eSENTIRE

DATA SHEET

esCLOUD for SaaS: Office 365

Comprehensive visibility. Rapid threat detection.

Microsoft Office 365 offers your organization access to critical information and enables collaboration anywhere, anytime and on any device. Under the shared security responsibility model, Microsoft is responsible for infrastructure and uptime, while your security team is accountable for controlling access and the data within. While native Office 365 security features provide a groundwork layer of protection, threat actors are demonstrating the ability to bypass these controls with speed and precision. Under-resourced and over-extended, your security team is challenged to rapidly detect and respond to malicious activity that bypasses native and existing security controls.

71%
of organizations use Office 365[1]

71%
of organizations have at least one compromised Office 365 account each month[2]

25%
of phishing attacks bypass Office 365's built-in security[3]

Collaborate in confidence with esCLOUD for SaaS. eSentire Security Operations Center (SOC) analysts, augmented by machine learning technology, monitor your Office 365 environment day and night identifying threats that bypass existing security controls. They investigate suspicious activity confirming threat actor presence with root cause determination. Minimizing threat actor dwell time, dedicated responders work directly with your internal security teams providing step-by-step guidance that eradicates threat actor presence and hardens your environment against future attack.

What does esCLOUD for SaaS solve for?

- Limited threat visibility across:
  - Office Suite
  - Exchange Online
  - Sharepoint
  - Power BI
  - Sway
  - Skype for Business
  - Delve
  - Yammer
  - OneDrive
  - Azure Active Directory
- Advanced analytics required to identify known, unknown and suspicious activity
- Resource limitations to hunt and confirm attacks without false positives
- Ability to correlate and map multiple events to Office 365 applications
- Incident prioritization and remediation that reduces threat actor dwell time
- Retention and collection of log data
- Reporting and compliance requirements

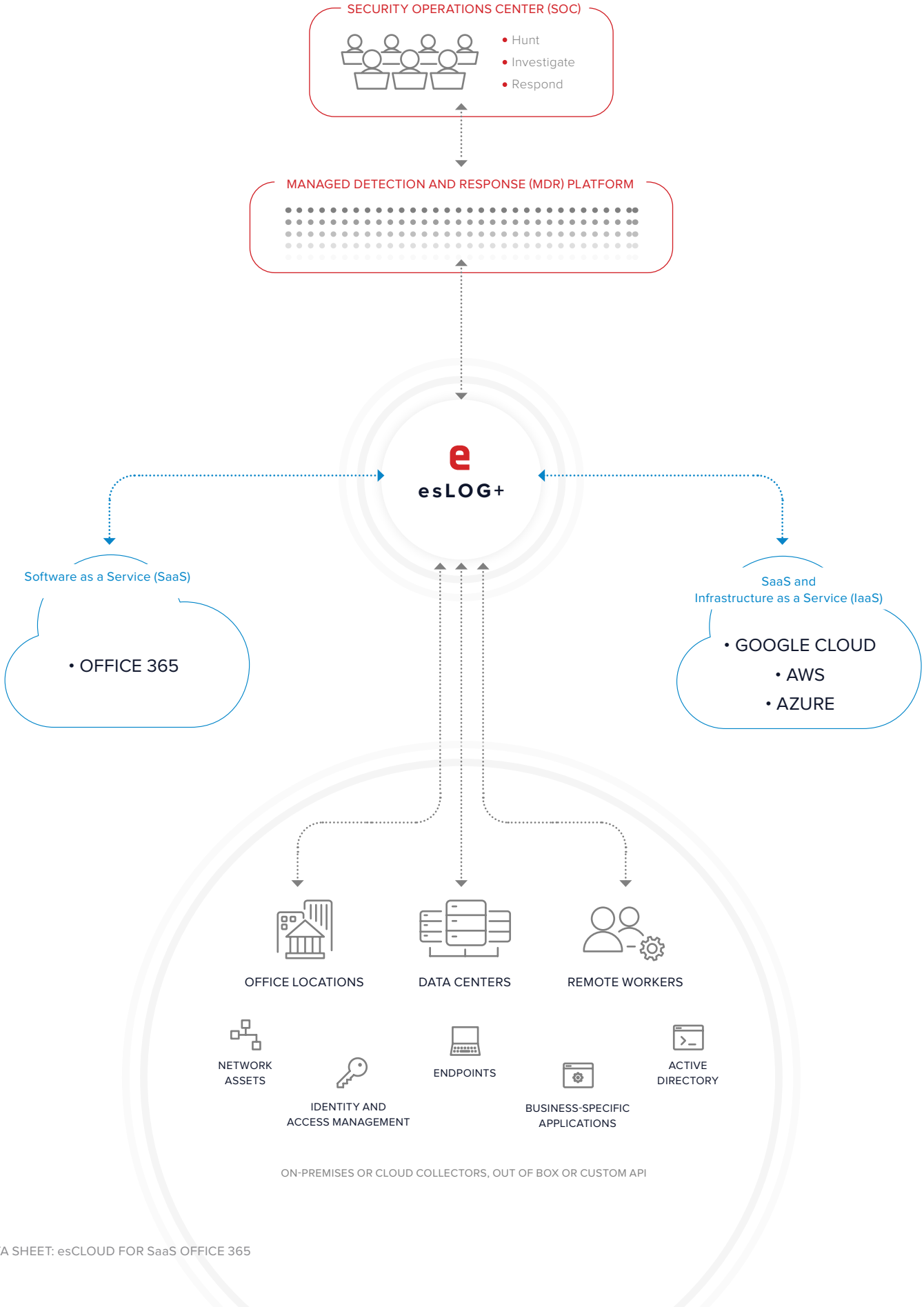
Get protection against:

[1]2018 Cybersecurity Insiders Cloud Security Report
[2]Definitive Guide to O365 Data Protection, McAfee
[3]https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/new-report-finds-25-of-phishing-attacks-circumvent-office-365-security

SHARED RESPONSIBILITY ALIGNMENT

Shared Responsibility Model			
SaaS Software-as-a-Service			
Cloud Transformation and Migration Cloud Security Program, Policies, Architecture and Response			
Responsibility (See table below)	Data Classification	**Function**	**Regulatory**
Client	- Your Office 365 log data - Access and control of your log data residing in Office 365 - Office 365 log data backup • Copy of your log data stored in a different location - Full log data Retention • Short term and long term log data retention filling any/all policy gaps granular and point-in-time recovery options - Log data control Internal • Accidental deletion • Malicious insiders • Employee retaliation • Evidence tampering - External • Ransomware • Malware • Hackers • Rogue apps	User Access Data	- Roles as a data processor • Data privacy • Regulatory controls • Industry certifications • HIPAA, Sarbanes Oxley
Cloud provider	- Microsoft Global Infrastructure - Uptime of the Office 365 Cloud Service - Office 365 data replication • DC to DC geo-redundancy - Recycle Bin • Limited, short term data loss recovery - Infrastructure level • Physical security • Logical security • App level security • User/admin controls	Applications Operating System Network Traffic Hypervisor Infrastructure	- Role as a log data owner • Answers to corporate and industry regulations • Demands from internal legal and compliance officers
esCLOUD for SaaS			

HOW DOES IT WORK?



FEATURES

24x7x365 Office 365 Application Monitoring and Visibility

- Sharepoint
- Power BI
- Sway
- Exchange Online
- Skype for Business
- Delve
- Yammer
- OneDrive
- Office Suite

Machine Learning Integration

Machine learning and predictive analytics make sense of expected and unexpected behavior across your Office 365 environment with pattern, anomaly and outlier detection accelerating investigation of potential threats.

Threat Containment and Full Remediation Support

Rapid lock down and isolation of threat actors prevents lateral spread and business disruption. Integrated response experts provide analysis detailing root cause determination with full remediation support that hardens your Office 365 environment against future attack.

Co-Managed Access

The co-managed model gives you access to run your own advanced search queries, generate alerts, manage profiles, run reports and investigate events alongside our SOC analysts.

Compliance Management Reporting

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.

Embedded Hunting and Investigation

Embedded human threat hunting teams investigate suspicious activity across your Office 365 applications, eliminating false positives and facilitating rapid detection and response to even the most elusive of threat actors.

Time to Value

Simple-to-deploy collectors and software can be up and running within minutes. Deployment specialists manage the onboarding process end-to-end, working with your teams to ensure rapid time to value.

Real-time Search and Visualizations

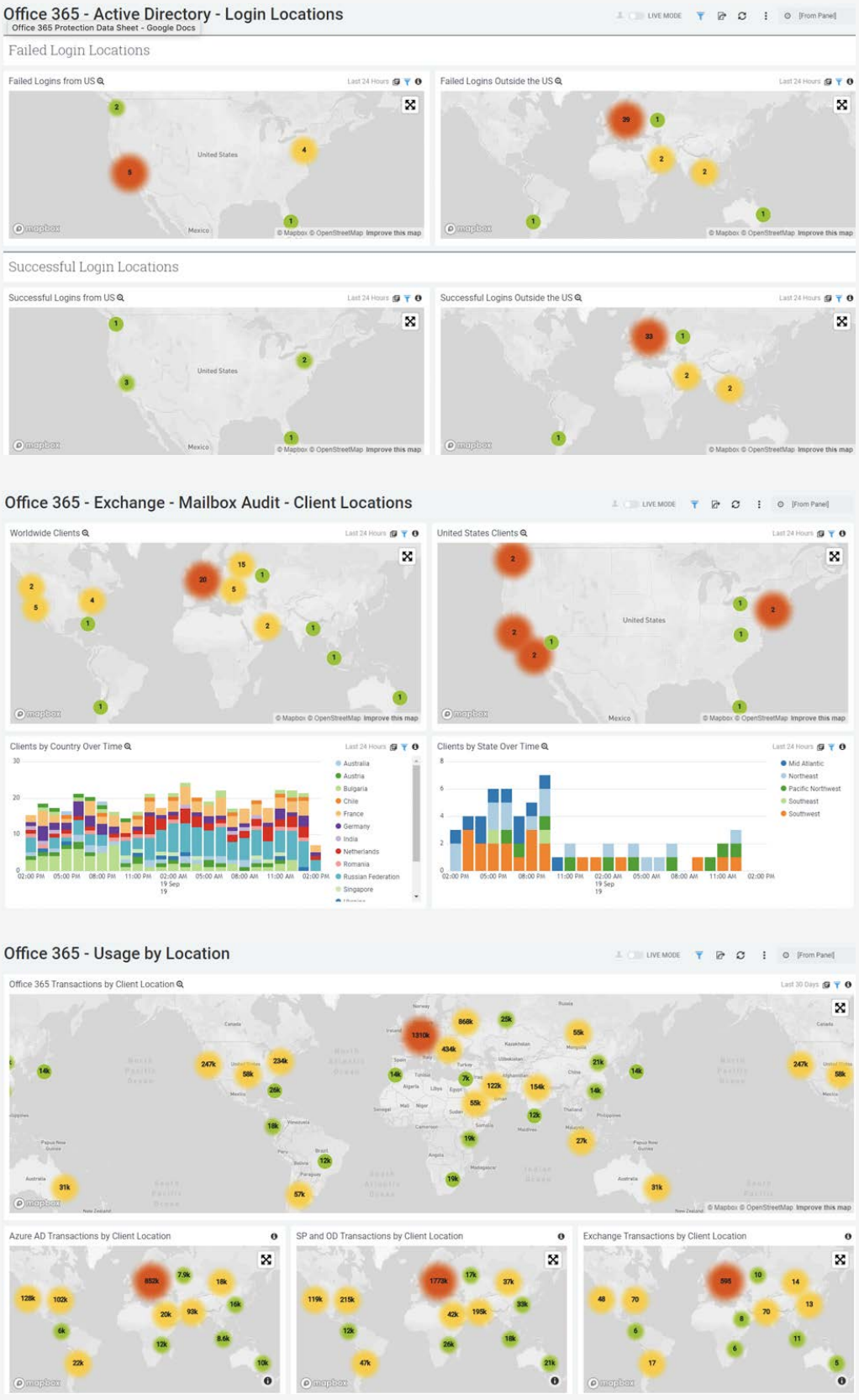
Preconfigured and customizable searches and dashboards with KPIs give our SOC analysts and your security team visibility into abnormal behaviors illuminating what matters most.

WHY eSENTIRE?

	eSentire
Initial Deployment and Setup	
Account/role setup	✓
Setup/deployment/configuration of collectors	✓
Configuration of sources	✓
Training and onboarding	✓
Dashboard setup	✓
Ongoing dashboard maintenance	✓

	eSentire
Ongoing Operations	
Deployment/setup of new collectors and apps	✓
Parsing operations	✓
Log collection, management and correlation	✓
Writing of search queries	✓
Modification of search queries	✓
Creation of reports	✓
Modification of reports	✓
Patches, hot fixes and functional updates	✓
Creation of correlation rules	✓
Modification of correlation rules	✓
Threat intelligence integration/updates	✓
Monitoring	
24x7 monitoring	✓
Incident Investigation and Management	
Threat hunting	✓
Forensics and investigation	✓
False positive elimination	✓
Alerts	✓
Response plan	✓
Remediation guidance	✓
Reporting	
Monthly reporting (system generated)	✓
Creation/maintenance of standard reports	✓
Creation/maintenance of customized reports	✓
Compliance report creation/updates	✓
Report validation and review	✓

Sample Visualizations



BENEFITS

- 24x7x365 threat visibility across Office 365 applications
- Flexibility to run your own queries, alerts, profiles, reports and investigation alongside eSentire analysts
- Unparalleled insight with data visualizations and customizable queries
- Simplifies compliance management and reporting
- Removes complexity and resource demands to:
  - Identify known threats and suspicious activity
  - Analyze, hunt and confirm threat actor presence
  - Account for shared security responsibility
  - Eliminate false positives
  - Conduct post-attack forensics
  - Contain and eradicate threat actor presence
  - Determine root cause and harden against future occurrence

MAKE THE CASE FOR eSENTIRE MDR

Client Satisfaction

97% Overall Improvement in Security Posture

100%	98%	98%	98%	98%
Deployment	Ongoing Operations and Tuning	Threat Detection and Response	Security Operations Center (SOC)	Customer Success

We now have greater visibility into security events in our environment.

IT Director
Small Business Financial Services Company

We are now quicker to respond to an incident should one happen.

IT Director
Large Enterprise Hospitality Company

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**.