Solution Brief

Automating Your Response to Automated Attacks

Automating incident response with eyeShare increases McAfee® Enterprise Security Manager's value

Ayehu and Intel Security have teamed up to accelerate incident response by integrating eyeShare v4.8 security process automation software with McAfee Enterprise Security Manager security information and event management (SIEM) system. Together, these industry-leading tools provide an enterprise-grade solution to easily automate and streamline security policy tasks (playbooks) executed in response to McAfee Enterprise Security Manager-generated alerts. The result is an immediate and reliable defense against detected threats to help mitigate damage from cybersecurity breaches. There will always be more security attacks than security staff, but eyeShare integrated with McAfee Enterprise Security Manager ensures that best practice responses are executed no matter who's on duty.

Manual Responses Are Losing Ground to Rising Volume of Cybersecurity Attacks

According to Gartner, "By 2019, 40% of large enterprises will require specialized, automated tools to meet regulatory obligations in the event of a serious information security incident." Since the vast majority of SOC's today investigate and remediate security incidents manually, this forecast heralds significant changes ahead for how enterprises deal with breaches to their IT environments.

Even IT organizations with plenty of qualified staff that have all the necessary expertise to carry out security operations properly can't be expected to keep pace with the growing volume of cybersecurity attacks, which are often automated.

ayehu

McAfee COMPATIBLE

McAfee Compatible Solution

Ayehu eyeShare v4.8

Security automation from eyeShare enables:

- Better preparation for cybersecurity Incidents.
- Data enrichment.
- Best practice responses 24/7/365.
- Automated playbooks.
- Rapid containment, eradication, and recovery.

intel Security

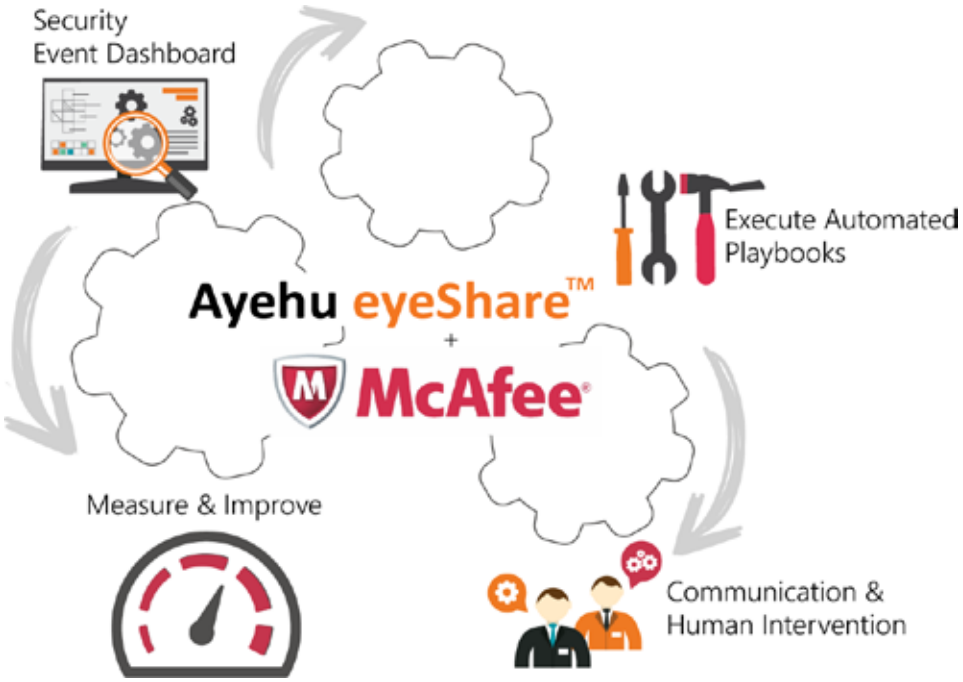


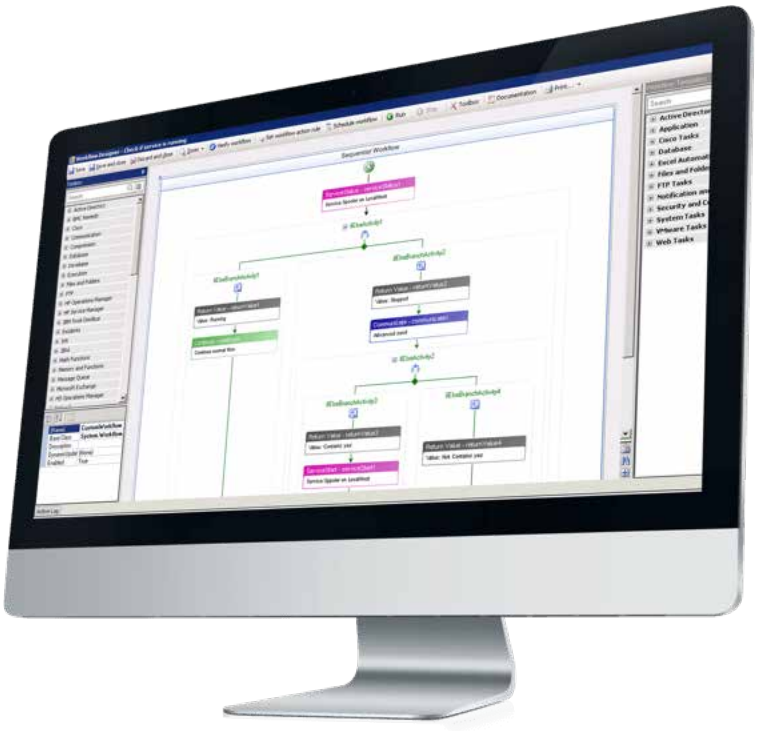
Figure 1. McAfee Enterprise Security Manager and eyeShare work together to automate incident response and resolution.

Intel Security and Ayehu Partner to Accelerate Incident Response

When it comes to remediating security breaches, automation is a force multiplier that makes the people on your staff far more effective at cybersecurity incident response than they would be responding manually without the help of any other tools.

eyeShare's enterprise-grade security automation capabilities integrated with McAfee Enterprise Security Manager is a solution that accelerates security incident resolution and mitigates financial losses caused by security breaches. Together, eyeShare and McAfee Enterprise Security Manager allow your SOC to automate multiple functions:

- **Data enrichment about security incidents:** eyeShare can collect relevant information about the context of the incident—which often must be integrated and correlated from multiple disparate systems—present it to SOC personnel for further analysis.
- **Best practice responses 24/7/365:** This ensures that the optimum incident response is executed no matter who's on duty.
- **Playbooks for numerous scenarios:** These help maximize response speed, reducing or eliminating human error and ensuring proper documentation and notifications.
- **Containment, eradication, and recovery:** The scope of damage from breaches can be mitigated, and systems can be returned to an operational state as rapidly as possible.



About Ayehu eyeShare

Ayehu is a cybersecurity operations and incident response automation provider that helps enterprise and medium-size IT organizations improve cybersecurity incident response time, reduce risk, and mitigate damage from breaches by automating playbooks that enable best practice responses 24/7/365. We do this with eyeShare, an easy-to-deploy enterprise-grade, agentless solution that seamlessly integrates with McAfee Enterprise Security Manager and many other tools.

About McAfee Enterprise Security Manager

McAfee Enterprise Security Manager—the foundation of the security information and event management (SIEM) solution family from Intel Security—delivers the performance, actionable intelligence, and real-time situational awareness at the speed and scale required for security organizations to identify, understand, and respond to stealthy threats, while the embedded compliance framework simplifies compliance.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com