eSENTIRE

DATA SHEET:

esCLOUD for IaaS

Critical cloud awareness. Rapid detection and response.

GAIN DEEP-LEVEL INFRASTRUCTURE INSIGHTS

Automated asset discovery with real-time insights into users, services and configuration changes establishes always-on infrastructure awareness.

IDENTIFY POTENTIAL RISKS AND ANOMALOUS BEHAVIORS

Cloud-native security controls with advanced analytics and purpose-built use cases proactively identify risks and potential malicious activity.

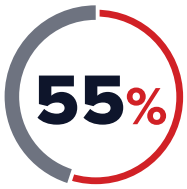
HUNT THREATS AND ENFORCE POLICIES

Proprietary attacker blacklists, automated policy enforcement and an elite team of threat hunters prevent and identify expected and unexpected attacks.

RESPOND AND OPTIMIZE CYBER RESILIENCE

Unlimited incident response ensures threats are eradicated and infrastructure is hardened against future attacks.

Traditional detection and prevention technologies are largely ineffective at addressing threats to your cloud environment. Cyberattackers understand this dynamic and capitalize on vulnerable cloud environments with increasing precision. Timely remediation of threats is challenging given the complexity of managing infrastructure as a service (IaaS), leading to increased incident dwell time and risk to your business.



year-over-year increase in cloud data breaches (2018-2019)[1]

claim traditional security solutions don't work at all or have limited functionality[2]

esCLOUD for IaaS combines cloud-native security technology with elite threat hunting to safeguard your cloud environments. Pinpoint vulnerabilities and misconfigurations and identify suspicious behaviors in real-time by leveraging eSentire's 24x7x365 Security Operations Centers (SOC). Full incident lifecycle support, ongoing cloud threat detection and policy development optimize your cloud security posture for the future.

SUPPORTED IAAS PLATFORMS

Amazon Web Services (AWS)

AWS is the world's most widely adopted cloud platform, comprised of over 175 services for use cases ranging from storage, development, web applications and more.

Azure

Microsoft's expanding set of cloud computing services, allows for seamless integration with existing Microsoft investments and a robust cloud active directory offering.

Google Cloud Platform (GCP)

GCP allows customers to utilize the same infrastructure that Google uses for its own assets, such as YouTube, Gmail and its iconic search engine.

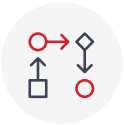
[1,2] 2019 Cloud Security Report, ISC 2

WHAT DOES esCLOUD FOR IAAS PROTECT AGAINST?

esCLOUD for IaaS facilitates timely detection and remediation of identified cloud threats, reducing potential threat actor dwell time and exposure of your cloud assets. Detection and response capabilities for risks include:

Anomalous activity

Flags deviations from baseline behavior correlating changes to user privileges, group policies, access keys and other configurations.



Exposed services

Identifies and remediates critical service exposures before threat actors have the opportunity to exploit.

Cryptojacking threats

Reveals illicit activity that leverages the computing power of your cloud environment to mine cryptocurrencies such as Bitcoin and Ethereum.

Account hijacking attempts and brute force attacks

Detects potential account hijacking attempts by identifying unusual login activities such as concurrent attempts, peculiar geo-locations and unknown browsers or operating systems.

Sensitive configuration updates

Notifies eSentire SOC analysts to sensitive modifications to ensure misconfigurations do not leave your environment in a vulnerable state.

FEATURES

Always-on infrastructure awareness

Automatically identifies and tracks assets and changes to your AWS, Azure and GCP environment.

24x7x365 monitoring

Provides around the clock inspection of your cloud infrastructure leveraging eSentire's SOC 2 accredited global SOCs.

Global blacklist integration

Automatically address activity from malicious IPs leveraging eSentire's proprietary blacklist of confirmed global attacker sources, curated by eSentire's global threat team.

Automated policy enforcement

Prevents attackers from gaining a foothold within your cloud environment with over 400 integrated best-practice policies and automated enforcement.

Integrated 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.

Full incident lifecycle support

From initial detection to hardening your environment against future attacks, security experts are with you every step of the way.

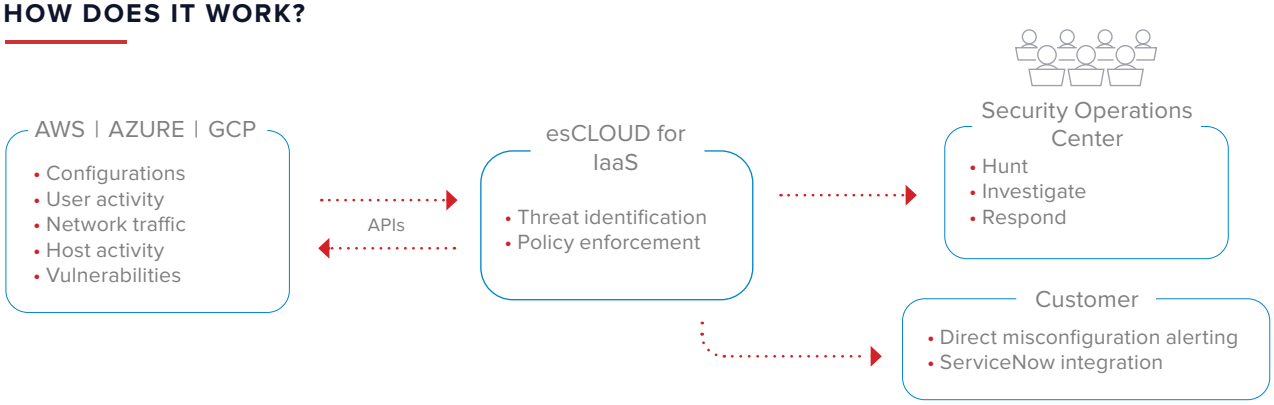
Compliance

Policies and reporting align with common standards and regulatory bodies such as GDPR, PCI, HIPAA, NIST CSF, SOC 2 and CIS standards specific to AWS, Azure and GCP.

Ongoing detector development

Advanced detection, policy and runbook developments keep you on the cutting edge of anti-adversarial tactics and strategy.

HOW DOES IT WORK?



MAKE THE CASE FOR esCLOUD

Don't rely on legacy security services for today's threat landscape. Control your risk and accelerate your business with a cloud-delivered Managed Detection and Response (MDR) solution that adapts to your shifting security needs.

	Typical Managed Security Service Provider (MSSP)	eSENTIRE
IaaS monitoring	✓	✓
User activity monitoring	✓	✓
Anomalous behavior monitoring	Limited (Typically to user behavior only)	Advanced (Integrated AI/ML inspects all cloud workload data)
Vulnerability identification	✓	✓
Real-time cloud asset discovery	Limited	✓
Real-time misconfiguration and policy violation alerting	Limited	Advanced (400+ out of box policy alerts)
Integrated proprietary attacker blacklist	✗	✓
Remediation of cloud threats	✗	✓
Integration with network and endpoint MDR capabilities*	Limited	✓
Ongoing policy and threat detector development	Limited	✓

*Requires esNETWORK and esENDPOINT

BUSINESS BENEFITS

- Reduced risk of business disruption
- Maintains real-time asset awareness
- Identifies threat activity and risky exposures around the clock
- Accelerates the remediation of risks in your IaaS investments
- Implements best practice policies with automates enforcement
- Securely enables changes and expansion of your IaaS environment
- Reduces complexity and alleviates resource constraint in your IT organization
- Satisfies shared responsibility models
- Aids in achieving compliance of regulatory body mandates

THE eSENTIRE DIFFERENCE

750+
GLOBAL CUSTOMERS

6
CONTINENTS

48
COUNTRIES

CUSTOMER RETENTION

> We have immediate visibility into attempts to penetrate our network and feel better knowing that eSentire's MDR is "manned" 24/7/365 with experienced cybersecurity experts.
>
> – Mark Fairhead, IT Associate Director, Rawlson & Hunter

> We're much more aware of things happening on the network. The metrics and weekly reports provide insight into the threats that are constantly probing our network.
>
> – Ted Chan, IT professional, Heartland Farm Mutual

eSENTIRE®

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** and follow **@eSentire**.