esCLOUD

Critical visibility. Rapid response. Transform to the cloud with confidence.

Transform with confidence
Assess risks, identify gaps and establish measurable benchmarks that support continuous business innovation.

Adapt without resource restrictions
Reduce complexity, alleviate resource constraints with dedicated experts that align to shared security responsibility and regulatory requirements.

Hunt threats without limitations
Identify expected and unexpected risks with 24x7x365 integrated threat hunting augmented by machine learning capabilities.

Respond wherever workloads reside
Quickly contain cloud threats with integrated response facilitates co-remediation and root cause determination.

esCLOUD INFRASTRUCTURE
- INFRASTRUCTURE
- THREAT DETECTION AND RESPONSE
- AZURE
- AWS
- GOOGLE CLOUD
- CLOUD INSIGHTS
- MALICIOUS BEHAVIOR
- VULNERABILITIES
- ASSET DISCOVERY
- MISCONFIGURATION

SaaS APPLICATIONS
- SaaS APPLICATIONS
- THREAT DETECTION AND RESPONSE
- DROPBOX
- SALESFORCE
- OFFICE 365
- GSUITE
- SERVICENOW
- BOX
- CUSTOM APIs

TRANSFORMATION
- CLOUD MATURITY
- CLOUD POLICIES
- CLOUD RESPONSE
- CLOUD ARCHITECTURE
- CLOUD TESTING
FEATURES

SECURE CLOUD TRANSFORMATION

Future-Proof Cloud Maturity
Advisory experts assess cloud security maturity against industry leading frameworks and business objectives plotting a course for measurable improvement in cybersecurity resiliency across security policies, architecture and incident response planning.

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.

FULL SPECTRUM CLOUD VISIBILITY

WORKLOADS

Infrastructure
Integrates with your AWS, Azure and GCP environments, providing a comprehensive view into potential malicious activity.

Applications
Collects and analyzes data with searchable trails of user activity, empowering unmatched anomaly detection that protects sensitive data and applications.

Extensive Integrations
Provides visibility across an extensive library of cloud-based applications and technologies, including Office 365, Salesforce, GSuite, ServiceNow, Dropbox, Box, Duo, Okta, Docker, Kubernetes, Zscalar, and more.

INSIGHTS

Vulnerability Management
 Continuously identifies vulnerabilities across your cloud assets with expert analysis and guidance that facilitates tracking, prioritization and remediation of risk.

Dynamic Asset Tracking
 Pinpoints the true identity of every resource in your cloud environment, enabling end-to-end identification and tracking of all assets in your cloud environment including shadow IT and unauthorized usage.

Misconfiguration Identification
Monitors system, database and application configuration change management processes utilizing best-in-class benchmarks, such as CIS and DISA STIG.

Container Security
 Provides end-to-end visibility and monitoring of container images, enabling seamless and secure DevOps production.

THREAT DETECTION AND RESPONSE

Machine Learning Integration
Machine learning and predictive analytics make sense of expected and unexpected behavior across your environment with pattern, anomaly and outlier detection accelerating investigation of potential threats.

Integrated human threat hunting
Elite security analysts perform deep forensic investigation aggregating and correlating disparate data from your cloud environment and other sources to identify elusive threats

Rapid Remediation of Threats and Misconfigurations
eSentire SOC analysts facilitate timely remediation of identified threats and policy violations reducing potential threat actor dwell time and exposures of your cloud assets.
Co-Managed Access
Co-managed model with access to run your own advanced search queries, generate alerts, manage profiles, run reports and investigate events alongside our SOC analysts.*

Real-Time Search and Visualizations
Preconfigured and customizable searches and dashboards with KPIs, giving our SOC analysts and your security team visibility into abnormal behaviors illuminating what matters most.

Compliance Management Reporting
Ensures compliance mandates are met with centralized logging, continuous monitoring and automated retention policies with various out-of-the-box and custom security reports that meet regulatory requirements such as HIPAA, PCI, SEC, GDPR and more.

*Managed Vulnerability Service and esLOG+ only

HOW DOES IT WORK? WHAT DOES IT SOLVE FOR?

1. Critical visibility with integrated threat detection and response across:
   - Cloud assets
   - Misconfigurations
   - Containers
   - Vulnerabilities
   - Malware and ransomware
   - Unauthorized access
   - Insecure interfaces/APIs
   - Hijacking of accounts
   - Malicious insiders
   - Rogue usage
   - Data sharing
   - Exfiltration

2. Maturation of cloud security:
   - Strategy and roadmap
   - Risk management
   - Policies and governance
   - Operations
   - Information management
   - Architecture
   - Response procedures
SHARED RESPONSIBILITY ALIGNMENT

| Cloud Security Program, Policies, Architecture and Response |
|-----------------|-----------------|-----------------|
| User Access     | User Access     | User Access     |
| Data            | Data            | Data            |
| Applications    | Applications    | Applications    |
| OS              | OS              | OS              |
| Network Traffic | Network Traffic | Network Traffic |
| Hypervisor      | Hypervisor      | Hypervisor      |
| Infrastructure  | Infrastructure  | Infrastructure  |
| Physical        | Physical        | Physical        |

Client Responsibility

Cloud Provider Responsibility

- esLOG+
- Managed Vulnerability Service
- Cloud Transformation
- esCLOUD for IaaS

MAKE THE CASE FOR esCLOUD

Protecting your cloud environment requires large investments across staff, operational tools, implementation, maintenance and technology. Constrained budgets spread across the entirety of the cybersecurity function leave most small and medium businesses (SMBs) with inadequate investment to monitor and manage threats across growing cloud workloads. Deployed and operational in a fraction of the time and cost versus a do-it-yourself (DIY) model, esCLOUD grows with your cloud environment, mitigating cloud risk with critical insights and 24x7x365 threat detection and response. In addition, esCLOUD extends to on-premises monitoring and infrastructure insights enabling protection across hybrid environments at little to no additional cost.

ALLEVIATES RESOURCE CONSTRAINTS

| Provisioning of technologies | ✔ |
| Onboarding and implementation | ✔ |
| Platform management and ongoing refinements | ✔ |
| Situational awareness of each client environment | ✔ |
| Contextual threat tuning | ✔ |
| Threat intelligence integration | ✔ |
**ALLEVIATES RESOURCE CONSTRAINTS (CONT.)**

<table>
<thead>
<tr>
<th>eSentire</th>
<th>24x7x365 threat monitoring*</th>
<th>✓</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cloud insights management and discovery (vulnerability, misconfiguration, container and asset)</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Dedicated cloud insights management**</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Threat hunting</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Forensic investigation</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Event management/false positive reduction</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Alerts</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Remediation guidance</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Remote managed threat containment</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Automated remediation and implementation of network changes</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Co-remediation</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Confirmation of post-event hardening</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Monitor for reentry</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Co-managed access to platform and technologies***</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Reporting</td>
<td>✓</td>
</tr>
</tbody>
</table>

*esENDPOINT & esLOG+ Only
**Managed Vulnerability Service
***Managed Vulnerability Service and esLOG+

**PROVIDES CLOUD COVERAGE AT A FRACTION OF DIY COST**

Figure 1 represents an example cost comparison yielding, on average, an 18x reduction versus do it yourself (DIY) models.

* DIY 24x7 SOC Cost Components: Technology includes Next-Gen AV + EDR (400 endpoints), Scanning of 400 IPs, SIEM with 7 G/B Daily Throughput and 2 Threat Intel Feeds. Staffing covers 12 SOC Analysts, 1 SOC Manager, 3 Intelligence Analysts, 1 Intelligence Manager, 1 Network Security Engineer, 1 Network Security Administrator. Operational Tools include workflow/automation/orchestration, investigation tools, response tools and threat management.

** eSentire pricing reflects MSRP. Actual pricing will vary by customer and environment.
BUSINESS BENEFITS

- Aligns business objectives, risk and cloud security strategy
- Securely enables acceleration of cloud adoption
- Promotes cloud security awareness with effective resource allocation
- Improves business-resiliency against real-world cloud attacks
- Lowers total cost of ownership
- Extends threat visibility across cloud-based environments
- Accelerates response time preventing business disruption
- Meets and exceeds compliance requirements

NEXT STEPS

esCLOUD Infographic

Managed Vulnerability Service: Cloud Insights

esCLOUD for IaaS: Amazon Web Services (AWS)

esCLOUD for SaaS: Office 365

About 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 $6 trillion AUM, 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](http://www.esentire.com) and follow @eSentire.