Protecting the Cloud
with FireEye Helix
and Cloud Security Solution
Solution Overview
The FireEye Ecosystem
Challenges in Security Operations

- **80**
  - Average number of security tools

- **10K**
  - Number of security alerts daily

- **20 MIN**
  - Time required to triage a single alert

- **78 DAYS**
  - Average time it takes to discover a breach

- **30 DAYS**
  - Average time it takes to respond to a breach
FireEye Helix Overview

Technology
- Next-Gen SIEM
- Behavior Analytics
- Cloud Visibility

Processes
- Automation
- Guided Investigation
- Compliance Reporting

Expertise
- Expertise On Demand
- Threat Intelligence
- Risk Prioritization
What’s New in 2019

- Expertise On Demand
- Self-Service Portal
- Federated Helix
- Support for Encrypted Syslog
- More Threat Intel Context
- Technical Integrations
Expertise On Demand

You see a suspicious domain. You want to know what FireEye knows about it.

Context Inquiries
- Provides context and overviews
- Highlights available Insight reports

You notice the domain is attributed to a particular malware family.

Insights
- Access the referenced Intel report, or brief analyst commentary

You now know enough to be nervous. You want to investigate the endpoint.

Analyst Investigations
- Request analyst evaluation of the malware or indicators
- Have the case investigated

You realize the endpoint is compromised and you need help.

Full Service Portfolio
- Transition to IR
- Provide a tailored threat briefing
- Engage Mandiant for security posture review

LEVEL OF ENGAGEMENT
Self-Service Portal for Cloud Data Integration

Helix Cloud Integrations Portal
This portal allows you to add, view, and change Helix cloud integration configurations.

Enabled Integrations
No integrations enabled.

Available Integrations
- AWS S3
- AWS VPC Flow Logs
- AWS CloudTrail
- AWS Security Hub
- Corelight
- CrowdStrike Falcon
- Digital Guardian
- Druva
- Entrust Intelliguard
- FireEye Detection on Demand for AWS
- FireEye Network Security
- FireEye Email Threat Prevention
- Google Cloud
- K sort
- Microsoft Azure
- Microsoft Defender ATP
- Okta
- Proofpoint SIEM Integration
- Proofpoint CASB Integration
- Sophos Antivirus SIEM Integration
To learn more about our product integrations, including additional tools and content to extend your FireEye experience, visit

https://fireeye.market
More Integrations
Roadmap Highlights

- Cloud Integrations Portal
- Custom Parsing
- Granular RBAC
- Aggregated threat view
- Password-protected emailed reports
- Email metadata streaming
- On-demand Endpoint integration
- Analytic workbench
- Encrypted Syslog collection
- Managed Defense investigation
- Automatic artifact collection
- Federated Console
- UEBA Dynamic Log Monitoring
- Case Management update
- Improved logging visibility
- SOC 2 Certification
Cloud Security
Common Security Challenges in the Cloud

- Lack of continuous visibility
- Inability to detect misconfigurations and credential misuse
- Lack of central management capabilities
Introducing FireEye Cloud Security

Cloud Security Solution
- FireEye Helix
- Network Security + iboss
- Network Security on AWS
- Detection On Demand

Other FireEye Solutions
- Mandiant Consulting
- Email Security, Cloud Edition
- Verodin Security Instrumentation
- Threat Intelligence
FireEye Cloud Security Solutions

- Ultimate cloud visibility and centralized monitoring
- Simplified integration via Cloud Integration Portal
- Cloud-focused threat rules, analytics, dashboards
- Single pane visibility across cloud vendors
Cloud Security Telemetry

Audit logs
App logs
Network logs
Security logs

Analytics Rules
Indicators Of Compromise
Threat Intelligence
FireEye on AWS Marketplace
Virtual Network Security on AWS Marketplace

- FireEye Full Packet Capture
- FireEye Investigation Analysis System
- Amazon EC2
- Web Front Ends
- Misc. App Services
- Database Services

User

VM

Network Zone

Network Traffic Communications

Replicated Network Traffic
Detection On Demand on AWS Marketplace

Available via AWS Marketplace

- Objects in your cloud
- SOC
- SIEM
- Files in web applications
Thank you.