GOSECURE

NEXT-GEN ANTIVIRUS (NGAV)

GoSecure Next-Gen Antivirus (NGAV) offers a compelling selection of capabilities, far beyond traditional AV but still covering the basics of this tried and true security technology. While some would tell you that traditional AV is obsolete, GoSecure believes you need a strong combination of traditional and next-gen to quickly, and effectively, protect endpoints. Malicious files taking advantage of exploits via file-less attacks is the new normal. Detecting, and protecting, against these multi-faceted attacks requires multiple approaches to endpoint security, and GoSecure NGAV delivers.

MANAGEMENT FOR OPTIMIZATION

Technology by itself provides a solid first step, but what happens with all the information (i.e., alerts) provided by the technology? The GoSecure Advanced Response Center (ARC) has over 400,000 hours of experience analyzing alerts, defining the severity and then executing a response. The combination of traditional and next-gen AV provides a steady flow of alerts, well beyond traditional AV by itself. The GoSecure ARC operationalizes your NGAV protection to optimize it's security capabilities.

GoSecure is recognized as a leader and innovator in cybersecurity solutions. The company is the first and only to integrate an Endpoint and Network threat detection platform, Managed Detection and Response services, and Cloud/SaaS delivery. Together, these capabilities provide the most effective response to the increased sophistication of continuously evolving malware and malicious insiders that target people, processes and systems. With focus on innovation quality, integrity and respect, GoSecure has become the trusted provider of cybersecurity products and services to organizations of all sizes, across all industries globally.

To learn more, visit: https://www.gosecure.net

Next-Generation Antivirus

Replace legacy antivirus solutions with the latest endpoint anti-malware technology to address emerging, fileless, memory-based attacks and more.

Machine Learning

All GoSecure products are backed by our industry leading Machine Learning. Developed to deliver the highest quality, and fastest, correlation possible, GoSecure Machine Learning is in a constant state of review to maintain the highest fidelity results.

Advanced Memory Scanner

Advanced Memory Scanner monitors the behavior of a malicious process and scans it once it decloaks in memory. Fileless malware operates without needing persistent components in the file system that can be detected conventionally. Only memory scanning can successfully discover and stop such malicious attacks.

Ransomware Shield

Ransomware Shield is an additional layer protecting users from ransomware. This technology monitors and evaluates all executed applications based on their behavior and reputation. It is designed to detect and block processes that resemble the behavior of ransomware.

Exploit Blocker

Exploit Blocker monitors typically exploitable applications (browsers, document readers, email clients, Flash, Java and more), and instead of just aiming at particular CVE identifiers, it focuses on exploitation techniques. When triggered, the threat is blocked immediately on the machine.

In-Product Sandbox

Today's malware is often heavily obfuscated and tries to evade detection as much as possible. To see through this and identify the real behavior hidden underneath the surface, we use in-product sandboxing. By emulating different components of computer hardware and software, sandboxing can execute a suspicious sample in an isolated virtualized environment.

Botnet Protection

Botnet Protection detects malicious communication used by botnets, and at the same time it identifies the offending processes. Any detected malicious communication is blocked and reported to the user.

Cross Platform Support

GoSecure NGAV supports all OSes including Windows, Mac and Linux.