Integrity360

your **security** in mind

VULNERABILITY MANAGEMENT SERVICES

Vulnerability Management Services

The problem

Microsoft releases patches for vulnerabilities on its products every month. So does Oracle. And Cisco. Don't forget the countless other vulnerabilities that never get patches.

Each month there's an endless parade of vulnerabilities, with the next exploit being classified as more critical than the previous one. Continuously identifying the seemingly endless stream of vulnerabilities, reacting to them and managing emerging vulnerabilities are challenges that most businesses are trying to figure out how to solve.

The data shows that many organisations are struggling to come up with a solution. Last year, over 22,000 new vulnerabilities were disclosed during the year, according to Risk Based Security. The average company struggled to remediate more than 10 percent of them at any given time, according to Kenna Security and the Cyentia Institute.

Apart from simply applying patches, businesses need to also be aware of the zero-day vulnerabilities that are continuously being identified. With a lag time in-between discovery and remediation, organisations need to have robust controls that allow them to rapidly identify affected systems and implement mitigating controls in the interim, until a patch is released.

Given the sheer size of the attack surface many enterprises are tasked with defending, identifying and managing vulnerabilities are critical challenges.

Add in the significant skills gap that currently exists in the security analyst market and essential operational oversight quickly becomes a dangerously scarce commodity.

The key to successfully managing vulnerabilities lies in the cross section of:

- ✔ Identifying the physical and digital assets in the corporate digital estate.
- ✔ Dedicating resources to continuously scan, identify and interpret vulnerability findings.
- ✔ Prioritising and implementing mitigations for vulnerabilities in a timely, secure fashion.
- ✔ Operating in accordance with a governance and reporting structure that ensures vulnerability mitigations or remediations meet pre-determined Key Performance Indicators.
- ✔ Ensuring that the cyber security analysts tasked with the project have the skills and knowledge to carry it out.

The solution

Vulnerability scanning and exposure assessment shouldn't be a one-off, annual activity. Similarly, remediation shouldn't be limited to ad-hoc patching of systems.

Continuous vulnerability management plays a key role in a well-functioning cyber security strategy by covering a variety of compliance requirements and protecting the business from the legal and reputational risks associated with a security incident.

Integrity360's Managed Vulnerability Assessment Service helps you meet four of the six basic controls in the CIS Top 20 through a combination of continuous vulnerability scanning, on-going assessments and actionable vulnerability insights. These are:

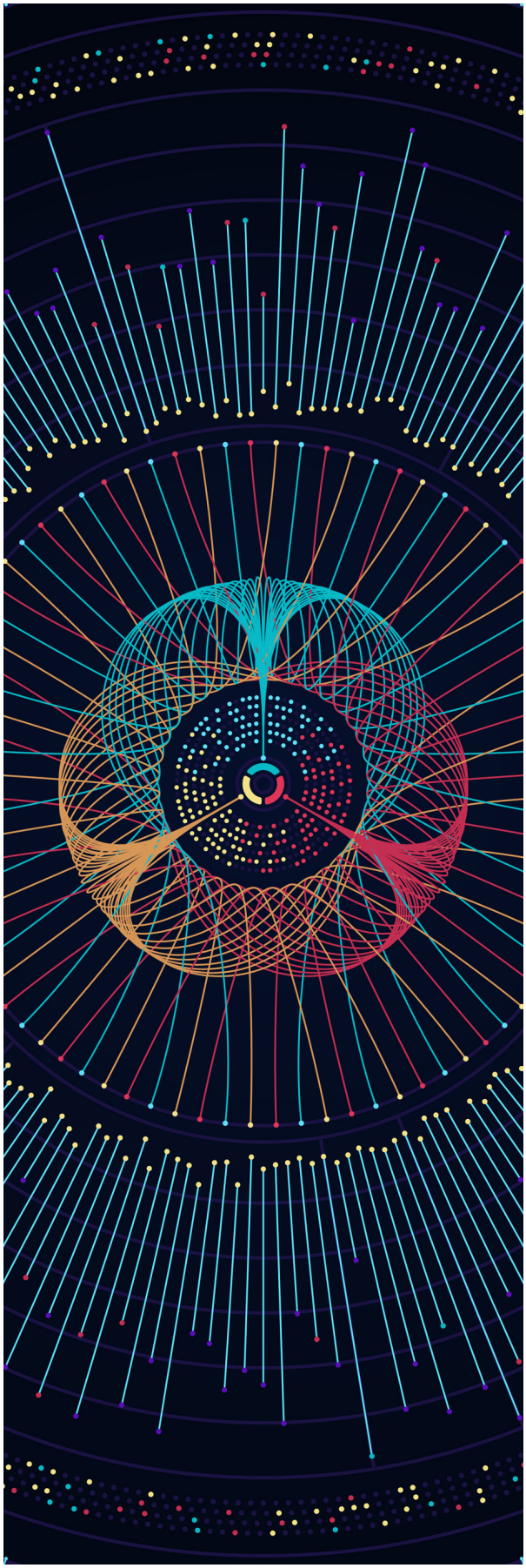
- ✔ Inventory and control of hardware assets
- ✔ Inventory and control of software assets
- ✔ Continuous vulnerability management
- ✔ Secure configuration for hardware and software on mobile devices, laptops, workstations and servers

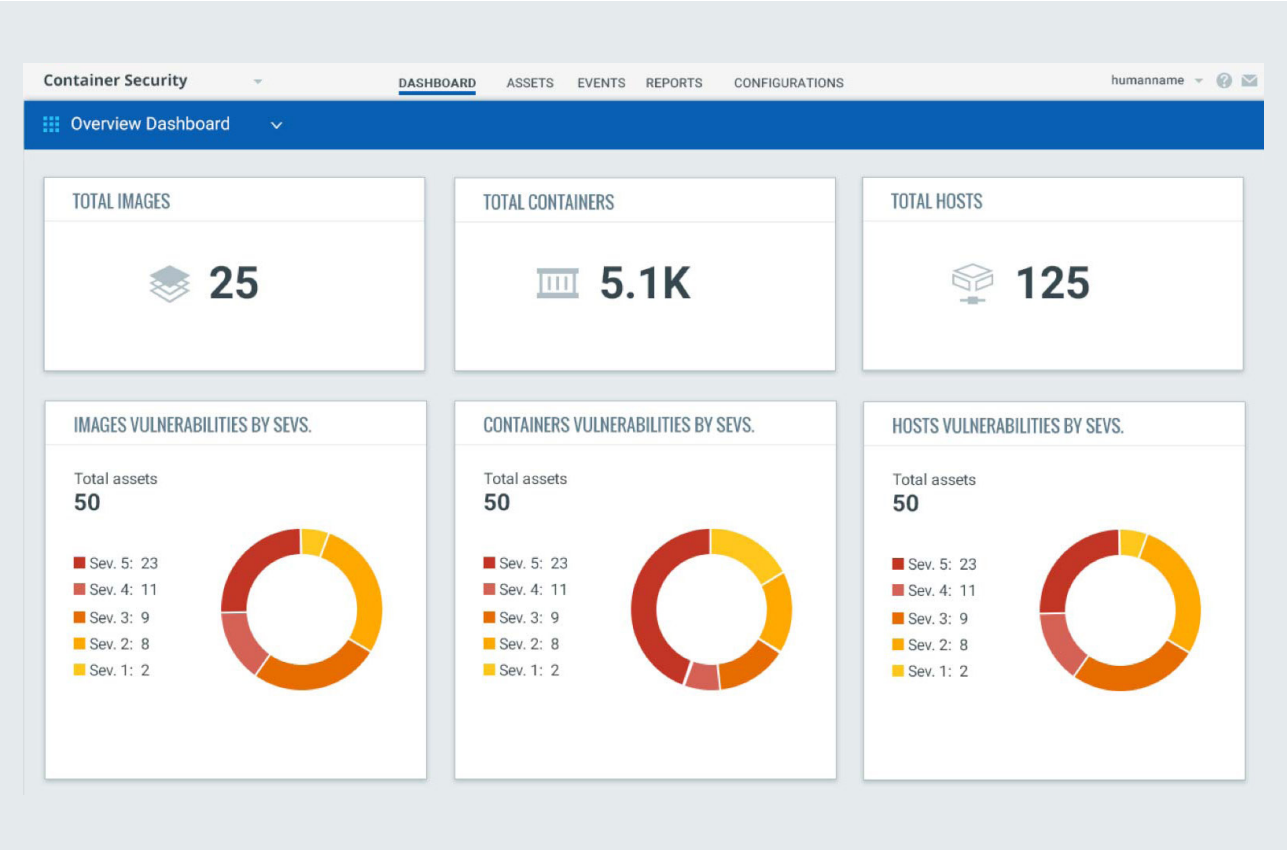
The service is offered at two levels, both of which can be tailored to align to your company's unique security strategy requirements and overall enterprise needs.

Our managed service provides fundamental support in helping companies get those basic controls right, in a world of cyber security that has grown increasingly complex.

We pride ourselves in not just being a solutions provider but being a security partner to our clients, working to understand your unique environment and act as a natural extension of your in-house team.

Our Managed Vulnerability Assessment Service is designed to deliver demonstrable value, valuable insight and continuous improvement of your security posture.





Managed Vulnerability Assessment Service Features

Our managed vulnerability assessment service expands on the on-demand, once-off vulnerability assessments offered by our cyber security testing team. The ad-hoc assessment serves as the baseline to develop a best-in-class managed vulnerability service.

Taking the initial engagement and turning it into a continuous service enables companies to greatly reduce their risk while simultaneously improving their security posture. We offer two levels of service – the first where we take care of all the tools and infrastructure for scanning and deliver regular, repeatable and reliable scan results to your own security analysts.

Don't have the analysts available to preform this specialised activity? Our next level service includes vulnerability assessments, where our qualified analysts review the scan outputs and provide a filtered, prioritised report with actionable insights. Further options are also available on a customised basis.

LEVEL 1

MANAGED VULNERABILITY SCANNING

Integrity360 deploys a cloud-based vulnerability scanning platform in the client's digital environment and continuously manages it. We perform scheduled vulnerability and asset discovery scans, which provides on-going reporting and the capability for self-service reporting and remediation.

Service features

1. Scanning infrastructure provision and costs bundled within the overall service, if needed.
2. Management of the scanning platform to ensure availability, reliability and performance.
3. Setup, onboarding and integration of client assets into the service
4. Regular monthly scanning and reporting including:
    a. Asset discovery
    b. Identifying vulnerabilities, prioritised based on criticality as identified automatically by best-of-breed toolset
5. Monthly reporting on service, capacity and security.
6. Quarterly service reviews.
7. Single predictable, recurring annually fee based on volume of estate.

LEVEL 2

MANAGED VULNERABILITY ASSESSMENT

Builds on the features of Level 1 by introducing an assessment from our Security Operation Centre (SOC) analysts to provide actionable insights. Our team prioritises vulnerabilities for your remediation based on vulnerability criticality and potential impact severity to the organisation. Vulnerabilities are continuously identified through a 24x7x365 management service and customers are alerted of critical vulnerabilities deemed to have a high potential for business impact.

Service features

1. Everything included in Managed Vulnerability Scanning.
2. Analysis and reduction of false-positive alerts.
3. Prioritisation of Vulnerabilities by Integrity360 analysts based on vulnerability severity and asset priority, informed by our real-world perspectives from the front-lines of cyber security.
4. Actionable insights.
5. Monthly reporting service, capacity and security.
6. Quarterly service reviews.
7. Single predictable, recurring annual fee based on volume of estate.

Managed Vulnerability Assessment Services Benefits

Continuous: Feeds the full life-cycle management of vulnerabilities and greater visibility of legacy vulnerabilities.	**Accessible**: Proactive human expertise pairs with a fully managed platform to provide automated reporting for decision-makers and board members.
Scalable: Empowers organisations to improve their security strategy through a function that fits to any architecture and supports modular capabilities.	**Cost-effective**: Modular licensing model supports on-demand incident analysis and remediation.
Actionable: Provides trending analysis on vulnerabilities within the digital estate which can fuel better business intelligence and visualise meaningful metrics.	**Supportive**: Enhances compliance against regulatory audits for NIST, ISO, PCI-DSS, SOX, CIS Top 20 and more.

Deployment and Operation

Integrity360's vulnerability management service is cloud-based, utilising always-on and always-available cloud infrastructure to perform scanning and identification of vulnerabilities.

Where necessary we're also able to deploy under a hybrid model, with on-premise network scanners and endpoint agents to provide greater visibility and flexibility of scans.

Through our mature onboarding process, the vulnerability scanning platform can be easily deployed with little impact to our clients' operations teams, giving additional insights into the array of hardware, software and cloud-based applications in use at any given moment.

By performing regular scans, our team can quickly identify vulnerabilities and provide a clear picture of what's in your environment and what needs to be addressed. This allows businesses to root out rogue assets before they become a threat.

Integrity360 SOC analysts are uniquely equipped to interrogate your vulnerability data to provide more meaningful insights.

Get Started Today

Integrity360 cyber security specialists have years of experience in assessing vulnerabilities on the digital estate, implementing vulnerability scanning platforms and continuously monitoring the digital infrastructure for threats. Work with us to ensure that your business maintains a proactive security stance in a field where new threats emerge daily.

Contact an Integrity360 advisor today to learn more about our services.

HEAD OFFICE
3rd Floor, Block D, The Concourse,
Beacon Court, Sandyford, Dublin 18.
+353 (0)1 293 4027

UK OFFICE
Church House, 32A Kneesworth
Street, Royston, SG8 5AB
+44 203 397 3414

NEW YORK OFFICE
260 Madison Avenue, 8th Floor
Manhattan, 10016
+1 212 461 3286

info@integrity360.com

www.integrity360.com

Integrity360

your **security** in mind