eSENTIRE

DATA SHEET

Managed Risk Programs for Cloud Transformation

Close gaps and mitigate risk as your network evolves.

FUTURE-PROOF CLOUD MATURITY

Advisory experts assess cloud security maturity against industry leading frameworks and business objectives, plotting a course for measurable improvement in your program.

COMPREHENSIVE RISK IDENTIFICATION

Simulated cyberattackers test the efficacy of your cloud prevention, detection and response capabilities with detailed findings and recommendations for increased cybersecurity resiliency.

CLOUD TRANSFORMATION

MATURITY

ARCHITECTURE

POLICIES

TESTING

RESPONSE

VIRTUAL CISO (vCISO)

Navigating the terrain of information security risk and compliance is challenging enough in traditional network environments. Now, cloud transformation adds a new dimension that your organization must account for in its security program. And, a deficit of skilled infosec experts makes it nearly impossible for small- to medium-sized businesses (SMBs) to recruit and retain staff who know how to secure data in the cloud. As a result, many resort to cross-functional efforts to piece together policies that may technically check compliance boxes, but don't align with a clear risk strategy or business goals.

vCISO (CONT.)

of SMBs do not have a CISO that determines security policies[1]

claim that no single function determines IT security policies[2]

BIGGEST OPERATIONAL CHALLENGES PROTECTING CLOUD WORKLOADS[3]		eSentire vCISO
Compliance	34%	✓
Setting consistent security policies	31%	✓
Lack of qualified staff	31%	✓

eSentire vCISO augments your team with a dedicated security policy and compliance expert to develop a scalable program that accounts for industry best practices and regulatory frameworks. In contrast to "one-and-done" or piecework consulting models, vCISO is designed to build momentum and measure progress over a longer term, ensuring your program is adaptable and resilient to the evolving threat landscape.

CORE AREAS COVERED

- Overall security program maturity assessment and recommendations based on the NIST Cybersecurity Framework and Cloud Security Alliance controls
- Policy guidance
- Incident response planning and tabletop exercises
- Security architecture review
- Third-party/vendor risk management
- Vulnerability management
- Security culture and awareness

DELIVERABLES

- Dedicated vCISO expert
- Annually updated plans customized to your risk profile and business objectives
- Quarterly health check
- Workshops pertaining to in-scope core areas
- Reporting pertaining to in-scope core areas
- Ad hoc support and guidance throughout the engagement

[1,2] Ponemon, 2018 State of Cybersecurity in Small and Medium Sized Businesses
[3] ISC(2), 2019 Cloud Security Report

PENETRATION TESTING

Discover your organization's cloud security weaknesses and blind spots with eSentire penetration testing. Certified experts simulate and/or exploit common cloud security threats to identify areas of risk in your security posture and deliver comprehensive reporting and remediation recommendations to inform corrective actions.

BIGGEST SECURITY THREATS IN THE CLOUD[4]		eSentire Penetration Testing
Unauthorized access	42%	✓
Insecure interfaces / APIs	42%	✓
Cloud platform misconfiguration	40%	✓
Hijacking of accounts	39%	✓
External sharing / exposed data	37%	✓
Malicious insiders	30%	✓

PENETRATION TESTING TYPES

EXTERNAL

The classic attack scenario, simulating an attacker trying to penetrate your defenses from outside your network.

INTERNAL

Test your internal security posture. Simulate the actions of an attacker or a malicious insider who already has access inside your network.

RED TEAM

"No holds barred." A long-term and intensive engagement designed to test your organization's ability to detect and respond to a sophisticated adversary.

METHODOLOGY

1 | Customized scoping and rules of engagement

2 | Test Execution

- Recon (passive, active, open source intelligence gathering)
- Open port and service enumeration
- Discovered vulnerability validation
- Exploitation
- Critical vulnerability notification (customer immediately notified if a critical vulnerability is dicovered)
- Bruteforcing and/or password spraying

3 | Debrief and reporting

DELIVERABLES

⊕ Detailed technical report

- Executive summary targeted toward a non-technical audience so they are aware of the discovered risks from the test
- Methodology employed
- Positive security aspects identified
- Technical finding of the discovered vulnerabilities and risks
- Remediation recommendations

⊕ Post-report re-scan

- Included in engagements to validate remediation of identified vulnerabilities

[4] *ISC(2), 2019 Cloud Security Report*

THE eSENTIRE MANAGED RISK PROGRAMS DIFFERENCE

18+
years offering cybersecurity advisory services

175+
advisory service customers

96%
reported overall improvement in their security posture

PERSONNEL PROFILE

vCISO

Average years of experience: **15+**

Average eSentire tenure: **3+**

Certifications: **CISSP, CISM, CRISC, CISA**

PENETRATION TESTING

Average years of experience (Pen Tester) : **15+**

Average eSentire tenure: **3+**

Certifications: **OSCP, CISSP, CISM, SSCP**

"We now have trust in our defensive posture."

Chief Information Officer
Medium enterprise consumer products company

"We know more about what is happening on our network, inner and outer. This leads to greater peace of mind, and we can respond appropriately. Thank you."

IT Analyst
Large enterprise professional services company

eSENTIRE

eSentire, Inc., the global leader in Managed Detection and Response (MDR), keeps 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 $5.7 trillion AUM in the financial sector alone, 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**.