2017 SECURITY BUYER'S GUIDE

For distributed data centers and public cloud

Presented by:

illumio

THE NEED FOR ADAPTIVE SECURITY

Information security is not keeping up with the speed of business and IT. The network- and perimeter-centric security model being used in many enterprises cannot adequately support today's dynamic and distributed model for infrastructure and operations.

Modern data centers need to accommodate rapid application changes and new deployments in private and public clouds. Security needs to allow for public cloud environments, where the enterprise doesn't own or control the underlying infrastructure. However, security implementations are still based on perimeter appliances and tied to the network, which means they lack the context and visibility necessary to protect applications and their interactions inside data centers or clouds. In addition, security policies (ACLs) are tied to network parameters like IP addresses, ports, subnets, and zones. As a result, security is highly manual, potentially error-prone, and inflexible to cloud migrations or application and computing environment changes.

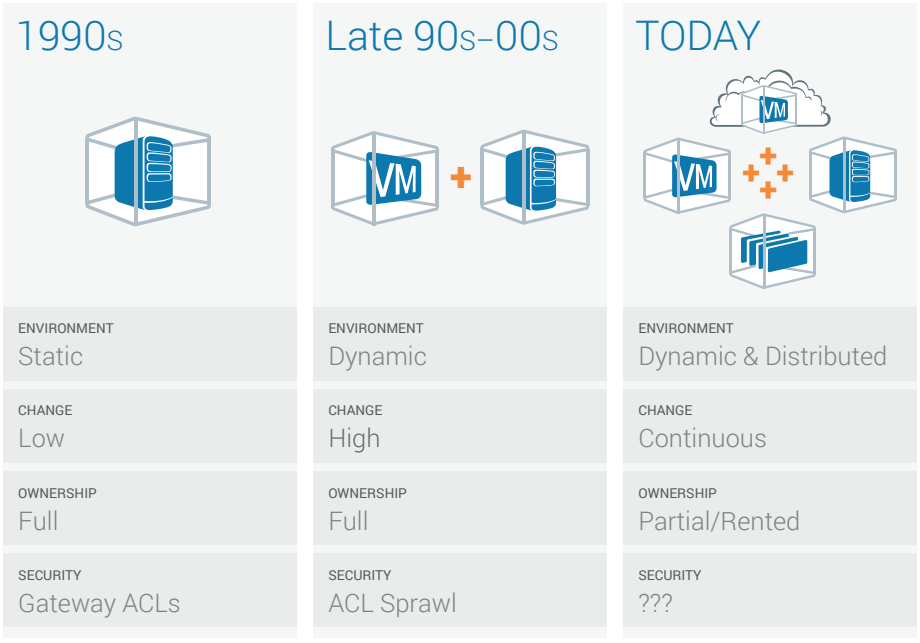


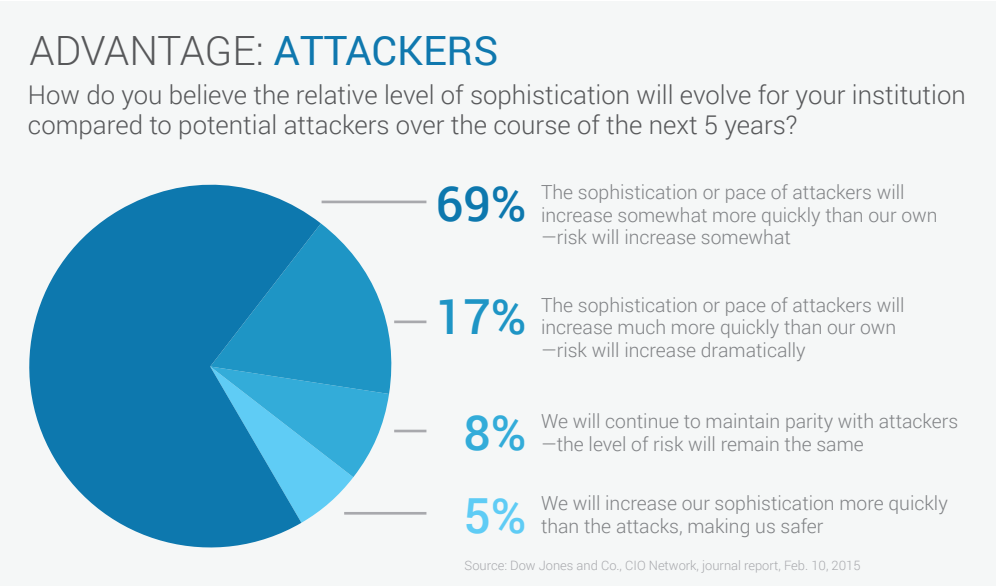
Figure 1: Evolution of computing and security

This static model of security forces enterprises into a reactive sequence of steps: Setting security policies based on a point-in-time view of applications and infrastructure, monitoring for adverse events, and then reacting to set things right. This process is then manually repeated whenever applications change, the computing environment changes, or a human error occurs.

In order to keep pace with the evolved operating model for today's infrastructures and applications, security needs a fundamentally different approach—one that is decoupled from the underlying infrastructure. Security can no longer be static. It must be adaptive to support diverse computing environments in data centers and clouds with physical servers, VMs, and containers.

Are you prepared for cyberattacks?

The volume and sophistication of cyberattacks also means that security architects need ways to prevent the lateral spread of attacks inside the data center or in the cloud. A recent CIO Network report by the Wall Street Journal found that a significant number of IT leaders think the sophistication of hackers will increase more quickly than that of their own enterprises. The report also found that most CIOs now believe that cyberattacks are inevitable and that their enterprises need to be better prepared to mitigate and recover from these attacks without losing critical assets.



The need for faster IT and security services

IT is under pressure to deliver newer services with initiatives like big data, and to provide cheaper and faster availability through cloud deployments. Security teams are saddled with old network-centric tools or a complicated layering of solutions when trying to provide granular segmentation and visibility of east-west traffic inside data centers, meet the application delivery needs of DevOps teams, and comply with industry regulations (e.g., PCI 3.0, HIPAA). Adaptive security solutions that can keep pace with today's fluid model of computation are an essential component of a modern enterprise's tool chest.

HOW TO USE THIS GUIDE

This security buyer's guide is based on research, deployment best practices, and conversations with more than 100 IT, operations, and security teams. It presents a set of guidelines and considerations to help IT leaders make security decisions while accounting for newer computing strategies likely to be considered by their organizations.

The guide is organized in sections, starting with a pre-assessment of your current security posture. With the data gathered from your pre-assessment, you can review the considerations for adaptive security to identify gaps/opportunities to improve your overall security posture, application delivery capabilities, and operations. Finally, use the adaptive security checklist at the end of the guide to identify key priorities and initiatives for your enterprise.

Definition of terms

For the purposes of this guide, an **application** is made up of a set of processes that may be spread across a single server—or multiple servers—in data centers or cloud environments. An application **workload** or server can be a physical server or virtual machine that represents a particular function within an application (e.g., a database or web server).

SECURITY PRE-ASSESSMENT:

Assess your current security posture for data center security. Record your answers to the following questions to understand your needs and identify gaps in your security posture.

1. What are your primary security strategies for data center or cloud applications? List out your technologies, including perimeter security appliances (IDS/IPS, APT, etc.), perimeter and internal firewalls, and other network security mechanisms (VLANs, security zones, etc.).
2. Do you have a common security strategy across VMs and physical servers in the private data center and your servers in the cloud?
3. How do you learn about application communications and east-west traffic inside the data center?
4. Does writing security policies involve knowing the details of the underlying network, including IP addresses, ports, subnets, zones etc.?
5. How do you separate application life cycle environments like development, test, staging, and production?
6. How do you evaluate and implement security changes when new applications are introduced or when applications change (auto scaling, decommission, etc.)?
7. How many firewall rules do you have and how long does it take (including change control processes and approvals) to make firewall rule changes?
8. How are you alerted about compromised servers and how long does it take to isolate such a server?
9. What is your process to encrypt sensitive data exchanged between applications (data in motion)?
10. Have you implemented (or are you considering) DevOps practices for application development and delivery? Are security considerations part of the process?

A FRAMEWORK FOR ADAPTIVE SECURITY

Adaptive security systems need to address application and network security without dependencies on the underlying infrastructure. But for security to be as dynamic as the assets it protects, it needs to be built into the operations and application life cycle. Figure 2 shows the two-dimensional framework for a modern security model that can support today's dynamic and distributed computing environments. The model highlights the necessary components of an adaptive security system that can secure any computing environment. The framework simultaneously addresses ways by which security can keep pace with application changes through integration with IT operations and application delivery processes.

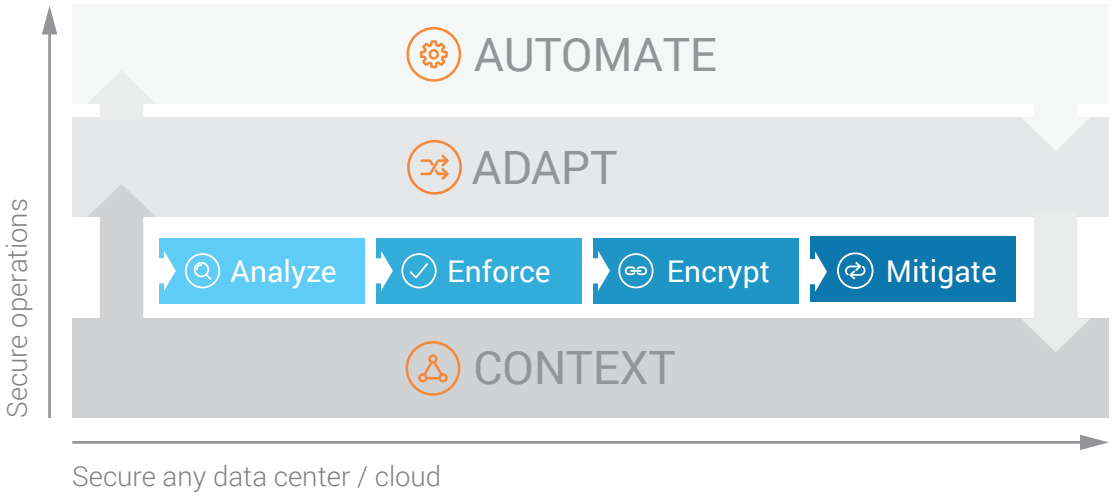


Figure 2: A framework for adaptive security

We'll now review the components of the adaptive security framework, as well as the capabilities they require.

CONTEXT

Using the dynamic context of application workloads, together with policies specified in natural language, allows security to be decoupled from the network. The context of each workload (including its system properties such as operating system, IP address, ports, and running processes; its interactions with other workloads; and its ecosystem such as the location, application, and environment) provides real-time status and collectively serves as a source of truth about the security state of the application at any given time. Adaptive security continuously listens for context information reported by workloads to create an up-to-date graph of dependencies within and between applications. It then fine tunes security policies dynamically in response to application migrations, changes, or additions.

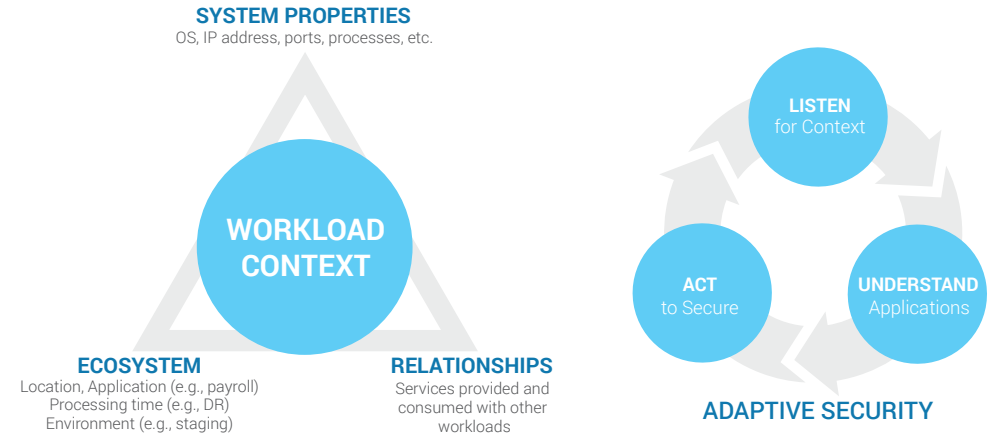


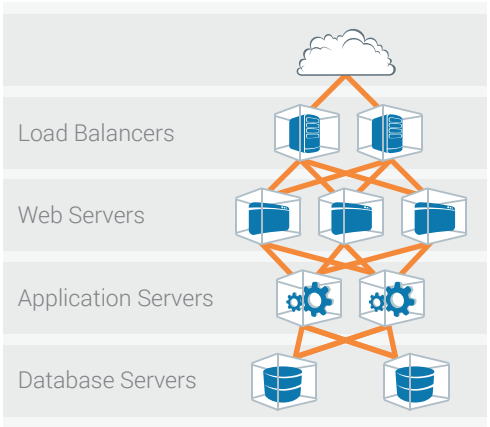
Figure 3: Using workload context in adaptive security

ANALYZE

Adaptive security begins with enabling security, application, and operations teams to come together to gain an understanding of their current security posture by mapping out all of the interactions between application workloads.

Graphical views of all east-west and north-south traffic

Multitier applications can have workloads spread across environments (e.g., a web tier in the cloud, databases in a private data center, and processing workloads in another data center). Administrators and DevOps teams need comprehensive visibility to all east-west and north-south traffic between workloads inside data centers or cloud deployments. In modern data centers, the applications—and environments they operate in—are constantly changing. When security is dependent on the underlying infrastructure, it becomes enmeshed in static network constructs and cannot adapt to changes. Instead, using the dynamic context of application workloads together with policies specified in natural language allows security to be decoupled from the network.



Application topology

The security system should display the topology of the application, including inter-application flows, irrespective of where individual workloads are located. Security architects should be able to click on individual application workloads and drill down for details on their context and interactions with other workloads. This will make possible the development of precise and well-informed security policies.

Figure 4: Interactions between tiers of an application

Ability to build and test policies before enforcing

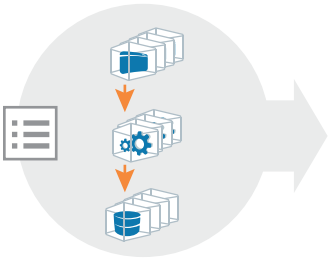
Application teams are often concerned about breaking legitimate flows when new security policies are applied. For example, some traffic flows—like batch processes—may occur infrequently, and enforcing policies without accounting for these flows could break the application. Adaptive security solutions should allow administrators to build new security policies interactively and put them in test mode while graphically displaying any policy violations or new flows that have not been accounted for.

ENFORCE

Adaptive security should provide the ability to capture security policies in natural language and apply fine-grained enforcement down to each application workload—without requiring network descriptions. This allows the policies to adapt to any changes while maintaining compliance requirements. The following attributes should be available at the enforcement stage.

Ability to write policies without network parameters

Adaptive security must include the ability to write security policies in natural language without the need for network parameters like IP addresses, ports, subnets, VLANs, or zones. Instead, the system should provide a mechanism to describe workloads and permitted interactions in terms of natural-language application interactions. For example, workloads can be described based on their function (database, web server, etc.); application name; environment or life cycle stage (staging, production, etc.), and location (Amazon, U.S. data center, etc.). Interactions between different workloads can then be described as policies between the provider and consumer of services. For example, in figure 6, application processing servers can use the PostgreSQL service of the database servers. Such security rules written in natural language can be specified to apply to all workloads in a specific application such as HRM, in the Production environment in the US location.



HRM : Prod : US

SERVICES	PROVIDED BY	USED BY
Apache	Web	Anything
Tomcat	Processing	Web
PostgresSQL	DB	Processing

Figure 5: Sample rules for an HRM application in a U.S. production environment

Precise, zero-trust policy model

A zero-trust security model prevents the problem of implicitly trusting workload interactions just because the workloads may be located inside a protected perimeter. Many attacks are the result of the lateral spread from compromised servers out to other servers within the environment. For enforcement to be precise, the policy model should require the explicit specification of security rules for both application interactions and each workload. Any interaction between workloads not specified by

policies should not be permitted. This results in granular enforcement for applications with an explicit trust model that only allows workloads to communicate with each other on permitted paths.

Continuous security computation and reprovisioning

The process of enforcing security on the individual workloads should be continuous with any changes. This requires the automatic computation and enforcement of new security policies.

Policy scaling and portability

Security policies should allow applications to scale without the need to duplicate rules, regardless of environment, life cycle stage, or location. For example, it should be possible to specify the interactions between the workloads in an application in the testing environment and have the same policies apply to the staging and production environments. Similarly, security policies should be portable without requiring any changes between the data center and cloud, or vice versa.

ENCRYPT

Application workloads are distributed across data centers and clouds connected by private and public networks. In many cases, confidential data is exchanged between application tiers, which requires encryption.

Policy-based encryption of data in motion

Enterprises have encrypted data in motion for a long time, but have lacked solutions that can provide policy-based encryption quickly and adaptively across workloads running in different operating systems. Enterprises should to be able to, for example, set up a policy to automatically encrypt any traffic between the web and application tiers of an application, and have that policy automatically handle new web workloads launched to auto scale the application.

On-demand encryption

The effort involved in setting up encrypted connections, including hardware, software, and configuration changes, is often a big reason that security projects are delayed. To accommodate rapid application deployments where encrypted connections are required, security administrators must be able to set up on-demand IPsec connections between application workloads.

MITIGATE

As the recent state of cyberattacks and data breaches has demonstrated, security violations and advanced attacks have become inevitable. Enterprise security is no longer just about preventative measures, it is also about providing mechanisms to contain, mitigate, and recover from such attacks.

Micro-segmentation and reducing the attack surface

Adaptive security strategies must secure the most granular components of applications—individual workloads, or containers or processes within those workloads. With adaptive security, enforcement occurs at each individual workload or service within the workload, which mitigates the impact of security violations. When the security system is able to segment and isolate individual workloads, the surface

area of a potential attack is also significantly reduced, which isn't the case with perimeter-enforcement models. The security alerts that are generated are also precise, which vastly reduces the number of false positives.

Ability to prevent the lateral spread of attacks

Since enforcement points are associated with each workload, all of the inbound and outbound communications are controlled, creating bidirectional enforcement of security between any combinations of workloads. This prevents potential attackers from launching reconnaissance processes or initiating connection requests from an infected system to spread their attacks. In addition, integration with SIEM solutions can allow additional forensic analysis and mitigation activities.

ADAPT

The ability to accommodate changes in application and infrastructure is the most important capability for adaptive security. Security architects are looking to address several use cases, spanning micro-segmentation and environmental separation, to public cloud migration, visibility to east-west traffic, and data residency. Enterprises cannot rely on static, network-centric security approaches to handle such needs. For example, a common requirement for application availability requires an elastic auto-scaling model where new application workloads can be brought into service or taken down to handle demand changes. Adaptive security can handle these types of application changes and movements through context-aware and continuously computed security.

AUTOMATE

The most significant opportunity for data center and cloud security lies in automating the implementation of policies and baking security into the application life cycle. Many vendors have previously promised this ability, but they've under-delivered, since application changes, additions, or migrations have always necessitated extensive manual intervention.

DevOps integration

Enterprises are adopting DevOps practices with orchestration and scripting tools to improve business and IT agility. However, security tends to be a lagging function, and security teams are not brought into the conversation until much later in the application rollout process. Even if they are involved early in the cycle, security cannot yet be fully defined since current strategies make security ultimately depend on the parameters of the network on which the application will be deployed. Adaptive security requires integration with tools like Chef, Puppet, or Ansible to build in security throughout the workload life cycle—from inception to decommission. All functions of an adaptive security framework should be exposed to security teams through standardized APIs to programmatically handle application changes.

ADAPTIVE SECURITY CHECKLIST

Using the adaptive security framework described above, evaluate the following attributes of your desired data center and cloud security solution. Assign each attribute below a score based on three criteria:

Low: Not a priority based on your current needs or handled well by your current security tools

Medium: Nice to have, but not something you need right away

High: A currently unmet and significant need that will drive a big improvement in security

Use the checklist to understand your priorities and focus areas for security decisions.

Security Attribute	Low	Medium	High
Visibility to servers, VMs, or server processes and their interactions	☐	☐	☐
Discover and view topology of applications in data center and cloud	☐	☐	☐
Test security policies before enforcing fine-grained security	☐	☐	☐
Gain control over firewall rules and avoid rule proliferation	☐	☐	☐
Avoid manual errors caused by policies written with IP addresses, ports, subnets, etc.	☐	☐	☐
Avoid the need to deploy internal firewalls to control application interactions	☐	☐	☐
Separate application life cycle environments without network constructs	☐	☐	☐
Prevent the lateral spread of attacks across the data center	☐	☐	☐
Handle application changes, migrations, and scale outs automatically	☐	☐	☐
Migrate to any public cloud without relying on network control for security	☐	☐	☐
Micro-segment without dependencies on hardware or hypervisor	☐	☐	☐
Reduce or eliminate the dependency on network layering (VLANs, zones, SDN) to achieve security	☐	☐	☐
Uniform security policies for applications across the data center and cloud	☐	☐	☐
Policy-based encryption of communication between servers anywhere	☐	☐	☐
Scale security policies across data centers, public, or hybrid clouds	☐	☐	☐
Automate security with scripting, orchestration, and DevOps integration	☐	☐	☐
Simplify the analysis of security violations or incidents	☐	☐	☐
Shorten compliance and audit tasks	☐	☐	☐