A Custom Technology Adoption Profile Commissioned By Alert Logic | June 2016

Evolve Your Security Operations Strategy To Account For Cloud

GET STARTED ▶

Evolve Your Security Operations Strategy To Account For Cloud

The growth of cloud computing and proliferation of complex service delivery models continue to accelerate as companies recognize the business and technology benefits inherent in cloud adoption. Data from Forrester's Global Business Technographics® Infrastructure Survey, 2015 shows that 46% of companies now use two or more cloud providers as part of their IT service delivery strategy. While the value of cloud for business and IT is widely recognized, new challenges are emerging. More than ever, companies require an agile security operations strategy to respond to changing infrastructure needs.

In March 2016, Alert Logic commissioned Forrester Consulting to evaluate the impacts that cloud adoption has had on cloud security operations, and the related challenges and benefits that IT professionals experience.

Demographics

100 US and UK IT professionals at the director level and above who have workloads in the public cloud and manage cloud security infrastructure

Top five industries

› Financial services/insurance: 21%
› Retail: 19%
› Manufacturing: 19%
› Software: 14%
› Telecommunications: 9%

Company size

› 100 to 499 employees: 18%
› 500 to 999 employees: 25%
› 1,000 to 4,999 employees: 43%
› 5,000 to 10,000 employees: 14%

Responsibility for cloud security infrastructure

› Final decision-maker: 68%
› Part of team making decisions: 30%
› Influence decisions: 2%

1 2

Security Operations Teams Are Not Adjusting Their Strategy For Public Cloud

Companies are adopting cloud infrastructure and computing in order to capitalize on business advantages such as rapid innovation and speed-to-market, but survey results show that security teams may not be adapting security operations to business demands.

IT professionals report that cloud adoption has changed their companies' security operations strategies in the following ways: They are increasing investment in security operations (51%), instituting new cloud security policies and controls (49%), and re-evaluating their security operations and controls across all environments (46%). Yet while security teams recognize that cloud adoption as a whole requires a transformation in security operations, 75% of IT professionals surveyed in this study are using the same security across their public and on-premises workloads.

"Is your security operations strategy the same for your public cloud infrastructure/workloads (versus your on-premises or hosted infrastructure)?"

25% No, we use different security operations methods for our public cloud infrastructure

75% Yes, we use the same SOC strategy for all infrastructure/ workloads regardless of location

Base: 100 US and UK IT pros at the director level and above who have workloads in the public cloud and manage cloud security infrastructure
Source: A commissioned study conducted by Forrester Consulting on behalf of Alert Logic, May 2016

A Custom Technology Adoption Profile Commissioned By Alert Logic | June 2016

Evolve Your Security Operations Strategy To Account For Cloud

OVERVIEW **SITUATION** APPROACH OPPORTUNITY CONCLUSIONS

1 2

Increasingly Complex Environments Require Adjustments In Security Operations Strategy

Fifty-three percent of companies have implemented or are expanding their in-house security operations center (SOC) capabilities, despite challenges.

Forty-four percent of companies report the ability to manage security content and identify multivector attacks are the primary challenges of security operations. Further, security roles are often distributed across the organization, adding to the difficulty of centralizing security operations and managing costs. Companies also struggle with finding skilled talent to build their teams.

Companies reported increased investment in security operations (51%), but find challenges in adjusting for cloud adoption.

"What are the challenges of bringing your security operations strategy in house?"

Challenge	%
Managing security content (signatures, blacklists, whitelists, rules)	44%
Ability to identify multivector attacks	44%
High costs	41%
Building out threat intelligence skills	40%
Difficulty making sense of all the data (data correlation)	33%
Staffing the SOC	33%

Base: 82 US and UK IT pros at the director level and above who work for companies that have their own SOC
Source: A commissioned study conducted by Forrester Consulting on behalf of Alert Logic, May 2016

1 2

Add Skills To Your Team To Meet Cloud Security Demands

Companies need a combination of technical and business skills to support their SOC. On the technical side, security teams must be skilled in network, application, and infrastructure security, as well as virtualization and threat intelligence. Effective security teams also require complementary business skills, including risk management, compliance management, change management, and industry expertise.

"What kind of *technical skills* do you need to bring on board in order to build your own SOC?"

Skill	%
Network security	42%
Virtualization, cloud infrastructure expertise	41%
Threat intelligence and analytics	41%
Application/infrastructure security	39%
Fraud management expertise	31%

Base: 100 US and UK IT pros at the director level and above who work for companies that have their own SOC
Source: A commissioned study conducted by Forrester Consulting on behalf of Alert Logic, May 2016

"What kind of *business skills* do you need to bring on board in order to build your own SOC?"

Skill	%
Risk management expertise	46%
Regulatory compliance expertise	43%
Industry experience	37%
Business process and change management	31%
Communication skills	26%

Base: 100 US and UK IT pros at the director level and above who have workloads in the public cloud and manage cloud security infrastructure
Source: A commissioned study conducted by Forrester Consulting on behalf of Alert Logic, May 2016

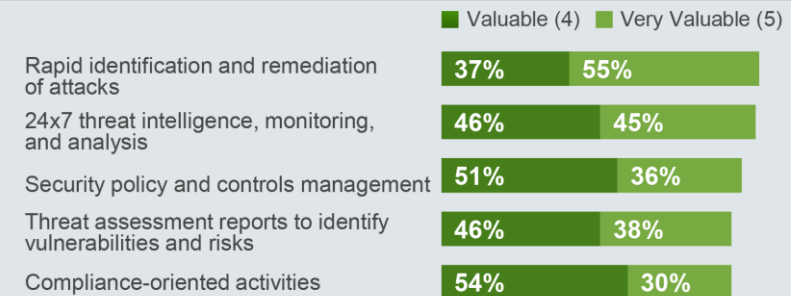# Evolve Your Security Operations Strategy To Account For Cloud

1   2

Expand Your Security Operations Capabilities

Companies require expanded security operations capabilities to respond to the demands of increasingly complex cloud service delivery models:

› Ninety-two percent of IT pros value the capability to quickly identify and remedy attacks, thus limiting their downtime and threat exposure.

› Ninety-one percent value 24x7 threat intelligence and monitoring and analysis to continuously protect and respond to attacks.

› Eighty-seven percent want an SOC with the capability to implement and manage security policies and controls in response to evolving threats.

"How valuable are the following features/capabilities in an SOC?"

■ Valuable (4)   ■ Very Valuable (5)

Feature/Capability	Valuable (4)	Very Valuable (5)
Rapid identification and remediation of attacks	37%	55%
24x7 threat intelligence, monitoring, and analysis	46%	45%
Security policy and controls management	51%	36%
Threat assessment reports to identify vulnerabilities and risks	46%	38%
Compliance-oriented activities	54%	30%

Base: 100 US and UK IT pros at the director level and above who have workloads in the public cloud and manage cloud security infrastructure
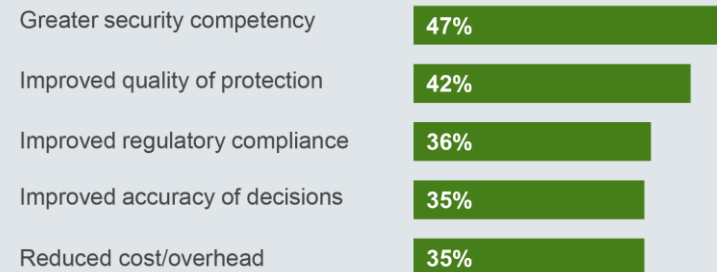Source: A commissioned study conducted by Forrester Consulting on behalf of Alert Logic, May 2016

IT Professionals Value Expertise From Security Partners

IT professionals value a SOC that provides them with access to security experts to augment their internal security capabilities. They are interested in working with a security expert for a variety of reasons, including threat intelligence analysis (83%), public cloud security (80%), security operations (77%), network security (76%), and data privacy and compliance (76%).

As a result of partnering with a security expert, companies recognize a range of valued benefits. Topping the list of benefits is greater security competency (47%).

Seventy-nine percent consider access to external security experts as a valuable or very valuable component of their security operations.

"What benefits have you achieved/do you expect to achieve as a result of partnering with a security expert to run or augment your security operations?" (Select all that apply)

Greater security competency	47%
Improved quality of protection	42%
Improved regulatory compliance	36%
Improved accuracy of decisions	35%
Reduced cost/overhead	35%

Base: 100 US and UK IT pros at the director level and above who have workloads in the public cloud and manage cloud security infrastructure
Source: A commissioned study conducted by Forrester Consulting on behalf of Alert Logic, May 2016

Evolve Your Security Operations Strategy To Account For Cloud

Conclusions

Increasing adoption of cloud and complex public, private, and hybrid cloud service delivery models presents opportunities and challenges for security teams. Companies recognize the need to adjust their security operations strategy in response, but building an in-house SOC with best-in-class expertise and capabilities is often difficult and cost prohibitive. The majority of IT professionals in this study reported that they are interested in working with a security expert to augment or outsource their security capabilities.

A combination of internal and external capabilities enables companies to improve their security operations strategies.

METHODOLOGY

› This Technology Adoption Profile was commissioned by Alert Logic.
› To create this profile, Forrester leveraged its existing research on cloud security infrastructure.
› Forrester Consulting supplemented this data with custom survey questions asked of US and UK IT decision-makers responsible for cloud security infrastructure.
› The auxiliary custom survey began and was completed in May 2016. For more information on Forrester's data panel and Tech Industry Consulting services, visit forrester.com

Project Director:

Andia Vokshi
Market Impact Consultant

Contributing Research:

Forrester's Security & Risk research group