SOLUTION BRIEF

eSentire Risk Advisory and Managed Prevention (RAMP)

Adaptive Cybersecurity at the Speed of Your Business

Attackers Evolve.

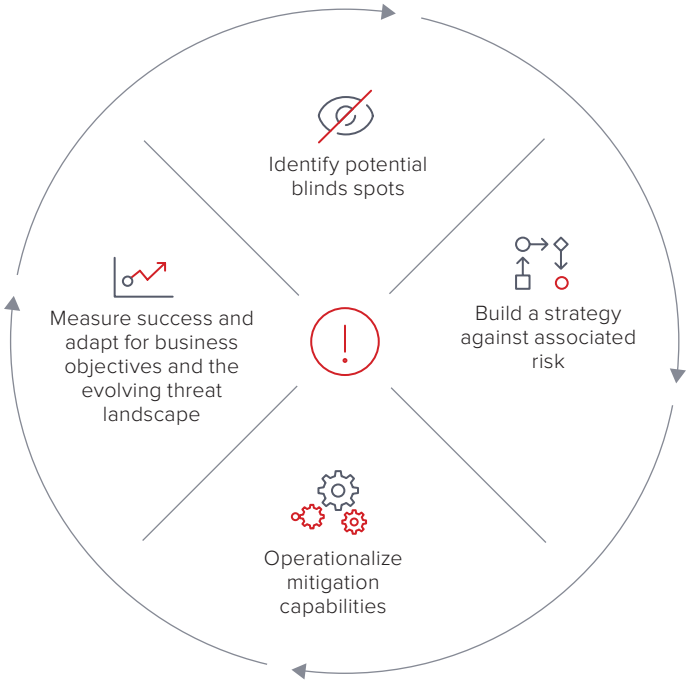
Risk is in Constant Fluctuation.

Security is a Never-ending Cycle.

Organizations Must Continuously Defend and Adapt.

THE PROBLEM

Evidenced by daily breach headlines, a security model that reactively invests in disparate solutions is inadequate. Without predictive and adaptive security that simultaneously addresses digital transformation, business objectives and unique threat landscapes, you risk on-going business disruption and regulatory penalties. As attacks come faster than ever, security teams are inadequately resourced to continuously:



- **54%** of attackers can complete an attack and exfiltrate data in under 15 hours[1]
- **56%** of organizations had a cybersecurity incident that resulted in business distruption in the last 2 years[2]
- **18%** of CISOs predict their organization will be fined for non-compliance in the next year[3]
- **72%** of security practitioners believe the rush to digital transformation increases data breach and cybersecurity[4]

[1] *The Black Report: Decoding the Mind of Hackers, 2018*
[2] *Ponemon Study: Cyber Resilient Organization, March 2018*
[3] *Ponemon Study: What CISOs Worry About, January 2018*
[4] *Ponemon Study: Bridging the Digital Transformation Divide, March 2018*

THE SOLUTION

eSentire Risk Advisory and Managed Prevention (RAMP) continuously identifies blind spots, builds a strategy around risk and operationalizes capabilities to predict and prevent known threats. Complimentary to our Risk Advisory and Managed Prevention suite of services, eSentire Managed Detection and Response (MDR) hunts and responds to the unknown. As a result, your security function is able to measure success over time and becomes adaptable to business performance drivers and the evolving threat landscape without increased risk or gaps in compliance mandates.

Identify

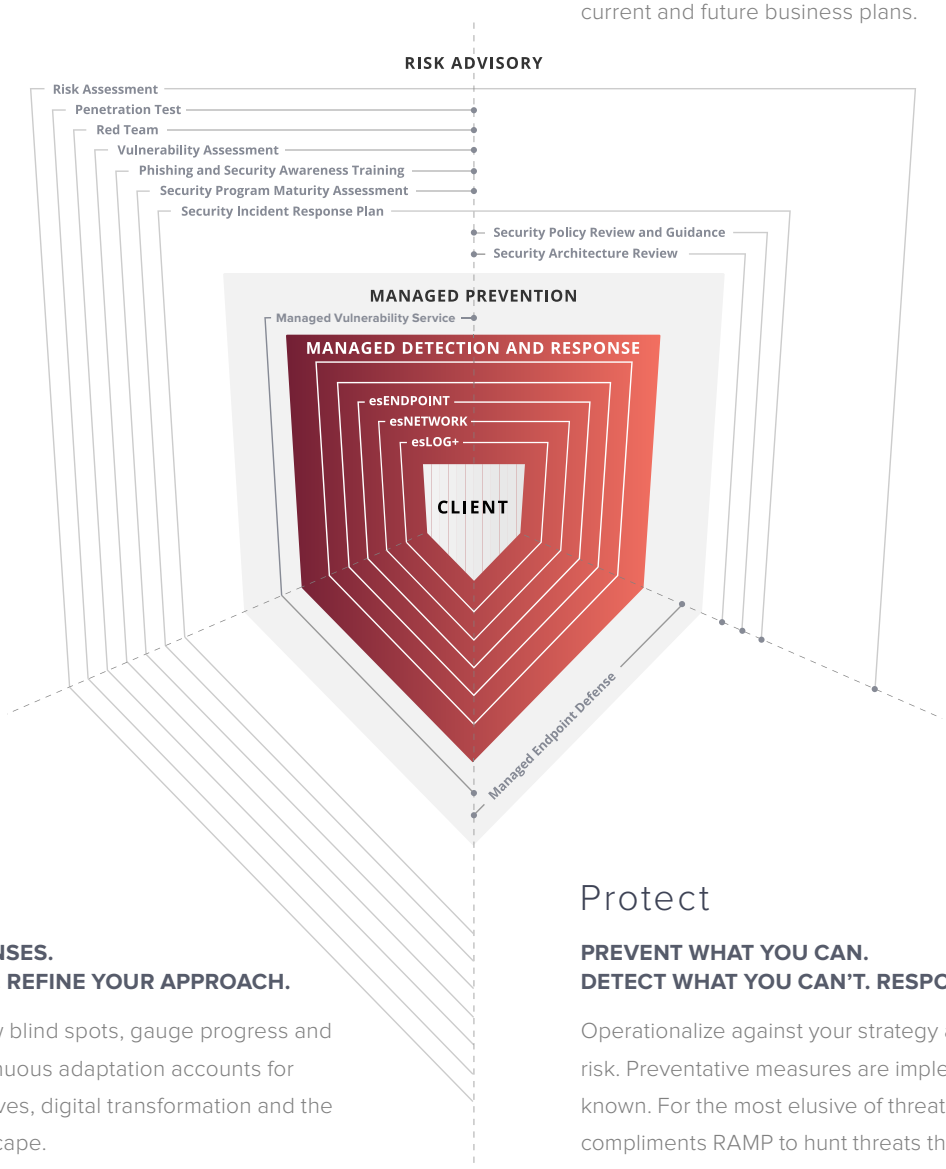
TEST YOUR DEFENSES.
ILLUMINATE BLIND SPOTS. DETERMINE RISK.

Assess your people, process, policies and technology for systemic risk that threat actors thrive on. From on-premises to the cloud, identify potential security gaps and resulting risk to your organization.

Build

ESTABLISH YOUR BASELINE. BUILD A STRATEGY.
DEFINE YOUR PLAN.

Evaluate your current security program maturity, policies, architecture and response capabilities. Risk is weighted against current strategic and tactical capabilities and a comprehensive and measurable plan is built accounting for current and future business plans.



Measure

REEVALUATE DEFENSES.
ASSESS PROGRESS. REFINE YOUR APPROACH.

Test defenses for new blind spots, gauge progress and refine strategy. Continuous adaptation accounts for new business objectives, digital transformation and the evolving threat landscape.

Protect

PREVENT WHAT YOU CAN.
DETECT WHAT YOU CAN'T. RESPOND SWIFTLY.

Operationalize against your strategy and areas of greatest risk. Preventative measures are implemented to block the known. For the most elusive of threat actors, eSentire MDR compliments RAMP to hunt threats that bypass preventative measures with integrated response capabilities to stop attackers before they can achieve their objectives.

Identify

WHAT DOES RAMP IDENTIFY?

- Known, surface-level security issues and misconfigurations
- Defensive blind spots and areas of greatest risk (people, process and technology)
- How prevention, detection and response capabilities stand up to the latest threat actor tactics, techniques and procedures
- Threats to assets and resources
- Threat actors already in an environment and new attacks over an extended timeframe
- Security program maturity and gaps that present potential business and operational risk
- Appropriate processes and procedures to quickly contain and remediate an attack
- Security investment tied to top risks and future roadmap

RISK ADVISORY SERVICES

- Vulnerability Assessment
- Penetration Test (Standard, Wireless, Web, App, Mobile)
- Phishing
- Red Team
- Risk Assessment
- Security Program Maturity Assessment (SPMA)
- Security Incident Response Plan (SIRP)

MANAGED PREVENTION SERVICES

- Managed Vulnerability Service

Build

WHAT DOES RAMP ASSESS AND BUILD?

- The security program's current state and roadmap for improvement
- Alignment of business objectives, risk and security strategy
- Organization-wide buy-in with effective resource allocation
- Security controls aligned to areas of greatest risk
- Systems, tools and processes to effectively implement or update an existing program
- Organizational security policies and duties
- Prioritization of changes and operational alignment
- Implementation of evolving regulatory requirements
- Adequate people and right mix of skills to effectively execute
- Security incident response plans and remediation opportunities

RISK ADVISORY SERVICES

- Security Program Maturity Assessment (SPMA)
- Security Incident Response Plan (SIRP)
- Security Policy Review & Guidance (SPRG)
- Security Architecture Review (SAR)
- Risk Assessment

Protect

HOW DOES RAMP PROTECT THE ORGANIZATION?

- Operationalizes rapid, accurate, and valuable use of endpoint prevention functionality
- Stops threats at the endpoint level before objectives can be achieved
- Minimizes threat actor dwell time
- Reduces costly staffing, management, and ongoing maintenance so resources can be focused on higher priorities
- Satisfies compliance mandates

MANAGED PREVENTION SERVICES

- Managed Endpoint Defense

Measure

WHAT DOES RAMP MEASURE?

- Emerging risks on the horizon and how they will affect an organization
- Different courses of action to take if risks increase to an unacceptable level
- Where an organization is on the maturity curve and progress toward desired "future state"
- Evolution of security program against threat landscape contextual to business objectives
- How security measures will hold up to the latest attacker's tactics, techniques and procedures
- If security investment is appropriate against business risks and objectives

RISK ADVISORY SERVICES

- Vulnerability Assessment
- Penetration Test (Standard, Wireless, Web, App, Mobile)
- Phishing
- Red Team
- Risk Assessment
- Security Program Maturity Assessment (SPMA)
- Security Incident Response Plan (SIRP)

MANAGED PREVENTION SERVICES

- Managed Vulnerability Service

SERVICES FOR THE SPEED OF YOUR BUSINESS

Risk Advisory

Vulnerability Assessment
A point-in-time exercise utilizing a scanning tool that deliberately probes a network or system to discover weaknesses. Results analyzed by security experts and prioritized by severity with remediation guidance.

Penetration Test (Wireless, Web App, Mobile)
Simulates actions of an external and/or internal attacker. Using the latest tactics, techniques and procedures, penetration tester attempts to infiltrate and exploit systems and gain access to data. Exercise results in identification of systematic weaknesses with areas of remediation ranked by criticality.

Phishing
Tests end users through customized simulated phishing engagements. Users that present potential risks via exploitation of the human element are identified and remediation guidance is provided to implement into security awareness programs.

Red Team
Combines various techniques to evade detection and prevention capabilities, including OSINT, phishing, wireless and covert physical and network attack tactics, techniques and procedures. Exercise results in assessment of prevention, detection and response capabilities against real-world scenario and identifies areas of greatest risk and remediation recommendations.

Risk Assessment
Identifies risk across four key areas: organizational, programmatic (security), human and technical. Leveraging intelligence from our MDR platform, we identify and organization's risk measured via assessments against industry standard frameworks, technical testing, phishing and malicious network activity monitoring.

Security Program Maturity Assessment
Security Program Maturity Assessment (SPMA) is the foundation for the vCISO program, providing in-depth assessment of the client's information technology environment maturity.

Security Incident Response Planning
Security Incident Response Planning (SIRP) develops a focused and pragmatic plan that identifies key steps to take when a security event happens.

Security Policy Review and Guidance
A fully realized Information Security Program that provides specific best practices for policies and procedures based on the eSentire Security Framework and NIST Cybersecurity Framework.

Security Architecture Review
Reviews technologies currently in use by your organization and provides detailed security controls and audit assessment criteria to secure the system.

MANAGED PREVENTION

Managed Vulnerability Service
Scans servers, databases, endpoints and web applications for known vulnerabilities. Security experts deliver actionable reporting and advice to remediate critical vulnerabilities and keep your organization safe.

Managed Endpoint Defense
Accelerates time to value quickly deploying, operationalizing and hardening industry leading Next-Generation Antivirus protection preventing attackers from executing payloads and compromising systems.

WHY eSENTIRE

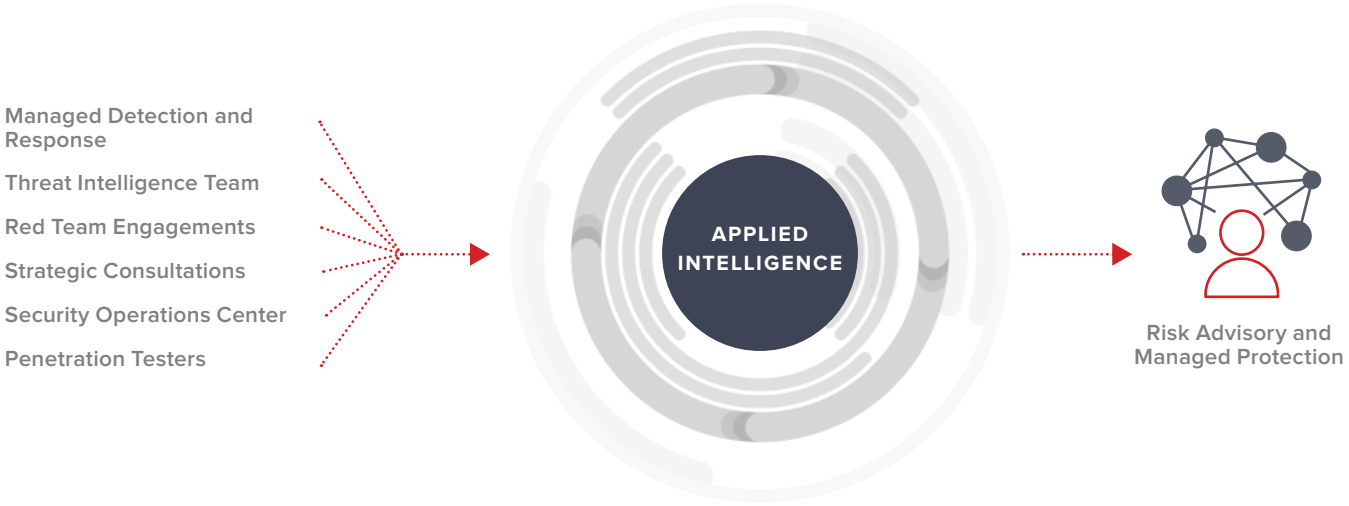
Adaptability

Wherever you are in your security journey, RAMP's services adapt to your unique requirements. Whether your organization is building your security function from the ground up or you are ready to be tested and operationalize against the industry's most sophisticated threat actors, RAMP helps you meet business objectives and account for your unique threat environment.

The Network Effect

RAMP integrates and applies practical intelligence to ensure your organization is measured and protected against the latest threats and compliance mandates derived from:

- eSentire's Global SOC that hunt and find threats that evade preventative measures via our MDR services
- Lessons learned from eSentire's Penetration Testers and Red Team that find new and elusive ways to break into client networks
- eSentire's Threat Intelligence Team that digs for the latest techniques, tactics and procedures used by today's threat actors
- Lessons collected from eSentire's Strategic Consulting Team that helps organizations harden their business and systems against the evolving threat landscape



eSENTIRE

eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyberattacks 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**.