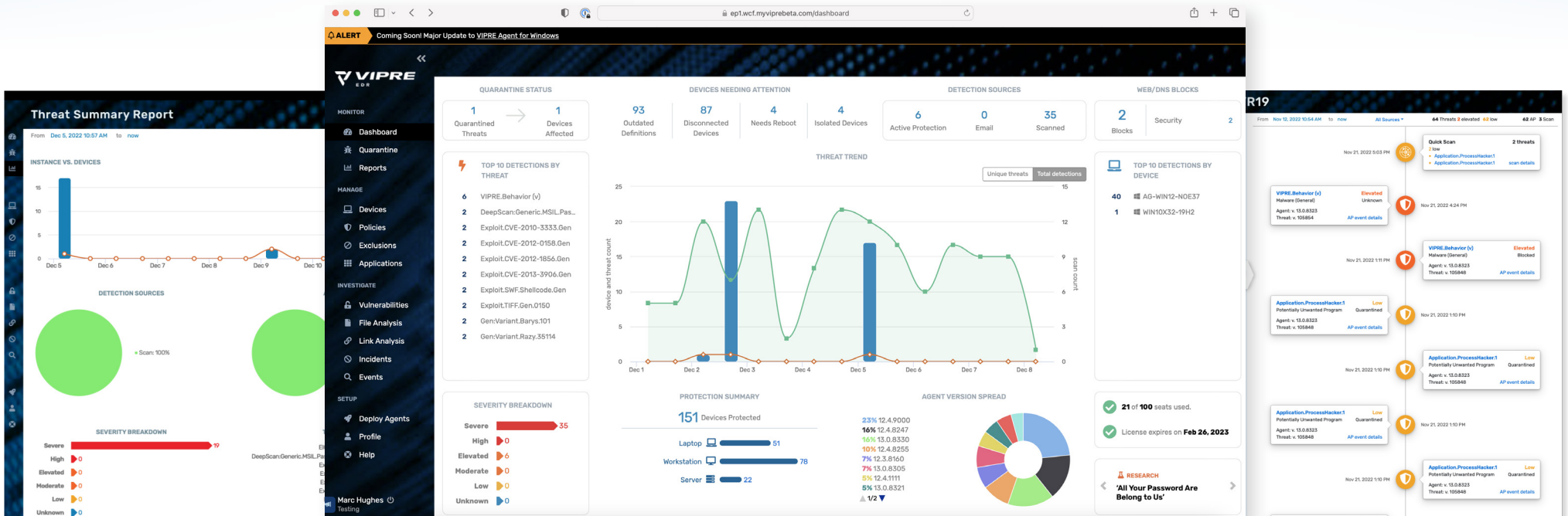
VIPRE EDR

VIPRE Endpoint Detection & Response (EDR) delivers streamlined, sophisticated EDR management in a single, easy to navigate console.

VIPRE EDR is the future evolution of Endpoint Detection & Response - a high performing, cloud-based solution without the complexity.



Detection

Powerful Dashboards

Speed-up or reduce initial assessment time, investigate trends and see an overview of your security posture and cyber risk.

EDR Built For All Devices Including Desktop And Mobile

Ultimate flexibility quickly respond to issues on-the-go, easily work out of hours, or just check in occasionally on your mobile device. VIPRE EDR works across all devices, operating systems and screen sizes to ensure you're always in the know and there are no surprises.

Malware Detection

Leverage a pipeline of powerful malware analysis engines that use a variety of techniques to detect the latest malware, viruses, and ransomware.

Threat Visualization

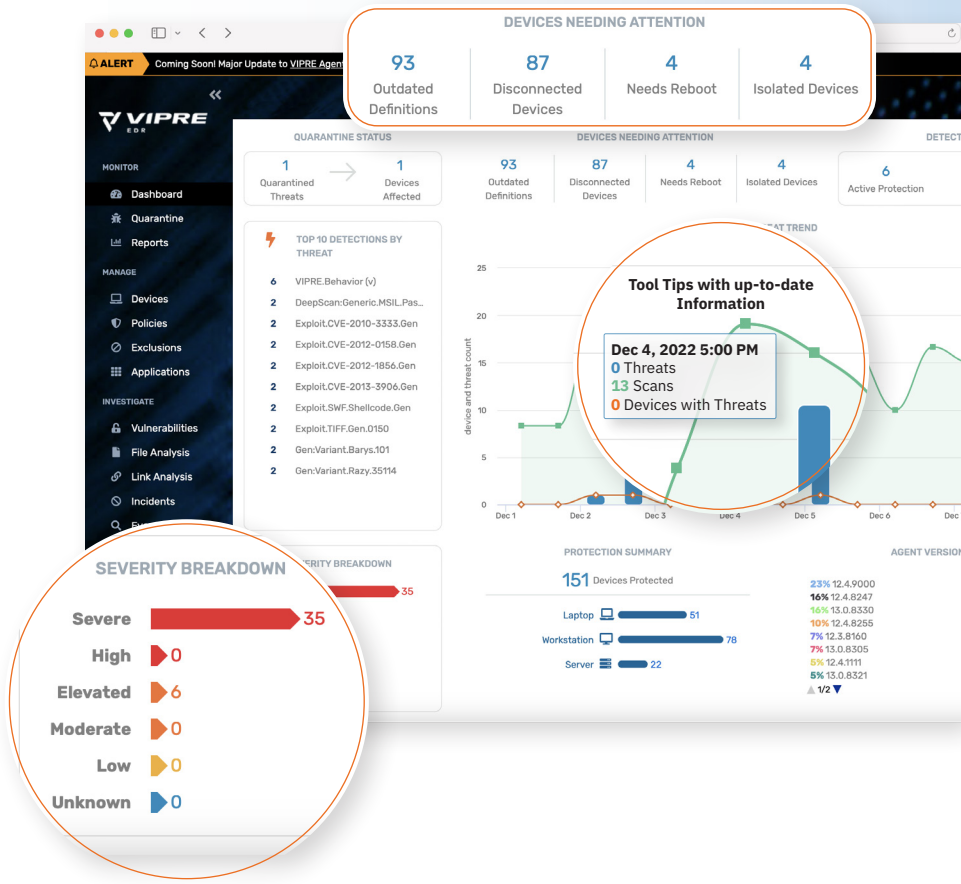
Quickly view and address all threat behavior from a central location. Understand how and when a potential threat impacted your systems.

Advanced, Persistent, Zero-day Attack Detection

Detect more sophisticated and file-less attacks via event and alert correlation on the endpoint which will generate incidents once a pattern of behavior has been identified as a risk.

Exploit Prevention

Proactively block exploits via DNS Protection, in-browser exploit prevention, and in-process anomaly blocking.



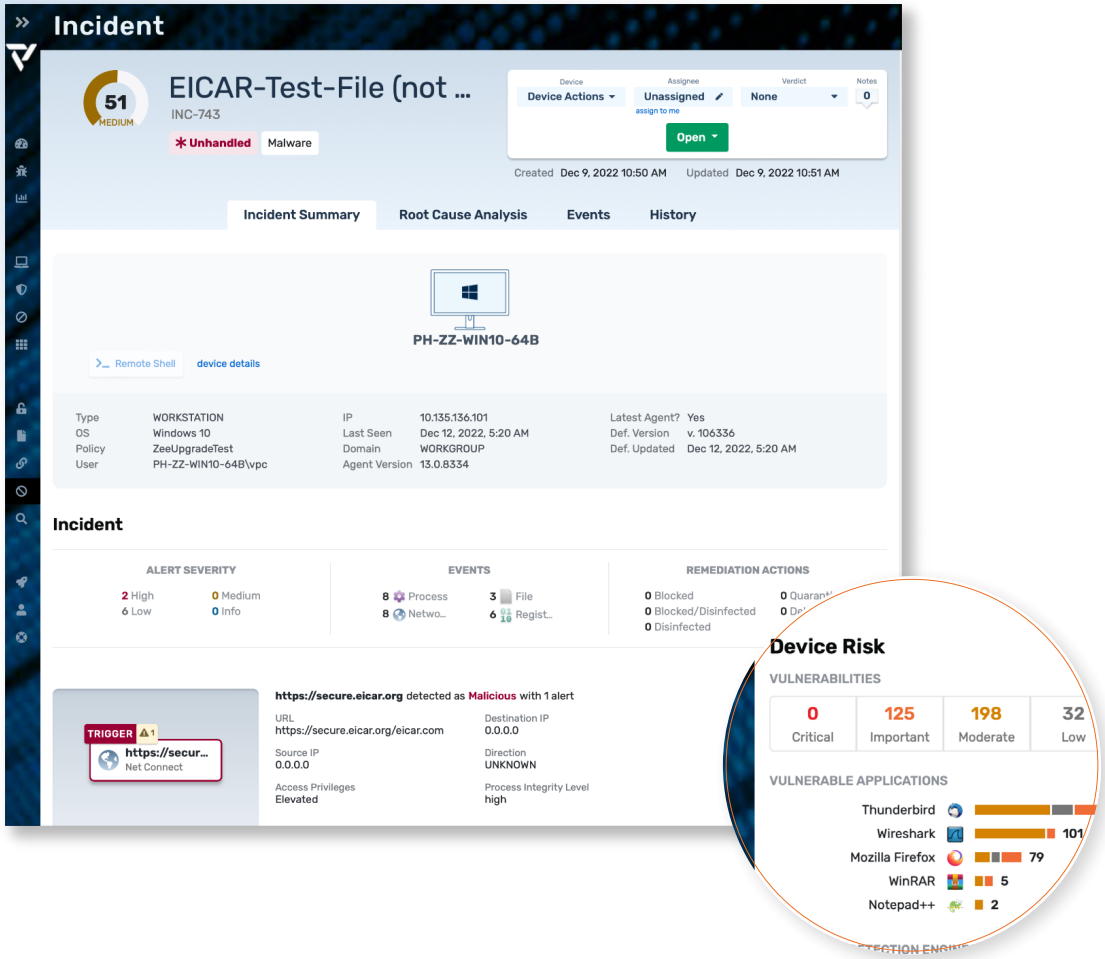
VIPRE EDR

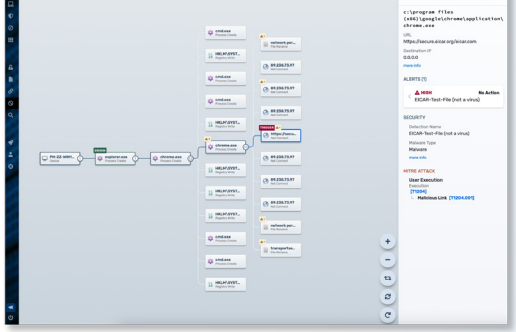
Investigation

VIPRE EDR's intuitive dashboards, easy-to-understand event logs and actionable intelligence provide visibility and direction.

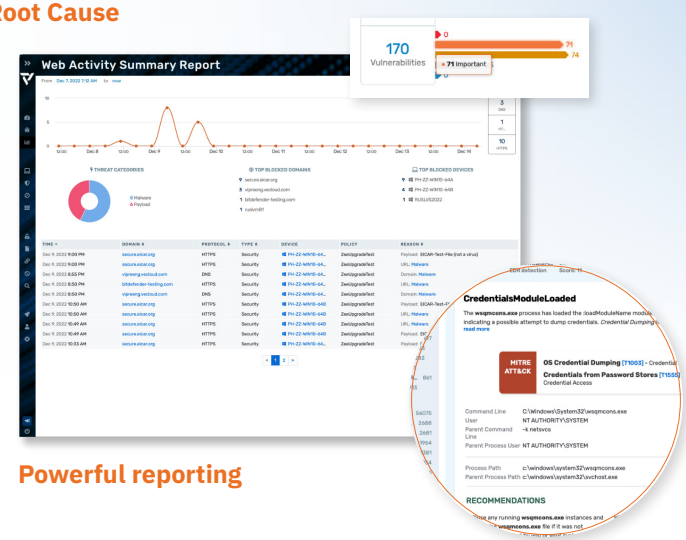
Incident Management

Most attacks will be automatically blocked, and VIPRE EDR incidents will help you visualize, understand, and remediate ongoing attacks as well as harden your environment from future attacks.





Analyze Root Cause



Powerful reporting

Fast Access to Contextual Data

When investigating a threat, VIPRE EDR's deep links enable quick access to contextual data that helps with the investigation. Drill down to the information you need, and explore the data in an intuitive way to aid decision making and speed up resolution times.

VIPRE EDR

Investigation

Scan and Threat Reports

INSTALLED VERSION		LATEST AVAILABLE	DEVICES	VULNERABILITIES	FIXE
22.2.20191	→	22.002.20212	1		
22.002.20212	✓✓	22.002.20212	1		
32.0.0.156	→	32.0.0.465	1	10	0
4.01.0	→	6.11	1	5	5
5.11.0	→	6.11	1	5	5
5.30.0	→	6.02	1	5	5
6.02.0	✓✓	6.02.0	2		
6.10.0	✓✓	6.10.0	2		
6.11.0	✓✓	6.11.0	10		
7.0.0.117	→	16.0.0.30	1		
2.7.0.0	✓✓	2.7.0.0	1		
3.0.0.10	→	3.1.0.1	1		
11.1.0.126	→	12.10.10.2	1	579	559
2.2.1960	✓✓	2.2.1960	1		
3.60.2.0	→	3.62.2	1		

« 1 2 3 4 5 »

Vulnerability Scanning

Scan endpoint systems for known vulnerabilities in third-party applications quickly and easily. Information is displayed within the EDR console clearly and logically so you can understand the risks caused by detected vulnerabilities.

Malicious File & URL Investigation

Any suspicious URL's or files can be sent to our cloud-hosted sandbox for a full report on any potential malicious behavior.

FILES:
Files found on disk, USB devices, attached to email, etc.

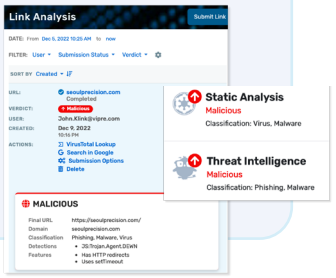
URL'S:
URLs found in network activity, embedded in emails or social posts, etc.

FILES: Identify malicious activity, network traffic, files/registry changes, and IoCs generated.

Isolation
Sandbox identifies malicious activity

URL'S: Identify Phishing attempts, or known malware components.

DETAILED REPORT:
Full report on any potential malicious behavior.



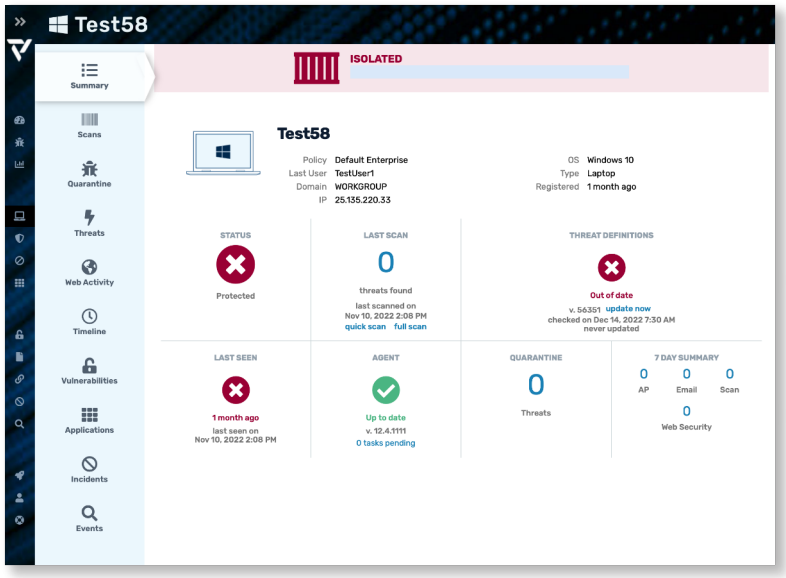
VIPRE EDR

Containment

Built-in incident management enables you to keep track of all open threats to ensure nothing falls through the cracks.

Endpoint Isolation

Prevent threat spread by quickly isolating an affected device on the network. Only you will be able to manage and interact with the device until your investigation is complete.



Integrated Remote Shell

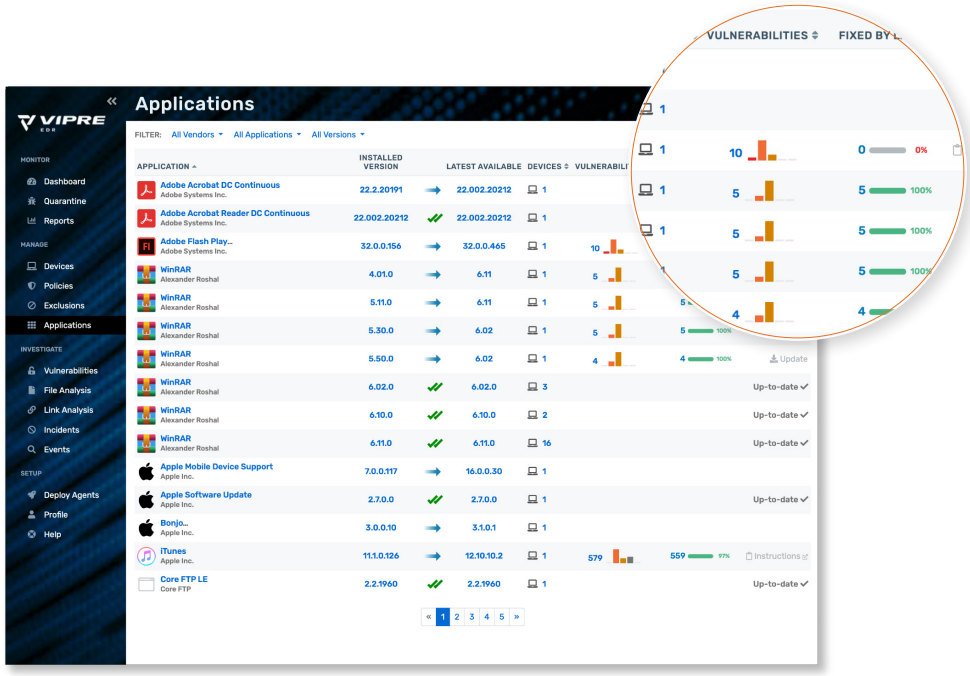
Want an even deeper look at what happened on the endpoint? Click a button and you will instantly have access to the remote device, no special installation required.

VIPRE EDR

Remediation

Application Scanning

Leverage endpoint integration to quickly discover installed third-party applications across all your protected devices, including app version information.

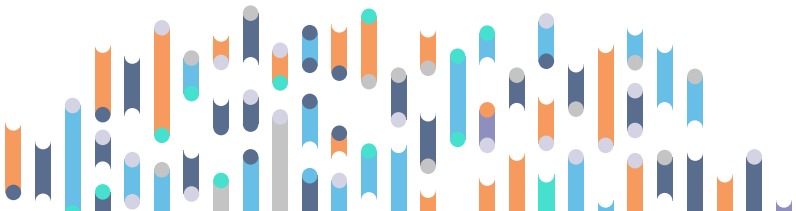


Endpoint Hardening

Scan your systems for installed third-party applications and known vulnerabilities, and, if necessary, easily close discovered vulnerabilities by patching those applications with a simple click.

Remote Shell

Contain breaches no matter where the compromised endpoints are located and reduce any downtime from an attack - by remotely killing processes, cleaning up files, etc.



VIPRE EDR

Why Choose VIPRE EDR?

VIPRE Security Group puts more than twenty years of advanced security intelligence, cutting-edge machine learning, real-time behavioral analysis, and a comprehensive threat intelligence network to work defending against known and unknown attacks.

Our streamlined approach to EDR is suitable for all security professionals providing what you need when you need it.

- ✓ The Best Protection at the Best Price - VIPRE is consistently ranked in the top tier alongside other market leaders in comprehensive independent tests.
- ✓ Easy to Use - VIPRE's intuitive solutions make it easier to secure your endpoints from ransomware and other threats.
- ✓ Rapid Deployment - Admins can deploy VIPRE quickly with minimal disruption to day-to-day activities.
- ✓ Reduced Downtime - VIPRE enables both speed and security protecting you from malware without slowing down any processes.
- ✓ Award-winning Support - included with all of our solutions is access to our award-winning, highly-qualified global tech support team with a consistent 90%+ CSAT rating.

What Next?

For more information and to request a demo:

Visit: **www.vipre.com/edr**

Call: **+1-855-885-5566** (US) **+44 (0)800 093 2580** (EMEA)

Email: **sales@VIPRE.com** (US) **uksales@VIPRE.com** (EMEA)

VIPRE EDR