NEHEMIAH SECURITY

Introduction to **AtomicEye**

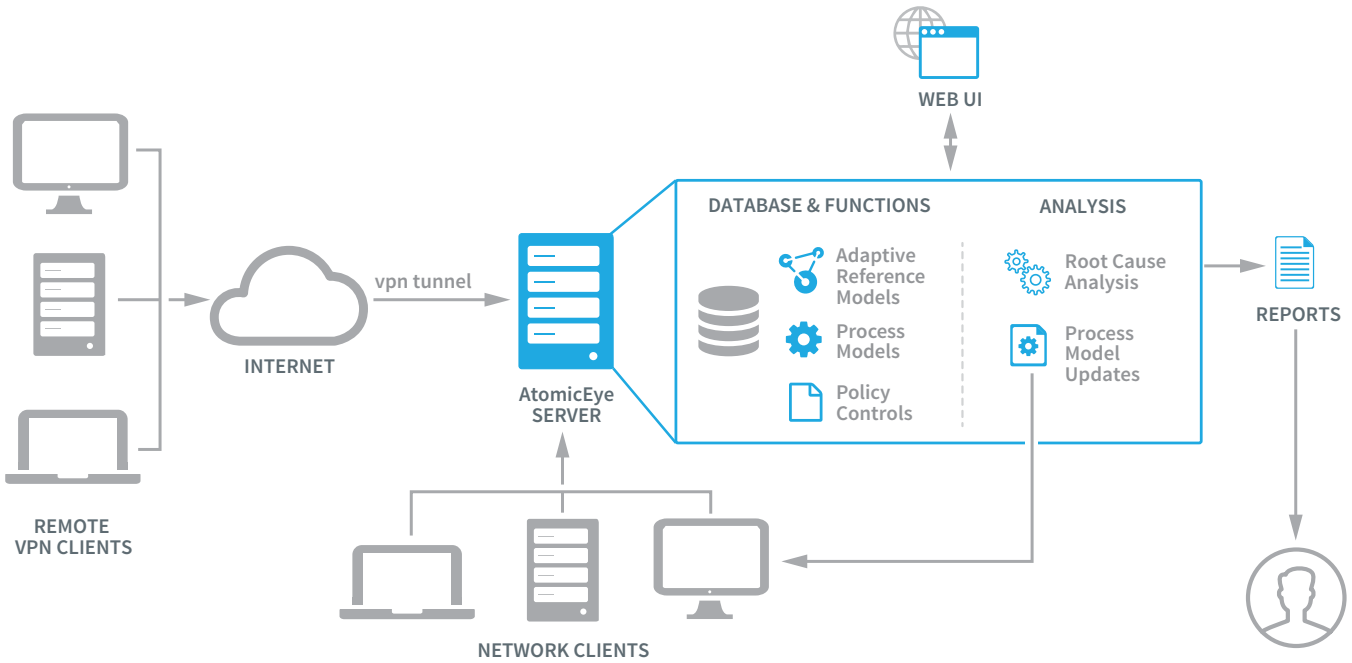
Instant Discovery and Near Real-Time Remediation: AtomicEye Finds What Others Cannot

As corporate networks face increasingly sophisticated attacks, it is clear that existing defenses are falling short. AtomicEye is the industry's first cybersecurity software solution that automatically detects and remediates exploits without the use of signatures of any kind. AtomicEye's patented machine learning enables AtomicEye to prevent attacks in near real-time as they are happening, even in volatile memory.

Persistent threats are automatically detected through continuous monitoring of over 1,000,000 attributes for each endpoint on the system. Intervention via AtomicEye happens during an attack or as part of best-practice cyber hygiene to reduce the attack surface of your system.

Remediation—automated and / or human-augmented—can be a repair of the total system to its pre-attack state without interrupting the user. Many organizations leverage this functionality within their asset management discipline to proactively empower configuration management, application management, asset (hardware / software) inventory, and patch auditing. AtomicEye can be deployed in a highly secure on-premise configuration or in a private cloud. Remote monitoring services are available to clients seeking to leverage advanced security expertise without adding staff.

Figure 1: Exploit Protection Analytics Approach



AtomicEye secures information on endpoint computers and systems in three ways:

Instant Detection

AtomicEye brings unprecedented visibility into machine behaviors, delivering an atomic-level view based on its capture of over over 1 million attributes for each machine. Its advanced algorithms and machine learning expose anomalies that indicate—with certainty, in real-time—the presence of advanced malware. AtomicEye prevents sophisticated in-memory exploits, APTs, zero-days, rootkits and targeted attacks. No signatures, whitelists, or any other form of prior knowledge is needed.

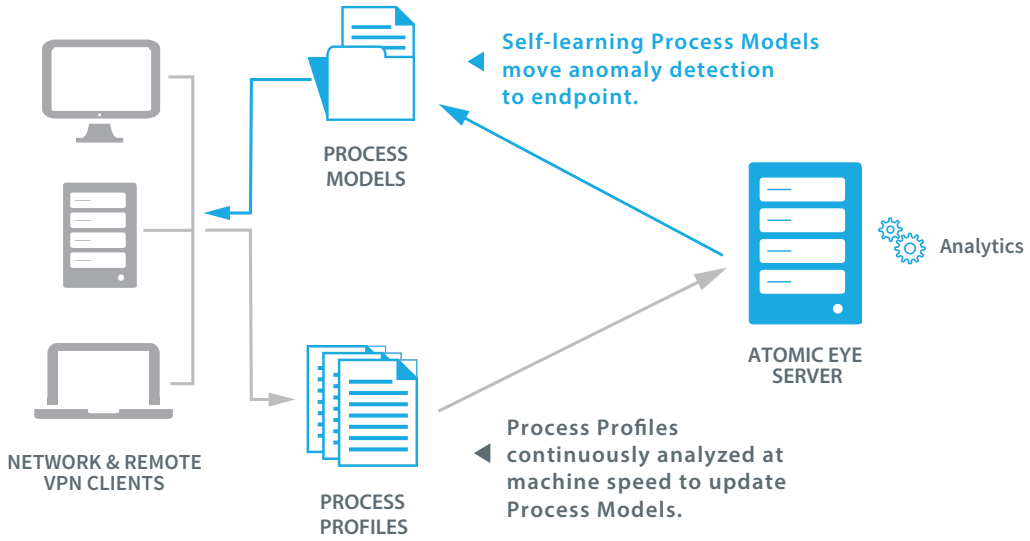
Rapid Response

The instant a potential threat is detected, remediation rulesets are activated that make it impossible for assets to be compromised. AtomicEye deploys granular scanning, change detection, machine learning and patented analytics to build a contextual remediation plan. The exploit and all of the associated collateral damage are surgically repaired, restoring the infected assets back to their original, pre-attack state. No re-imaging is required, and no interruption to the business operations is experienced.

Automated Remediation

AtomicEye stops the offending executable, repairs altered configuration settings, restores deleted or corrupted files, and closes open ports. File restoration occurs through our patented Donor Technology, which borrows intact files from uninfected machines to replace damaged files on infected machines. Remediation occurs instantly without the need to re-image or reboot, and without interruption to the user.

Figure 2: Memory Process Data Analysis



SUMMARY

AtomicEye requires little to no human action or interpretation, ensures no attacker can leave with proprietary information, and promises no interruptions to your business. Operate your business each day with the confidence that comes from knowing your endpoints are secure, configured, compliant, and ready for business in an increasingly hostile environment. Contact us to find out how you can deploy AtomicEye today.