



Cisco Tetration Platform

Meeting the growing need for holistic workload protection

Multi-cloud strategy... Are you ready for it?



Enterprises today are embracing hybrid IT and multi-cloud



Leading to increasingly complex and distributed application environments



Resulting in a need for a consistent security policy protecting their workloads

Challenges of point products

Point products have limited ability to address multiple use cases as multi-cloud workloads get increasingly distributed.

Multi-cloud adoption brings larger attack surfaces and manifold points of vulnerability.



Today, enterprises use a range of point products that function as disconnected pieces providing only partial elements of workload protection.

Point products inherently lack the ability to deliver network effects or cannot be expanded to cover broader use cases¹.



Customers are least satisfied with the point products' initial up-front costs and ongoing annual costs.



What is a more comprehensive and all-encompassing approach to workload integrity and protection?

There is a strong enterprise interest in a platform-based approach to holistic workload protection.

42%

Use point products on a daily basis.

85%

Are looking to move to a platform-based approach in the next year.

Point Products Purchased

Application Dependency Mapping 63.7%

Cloud Workload Protection/micro-segmentation 62.5%

Network Forensics 51.0%

Network Visibility 50.4%

Container Security 47.8%

Compliance and Audit 46.9%

Simulation 32.4%

Total (N = 504; Base = % of respondents)

Anticipated Benefits of Platform Adoption

Operational efficiencies 48%

Network effects 44%

Cost savings 42%

DevOps/developer benefits and related value 41%

Time saving 41%

Reduction in number of point solution 40%

Total (N = 504; Base = % of respondents)

With Cisco Tetration you can:

Quickly identify security incidents and reduce attack surfaces. Support on-premises workloads, private clouds and multiple public clouds.

- 1 Comprehensive workload protection across any infrastructure and any workload type (VM, baremetal and containers).
- 2 Consistent implementation of micro-segmentation to contain lateral movement.
- 3 Enhanced micro-segmentation policy by restricting user access to applications based on user groups or behavior.
- 4 Reduce attack surface by detecting and remediating common vulnerabilities.
- 5 Flexible consumption options using on-premises or SaaS.

For more information, please visit:

Cisco Tetration

Methodology for IDC surveys: 504 web-based surveys. Global; 7 countries; 3 regions.

Worldwide survey as well insights from interviews with enterprise customers, IDC

¹network effects- when a product or technology is used systemically across a growing number of use cases, with benefits and value multiplying as it addresses each additional use case.

²Platform based approach - addresses 3 or more use cases from application discovery, security forensics, network security - micro-segmentation and visibility.

© 2019 Cisco and/or its affiliates. All rights reserved.