TECH DRIVEN. PEOPLE POWERED.

Solution Brief: Wingman Vulnerability Management

Part of Wingman GRC

By preventing data breaches and other security incidents, vulnerability management can prevent damage to a company's reputation and bottom line. Additionally, vulnerability management can improve compliance with various security standards and regulations, including PCI DSS 4.0, GDPR, CCPA, PSD2, HIPAA, DORA, and FINRA.

As enterprise attack surface continues to grow exponentially both on-premises and in the cloud, the current practice of identifying, classifying, prioritising, and remediating vulnerabilities with multiple technologies and tools is ineffective.

Powered by Qualys, Wingman Vulnerability Management has built-in orchestration giving the ability to identify all known and unknown assets in your global IT environment automatically. Wingman Vulnerability Management allows customers to discover, categorise and workflow known and unknown assets within their infrastructure.

Identify assets automatically

Automatically discover and categorise known, unknown, internal and internet-exposed assets, and continuously identify unmanaged assets.

Detect vulnerabilities and misconfigurations

Continuously detect critical vulnerabilities and misconfigurations across mobile devices, operating systems, and applications per industry standards.

Reduction in administration through automation workflows

Workflows can be created allowing auto-remediation of specific issues using a set of flexible rules. Auto patch only what you are comfortable with. Discover, assess, prioritise, and patch critical vulnerabilities up to 50% faster.

Measure web applications and API risks

Get complete discovery, inventory and custom tagging of every web app and API asset across your environment, including on-prem, web apps, multi-cloud, API gateways, containers, microservices and more.

Risk remediation

Efficiently schedule tailored patch deployments. Improve end-user communication with prompts and messages to encourage patch installations to ensure that your patch remediation risk is reduced.

Streamline responses, identify root causes, and drive compliance. Enable patch installation on remote endpoints without a VPN, with binaries downloaded directly from the vendor.

Co-managed or consultancy support

SEP2's experts can co-manage your platform to ensure you are getting the most out of your Vulnerability Management. While having full visibility, take the guess work out of having it configured correctly. For a more hands-off approach, rest assured that SEP2 will be able to install, configure and monitor your vulnerability management while letting you know what's critical when you need to know.

Monthly or quarterly reporting

Keep on track with your choice of monthly or quarterly reporting on your assets and any patching that may be required.

Available modules

Core modules:

- Vulnerability Management, Detection & Response (VMDR)
- Web Application Scanning (WAS)
- Patch Management (PM)

Additional modules:

(Speak to your Sales Representative for more information)

Asset Management

- CyberSecurity Asset Management (CSAM)
- External Attack Surface Management (EASM)

Vulnerability & Configuration Management

- Enterprise TruRisk Management (ETM)

Risk Remediation

- Custom Assessment and Remediation (CAR)
- TruRisk Eliminate (TE)

Compliance

- File Integrity Monitoring

Cloud Security

- SaaS Security Posture Management (SSPM)
- Cloud Workload Protection (CWP)
- Cloud Detection and Response (CDR)
- Container Security (CS)

If you would like to discuss Wingman Vulnerability Management please get in touch at info@sep2.security