

Integrated Global Intelligence Problem Solved

Comodo Valkyrie Verdict Driven, File Analysis

Valkyrie has massive scale. 73 billion file queries, and 300 million unique unknown files submitted annually. Valkyrie also provides a verdict for 200 million known, and 1 million unique, unknown files each day.

Accelerated Verdict at Internet Speed and Scale

Comodo Valkyrie is a cloud based File Analysis Platform that provides static, dynamic and even human expert analysis for submitted files of unknown and zero day files. Valkyrie's verdict driven platform processes over 200 million unknown file submissions each day, uncovering more than 300 million unknown files every year, through tightly integrated Comodo solutions, partnerships, and our active global community of threat researchers. Static and dynamic analysis provides a verdict in an average of 45 seconds - 5x's faster than competitors. Integrated expert human analysis prevents the 'near positive' detection gap inevitable from competing solutions, when unsupported or unrecognizable file types leveraging new sandbox evasion techniques slip through the cracks undetected.

Unlike virtualization dependent sandboxes which leave you open to 'patient zero' exploits, Valkyrie's implementation of sandbox analysis accelerates the verdict process, assisting existing protection in Comodo solutions such as automatic containment in AEP or portable containment in Comodo Dome. The result is the most complete coverage of unknown and zero day executables delivered in the market today.

Integrations

Valkyrie is both tightly integrated into the Comodo Endpoint, Network and Boundary solutions and is also available as a no cost research portal with an active community. Qualifying institutions may leverage Valkyrie plugins which are available via web services REST API. For those requiring custom detection or multi-vendor integration, Valkyrie offers script based embedded detectors.

COMODO

Key Features

Whitelisting	<ul style="list-style-type: none">• Comodo is the world's largest certificate authority and is uniquely positioned to have intelligence on known good, digitally signed applications and publishers, better than any competing vendor on the market today.
Static Analysis	<ul style="list-style-type: none">• 26+ Static Detector Groups, containing 1,000+ static analysis detectors.• Static analysis detectors include binary level analysis, included libraries, system calls embedded in the code, extractable links, unpackers, string analysis and many more detectors that determine a verdict.• Over 450 unpackers
Dynamic Analysis	<ul style="list-style-type: none">• Sandbox based dynamic analysis is performed on the file. Behavioral and environmental analysis is performed, watching for 'anti-VM' evasion, VM escape attempts, mass sleep commands, registry changes, file system pollution, API calls and returns and much more.
Machine Learning	<ul style="list-style-type: none">• Comodo Valkyrie integrates machine learning (ML) throughout the automated Verdict Driven Platform. Examples of ML techniques include support vector machines, naive bayes, decision trees, random forest classifier, linear discriminant analysis, stochastic gradient descent, hidden markov models, neural networks and more.• ML based models ensure a high degree of accuracy, reduced management and overhead typically associated with exploit validation and response.
Reputation Analysis	<ul style="list-style-type: none">• Comodo Valkyrie takes the concept of reputation in a different direction. Analyzed malicious files receive a verdict, embedded URLs are extracted and matched against known bad URLs (web blacklist), as well as correlated against all known bad malware URLs to draw associations between polymorphic code, campaigns and threat actors.
File Lookup Service (FLS)	<ul style="list-style-type: none">• The Valkyrie File Lookup Service is a lightweight, swift reply to integrations queries related to globally known bad processes or executables.
Expert Human Analysis	<ul style="list-style-type: none">• On average 85% of all files submitted to Valkyrie are provided with an accelerated verdict through static and dynamic automated analysis. 15% of files are typically not able to be analyzed by any automated system and require an expert human malware analyst.• The industry's only SLA backed, advanced malware analysis platform with human analysis to ensure 100% verdict on all unknown files.
Valkyrie Hunter	<ul style="list-style-type: none">• Freely available, easy to use, hunting tool available on valkyrie.comodo.com.• Helps identify unknown files in your area network on Windows devices.• Windows based executable downloaded from the Comodo Valkyrie website.

About Comodo

The Comodo organization is a global innovator and developer of cybersecurity solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information. With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online®. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom. For more information, visit comodo.com.

Comodo and the Comodo brand are trademarks of the Comodo Group Inc. or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. The current list of Comodo trademarks and patents is available at comodo.com/repository