eSENTIRE

DATA SHEET

Managed Vulnerability Service

in partnership with Tenable

Comprehensive Vulnerability Management. Rapid Risk Reduction.

Your network is an ever-expanding ecosystem of dynamic assets. With applications spread across disparate systems, your expansive business environment presents potential blind spots threat actors can and will exploit. Resource limitations create challenges when trying to rapidly identify and remediate vulnerabilities before threat actors exploit them. Find your vulnerabilities and stop the clock before your business is disrupted with eSentire Managed Vulnerability Service.

COMPREHENSIVE VULNERABILITY IDENTIFICATION

Identify asset vulnerabilities with precision across traditional and dynamic IT assets for continuous visibility across your expanding business environment.

ACTIVE RISK PRIORITIZATION AND LIFECYCLE TRACKING

Focus on vulnerabilities that present the greatest potential risk with expert guidance to facilitate remediation prioritization against dangerous exploits.

DEDICATED EXPERTISE DRIVING CONTINUOUS OPTIMIZATION

Alleviate resource constraints with dedicated experts that provide end-to-end management and platform refinement for greater operational efficiency.

CO-MANAGED FLEXIBILITY WITH CUSTOMIZED REPORTING

Focus on vulnerabilities that present the greatest potential risk with expert guidance to facilitate accuracy and prioritization against dangerous exploits.

THE PROBLEM

Unpatched Vulnerabilities

of organizations that were breached in the past two years say the root cause was an unpatched known vulnerability[1]

Overwhemling Infrastructure

of security teams say software vulnerability volume is overwhelming[2]

Attackers Capitalize Faster Than Ever

decrease in the time window from vulnerability discovery to attack over the last two years[3]

[1]Ponemon Institute, "Today's State of Vulnerability Response: Patch Work Demands Attention", [2]Tenable/Enterprise strategy group, 2018
[3]Ponemon Institute, "Today's State of Vulnerability Response: Patch Work Demands Attention"

CONTRIBUTING FACTORS

Resource Constraints

People

- **64%** of organizations anticipate need for more headcount to support vulnerability management in the next 12 months[4]
- **29%** of all security personnel time is dedicated to managing vulnerability response[5]

Process

- **55%** of organizations are not satisfied with their ability to remediate[6]
- **65%** of organizations say lack of prioritization is a contributing factor to patching delay[7]

Technology

- **51%** of organizations are not satisfied with their ability to scan for vulnerabilities[8]
- **56%** of organizations are not satisfied with analysis and prioritization out of current tools[9]

THE SOLUTION

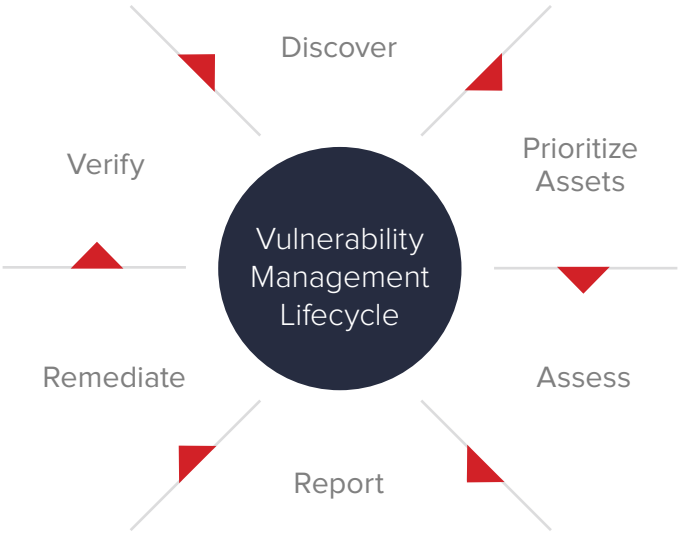
Managed Vulnerability Service, in partnership with Tenable, identifies vulnerabilities with precision across traditional and dynamic IT assets such as mobile devices, OT, IoT, virtual machines and cloud instances for full visibility across your business environment. Integrated eSentire experts are an extension of your team providing analysis and guidance that facilitates accuracy of asset classification and lifecycle tracking with prioritization of risk contextual to your business objectives. Delivered as a flexible co-managed model with you, Managed Vulnerability Service alleviates the managerial burden for your team providing continuous platform refinement and progress measurement. Your team receives full system access to run customized scans and reports for greater operational efficiency and satisfaction of regulatory requirements.

WHAT DOES MANAGED VULNERABILITY SERVICE SOLVE FOR?

- Continuous identification and tracking of new and existing assets
- Flexibility and timely scanning completion
- Scan accuracy and contextual risk prioritization
- Reducing time frame from vulnerability discovery to remediation
- Continuous optimization and tuning of vulnerability scanning platform
- Comprehensive tracking of vulnerability lifecycle
- Time and effort to analyze and prioritize remediation
- Resource expenditures investigating false positives
- Vulnerability closure verification
- Human resources dedicated to vulnerability management
- Increasing regulatory and reporting requirements (PCI, GDPR, SEC, FINRA, HIPAA, etc.)

[4] Ponemon Institute, "Today's State of Vulnerability Response: Patch Work Demands Attention", [5] Ponemon Institute, "Today's State of Vulnerability, [6] Skybox Security: Enterprise Vulnerability Management Report, [7] Ponemon Institute, "Today's State of Vulnerability Response: Patch Work Demands Attention [8,9] Skybox Security: Enterprise Vulnerability Management Report

HOW DOES IT WORK?



Discover

- Managed Vulnerability Service team schedules and executes regular scans of internal and external IT assets
  - Monthly scans of internal assets
  - Weekly scans for external assets
- Co-managed model gives you access to ad-hoc scanning and reporting
- Managed Vulnerability Service team alerts with newly discovered critical vulnerabilities

Prioritize and assess

- Managed Vulnerability Service team works with your team to continuously redefine your unique risk profile
- Assets are grouped, categorized and tracked for quicker analysis and visualization
- Managed Vulnerability Service team analyzes and prioritizes vulnerabilities that present the greatest risk

Report

- Managed Vulnerability Service team prepares and delivers a customized report bundle
  - Executive summaries for non-technical audiences
  - Detailed summary for technical audiences
- Pre-configured and customizable dashboards available in Tenable.IO

Remediate and verify

- Managed Vulnerability Service team monitors scans for errors and accuracy
- Managed Vulnerability Service team provides guidance and recommendations during remediation process
- Ad-hoc scanning to verify vulnerabilities have been remediated effectively

FEATURES

Comprehensive Visibility
Industry-leading IT asset coverage with scanning available for more than 109,000 vulnerabilities.

Elastic License Model
Assets-based licensing built for dynamic and quickly changing environments that consumes a single license unit per asset, even if the asset has multiple IP addresses.

Dynamic Asset Tracking
Group and classify assets in a single pane of glass with attributes beyond IP addresses to more accurately identify and prioritize new and existing vulnerabilities.

Business Contextual Risk Prioritization
eSentire dedicated Managed Vulnerability Service experts provide risk prioritization and guidance specific to your unique business context.

Continuous Optimization and Focused Guidance
eSentire dedicated Managed Vulnerability Service experts become a genuine extension of your team providing end-to-end management that optimizes the vulnerability management lifecycle including remediation guidance, verification, scan quality assurance, and weekly communication on newly discovered vulnerabilities.

Executive and Technical Reporting
Custom executive and detailed summary reporting available for technical and non-technical audiences.

Regulatory Requirement Reporting
Pre-built compliance reporting and dashboards for multiple security frameworks including PCI, NIST, ISO, and CIS.

Co-managed Flexibility
Full system access and flexibility to run your own customized scans and reporting alongside eSentire's dedicated Managed Vulnerability Service experts.

Web Application Scanning (Add On)
Safely and accurately scan your web application portfolio without the worry of performance latency or disrupting your development team.

PCI Approved Scanning Vendor Solution (Add On)
Streamline and comply with quarterly scanning requirements required by PCI 11.2.2.

MAKE THE CASE FOR MANAGED VULNERABILITY SERVICE

DIY vs. Typical Provider vs. Managed Vulnerability Service

eSentire's Managed Vulnerability Service service is a single tier, all-inclusive, and completely transparent. Typically, vulnerability management service offerings from legacy service providers have multiple tiers of service levels with hidden costs and confusing service level agreements.

	DIY	Typical Service Provider	eSentire
Recruiting, retaining and dedicating knowledgeable IT security staff to manage and analyze scans	Required	Not Required	Not Required
Comprehensive pre-built and customized reporting for various audiences (executive, technical, regulatory)	✗	✓	✓
Sourcing, set-up, platform maintenance	✓	✓	✓
Ad Hoc scanning	✓	Extra Cost	✓
Ongoing vulnerability prioritization contextual to evolving business risk profile	✗	Extra Cost	✓
Scan accuracy verification and continuous optimization accounting for changing IT environment	✗	Extra Cost	✓
Ongoing threat intelligence communications on emerging vulnerabilities	✗	Extra Cost	✓

BENEFITS

- Identifies vulnerabilities across dynamic and expanding IT assets
- Improves scanning consistency and timeliness
- Tracks and measures the vulnerability lifecycle
- Prioritizes remediation against greatest potential business risk
- Verifies remediation and quality assurance
- Minimizes the vulnerability discovery to remediation timeframe
- Tracks and measures programmatic improvements
- Reduces operational, staffing and resource constraints
- Satisfies regulatory requirements

About eSentire:

eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business-disrupting events. Protecting more than $6 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.eSentire.com** and follow **@eSentire**.