a8e13827565...	May 13, 2020 9:12:45 AM
SHA-256 127e6fbfe24a750e72930c220a8e13827565...	May 13, 2020 9:12:45 AM
SHA-256 127e6fbfe24a750e72930c220a8e13827565...	May 13, 2020 9:12:45 AM

IoC Type
SHA-256

IoC Value
127e6fbfe24a750e72930c220a8e138275656b8e5d8f48a98c
3c92df2caba935

Detection name
Keylogger

Figure 4. Know what requires attention in your environment to proactively counter the threat.

Significantly Accelerate Detection and Response Time

MVISION Insights helps your enterprise take the next critical proactive step to change and remediate your unique environment with prescriptive guidance and automated actions. Automation increases effectiveness against outside attacks, automatically analyzing and comparing outside threats and proactively defending against them before they attack.

- **Reduce mean time to detection and to resolution from months to minutes:** Human-machine teaming (deep learning and machine learning) and advanced analytic capabilities are expanded to sift through enormous quantities of data and present actionable intelligence. Expanded detection capabilities preemptively accelerate response times and significantly reduce risk.
- **Improve signal-to-noise ratio for threat indicators:** Advanced analytics expand detection and help you make better sense of alerts. MVISION Insights threat analysis can easily pivot to McAfee® MVISION EDR to search on additional context like indicators of compromise (IoCs) to reduce investigation cycles. Critical context on threat actors/crime syndicates behind the campaign is shared: the tools they have used, the common vulnerabilities and exposures (CVEs) they have been associated with, the standard tactics/sub-techniques and the associated IoCs, and credible sources on the syndicate.
- **Threats are presented to you in a manner that is understandable, with prioritization and actionability:** A comprehensive and unified security posture includes both endpoint and cloud assessment and allows you to focus on what matters across your environment. Guided response based on analyzed and prioritized intelligence and insight elevates even novice analysts. From the integrated console, quickly and easily respond by making changes to your configurations, isolating infected devices, updating policy, or pivoting to endpoint detection and response (EDR).

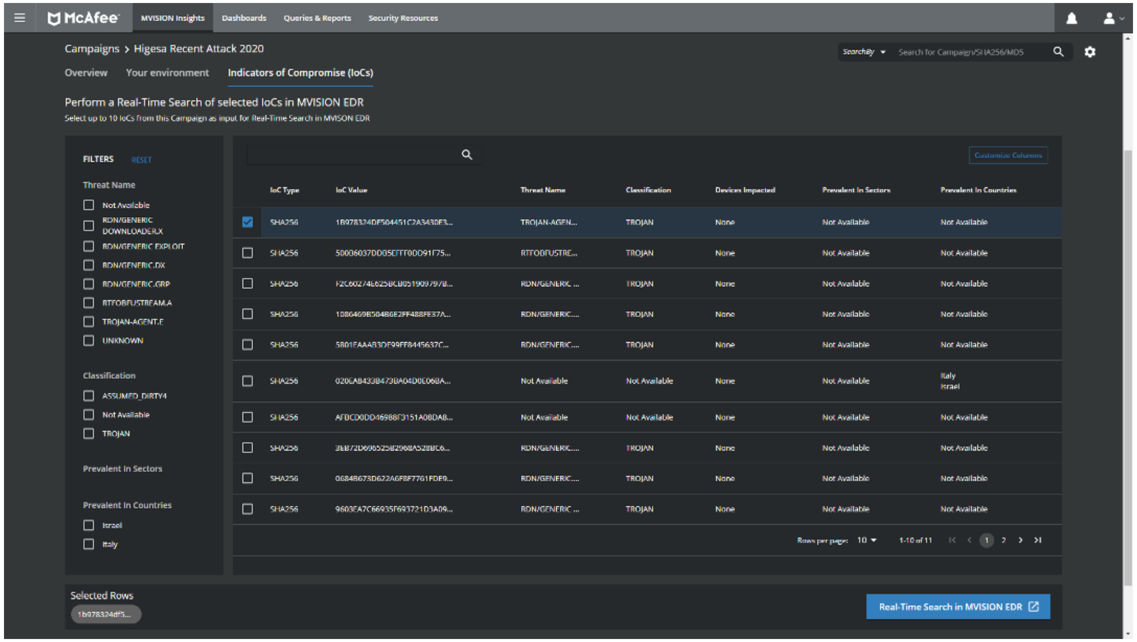
Empower SOC Resources

Security teams are overwhelmed by the immense volume of intelligence they must sift through to protect their environments. Limited resources and time inhibit analysis of threats and defenses. Using human-machine teaming, analytic capabilities are expanded—no matter the skill level of analysts—to crawl enormous quantities of data and present it as actionable intelligence. MVISION Insights allows your enterprise to address its skills gap and empower SOC functions. Security teams are better informed so they can make better decisions.

- Human insight gained by using the data intelligence provided allows security teams to customize and maximize your enterprise's defense for optimum protection without the need to increase staff size or rely on higher levels of expertise. MVISION Insights offers more purposeful insights into MVISION EDR to reduce the length of the investigation cycle, providing the expertise and resource needed to carry out investigations. Analysts can verify the risk of the incident and root cause with increased speed and efficiency.

- Helps chief security officers (CSOs) get the most out of their staff and products by freeing security analysts from mundane tasks and helping even junior-level team members become more effective. Organizations can realize a reduction in hours associated with security management. Workflows can be streamlined to accelerate additional safeguards.
- Preemptively automates detection, response, and defenses on prioritized threats from a single console, alleviating the need for analysts to toggle between tasks. MVISION Insights accumulates and analyzes relevant data elements with actionable guidance in one place, placing it at the fingertips of security analysts when needed.

Deeper Insights



Campaigns > Higesa Recent Attack 2020

Overview Your environment Indicators of Compromise (IoCs)

Perform a Real-Time Search of selected IoCs in MVISION EDR

Select up to 10 IoCs from this Campaign as input for Real-Time Search in MVISON EDR

FILTERS RESET

Threat Name
☐ Not Available
☐ RDN/GENERIC DOWNLOADER.X
☐ RDN/GENERIC EXPLOIT
☐ RDN/GENERIC.DX
☐ RDN/GENERIC.GRP
☐ RTFOBFUSTREAM.A
☐ TROJAN-AGENT.E
☐ UNKNOWN

Classification
☐ ASSUMED_DIRTY4
☐ Not Available
☐ TROJAN

Prevalent In Sectors

Prevalent In Countries
☐ Israel
☐ Italy

	IoC Type	IoC Value	Threat Name	Classification	Devices Impacted	Prevalent In Sectors	Prevalent In Countries
☑	SHA256	1B978324DF504451C2A3430F3...	TROJAN-AGEN...	TROJAN	None	Not Available	Not Available
☐	SHA256	50006037DD05EFFF0DD91F75...	RTFOBFUSTRE...	TROJAN	None	Not Available	Not Available
☐	SHA256	F2C60274E625BCB051909797B...	RDN/GENERIC ...	TROJAN	None	Not Available	Not Available
☐	SHA256	1086469B504B6E2FF488FE37A...	RDN/GENERIC....	TROJAN	None	Not Available	Not Available
☐	SHA256	5801EAAAB3DE99FF8445637C...	RDN/GENERIC....	TROJAN	None	Not Available	Not Available
☐	SHA256	020EA8433B473BA04D0E06BA...	Not Available	Not Available	None	Not Available	Italy Israel
☐	SHA256	AFBCD0DD46988F3151A08DA8...	Not Available	Not Available	None	Not Available	Not Available
☐	SHA256	3EB72D69652582968A528BC6...	RDN/GENERIC....	TROJAN	None	Not Available	Not Available
☐	SHA256	0684B673D622A6F8F7761FDE9...	RDN/GENERIC....	TROJAN	None	Not Available	Not Available
☐	SHA256	9603EA7C66935F693721D3A09...	RDN/GENERIC ...	TROJAN	None	Not Available	Not Available

Rows per page: 10 1-10 of 11 1 2

Selected Rows

1b978324df5...

Figure 5. Dig deeper to understand threat events and determine your ability to defend your organization with an option to pivot to EDR capability.

MVISION Insights Requirements

MVISION Insights is managed by McAfee® ePolicy Orchestrator® (McAfee® ePO™) software 5.10 (on premises and IaaS) and McAfee® MVISION ePO™ (SaaS). It is optimized for use with our latest endpoint protection technology: McAfee® Endpoint Security and McAfee® Agent. MVISION Insights requires McAfee Endpoint Security telemetry to be opt-in to work effectively.

Sample Use Cases

Problem	Solution	Outcome
Am I being targeted? **Is this a new campaign variant?**	▪ Known campaign threat assessment ▪ Severe threat group or actor assessment ▪ Selected retrospective attack analysis ▪ Comparative protection efficacy reporting ▪ User IoC retrospective attack analysis	Answer the question: Am I at risk? Is there a specific threat actor targeting me? Is there campaign likely to attack me?
What is my overall security posture?	▪ Unified security posture from endpoint to cloud	Assess and act on my comprehensive security hygiene
Can my current protection configuration protect me?	▪ Local protection posture check	Assess my current security posture
What specifically do I have to change to be protected?	▪ Local protection posture check	Prescriptive guidance on what to do
Can my other security functions isolate?	▪ Publish to isolate or contain to other security functions	Send contain actions to other security functions to further mitigate the risk (via Data Exchange Layer [DXL])

Learn More

For more information, visit www.mcafee.com.

McAfee™

6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com

4750_0521
MAY 2021