



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.

The screenshot displays the VIPRE EDR dashboard with the following sections:

- QUARANTINE STATUS:** 1 Quarantined Threats, 1 Device Affected.
- DEVICES NEEDING ATTENTION:** 93 Outdated Definitions, 87 Disconnected Devices, 4 Needs Reboot, 4 Isolated Devices.
- DETECTION SOURCES:** 6 Active Protection, 0 Email, 35 Scanned.
- WEB/DNS BLOCKS:** 2 Blocks, Security 2.
- THREAT TREND:** A line chart showing device and threat count from Dec 1 to Dec 8. The y-axis ranges from 0 to 25. A significant spike is visible on Dec 3.
- TOP 10 DETECTIONS BY THREAT:**
 - 6 VIPRE.Behavior (v)
 - 2 DeepScan.Generic.MSIL.Pas...
 - 2 Exploit.CVE-2010-3333.Gen
 - 2 Exploit.CVE-2012-0158.Gen
 - 2 Exploit.CVE-2012-1856.Gen
 - 2 Exploit.CVE-2013-3906.Gen
 - 2 Exploit.SWF.Shellcode.Gen
 - 2 Exploit.TIFF.Gen.0150
 - 2 Gen.Variant.Barys.101
 - 2 Gen.Variant.Razy.35114
- SEVERITY BREAKDOWN:** Severe: 35, High: 0, Elevated: 6, Moderate: 0, Low: 0, Unknown: 0.
- PROTECTION SUMMARY:** 151 Devices Protected. Breakdown: Laptop (51), Workstation (78), Server (22).
- AGENT VERSION SPREAD:** A donut chart showing the distribution of agent versions. Key versions include 12.4.9000 (23%), 12.4.8247 (16%), 13.0.8330 (16%), 12.3.8160 (7%), 13.0.8305 (7%), 12.4.1111 (5%), and 13.0.8321 (5%).
- SEVERITY BREAKDOWN (Bottom):** 21 of 100 seats used. License expires on Feb 26, 2023.
- RESEARCH:** 'All Your Password Are Belong to Us'
- Threat Summary Report (Left Panel):** Shows instance vs. devices, detection sources (Scans: 100%), and a severity breakdown (Severe: 19, High: 0, Elevated: 0, Moderate: 0, Low: 0, Unknown: 0).
- Event Log (Right Panel):** Lists events such as 'VIPRE.Behavior (v) Malware (General)', 'Application.ProcessHacker1', and 'Application.ProcessHacker1 Potentially Unwanted Program' with their respective severities and actions.



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.



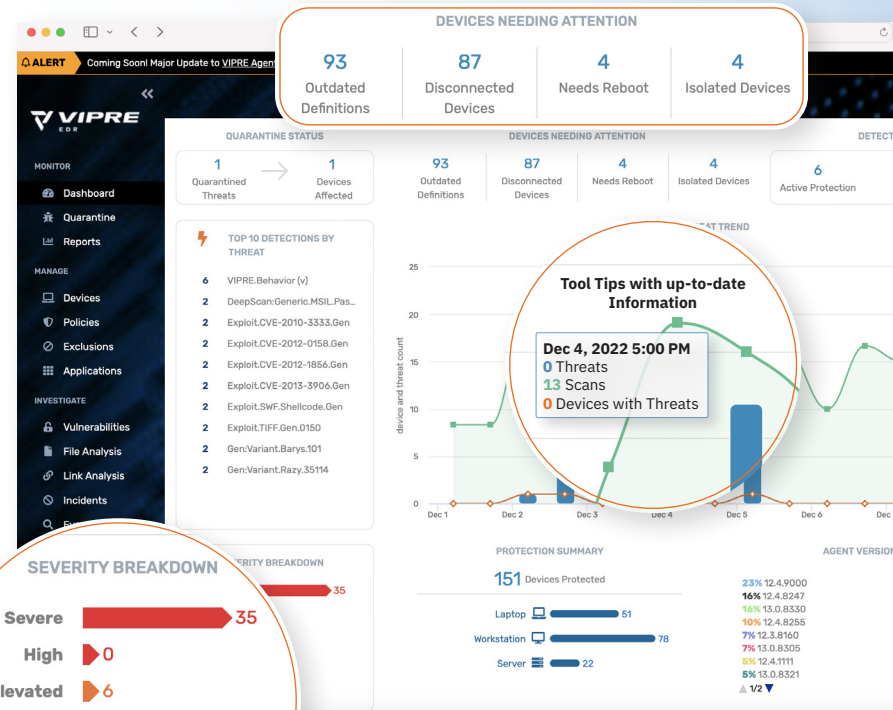
Advanced, Persistent, Zero-day Attack Detection

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.



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.

Incident
51 MEDIUM
EICAR-Test-File (not ...)
 INC-743
 * Unhandled Malware
 Device: PH-ZZ-WIN10-64B
 Assignee: Unassigned
 Verdict: None
 Notes: 0
 Created: Dec 9, 2022 10:50 AM Updated: Dec 9, 2022 10:51 AM

Incident Summary | Root Cause Analysis | Events | History

PH-ZZ-WIN10-64B

Type: WORKSTATION | OS: Windows 10 | IP: 10.135.136.101 | Latest Agent?: Yes
 Policy: ZeeUpgradeDefeat | User: PH-ZZ-WIN10-64B\vpcc | Last Seen: Dec 12, 2022, 5:20 AM | Def. Version: v.106336
 Domain: WORKGROUP | Agent Version: 13.0.8334 | Def. Updated: Dec 12, 2022, 5:20 AM

Alert Severity: 2 High, 0 Medium, 6 Low, 0 Info

Events: 8 Process, 3 File, 8 Netwo..., 6 Regist...

Remediation Actions: 0 Blocked, 0 Quarant..., 0 Blocked/Disinfected, 0 Dr..., 0 Disinfected

Device Risk

Vulnerabilities: 0 Critical, 125 Important, 198 Moderate, 32 Low

Vulnerable Applications: Thunderbird, Wireshark, Mozilla Firefox (79), WinRAR (5), Notepad++ (2)

Trigger: https://secure.eicar.org detected as Malicious with 1 alert

URL: https://secure.eicar.org/eicar.com | Destination IP: 0.0.0.0
 Source IP: 0.0.0.0 | Direction: UNKNOWN
 Access Privileges: Elevated | Process Integrity Level: high

Incident
51 MEDIUM
EICAR-Test-File (not a viru...
 INC-743
 Unhandled Malware
 Created: Dec 9, 2022 10:50 AM Updated: Dec 9, 2022 10:51 AM

Root Cause Analysis

Timeline of events showing the progression of the incident from initial detection to the final alert.

Analyze Root Cause

Web Activity Summary Report

170 Vulnerabilities (71 Important)

9 HIGHEST CATEGORIES: Malware, Suspicious, Suspicious, Suspicious, Suspicious, Suspicious, Suspicious, Suspicious, Suspicious

10 TOP BLOCKED DOMAINS: https://secure.eicar.org, https://secure.eicar.org, https://secure.eicar.org, https://secure.eicar.org, https://secure.eicar.org, https://secure.eicar.org, https://secure.eicar.org, https://secure.eicar.org, https://secure.eicar.org, https://secure.eicar.org

CredentialsModuleLoaded

HITRE ATTACK OS Credential Dumping (T1005) - Credentials from Password Stores (T1550) - Credential Access

Command Line: C:\Windows\System32\cmd.exe
 User: NT AUTHORITY\SYSTEM
 Parent Command: powershell
 Line: powershell
 Parent Process User: NT AUTHORITY\SYSTEM
 Process Path: C:\Windows\System32\cmd.exe
 Parent Process Path: C:\Windows\System32\cmd.exe

RECOMMENDATIONS

Any running `wspocms.exe` instances and `wspocms.exe` file is not used.

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.

Scan and Threat Reports



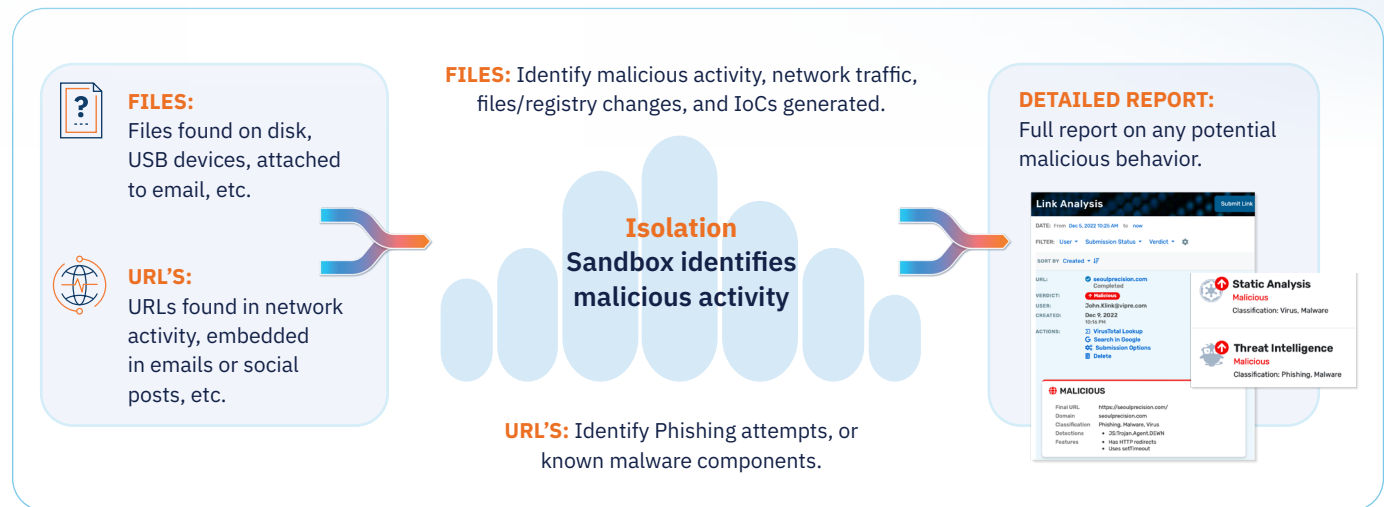
Vulnerability Scanning

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.

INSTALLED VERSION	LATEST AVAILABLE	DEVICES	VULNERABILITIES	FIXED
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		

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.

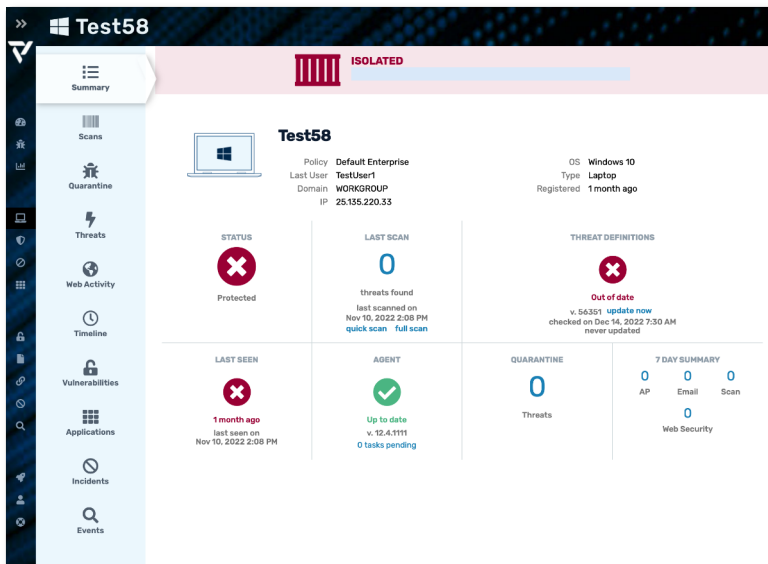


Containment

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

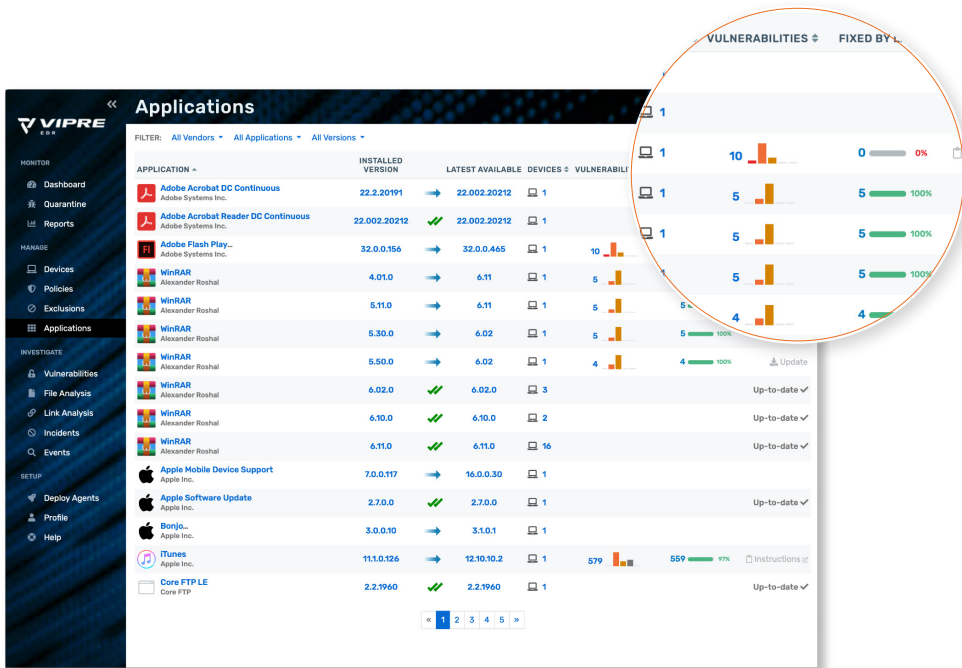
Want an even deeper look at what happened on the endpoint? Click a button and you will instantly have access to the remote device, no special installation required.



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.





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)