

# Applying the Top 20 Critical Security Controls to the Cloud

Bart Westerink

Senior Director of Security & Compliance  
CloudPassage

Professional Techniques – T33



The "CyberSizelT" logo is rendered in a large, stylized, red font with a white outline. The letters are slightly irregular and have a hand-drawn feel. In the background, there is a silhouette of the San Francisco skyline, including the Golden Gate Bridge and various skyscrapers, set against a light, hazy sky.

# Agenda

- Migration to the cloud
- Overview of top 20 security controls
- Adapting controls to the cloud
- Leverage controls to build a highly secure cloud infrastructure



# MIGRATION TO THE CLOUD



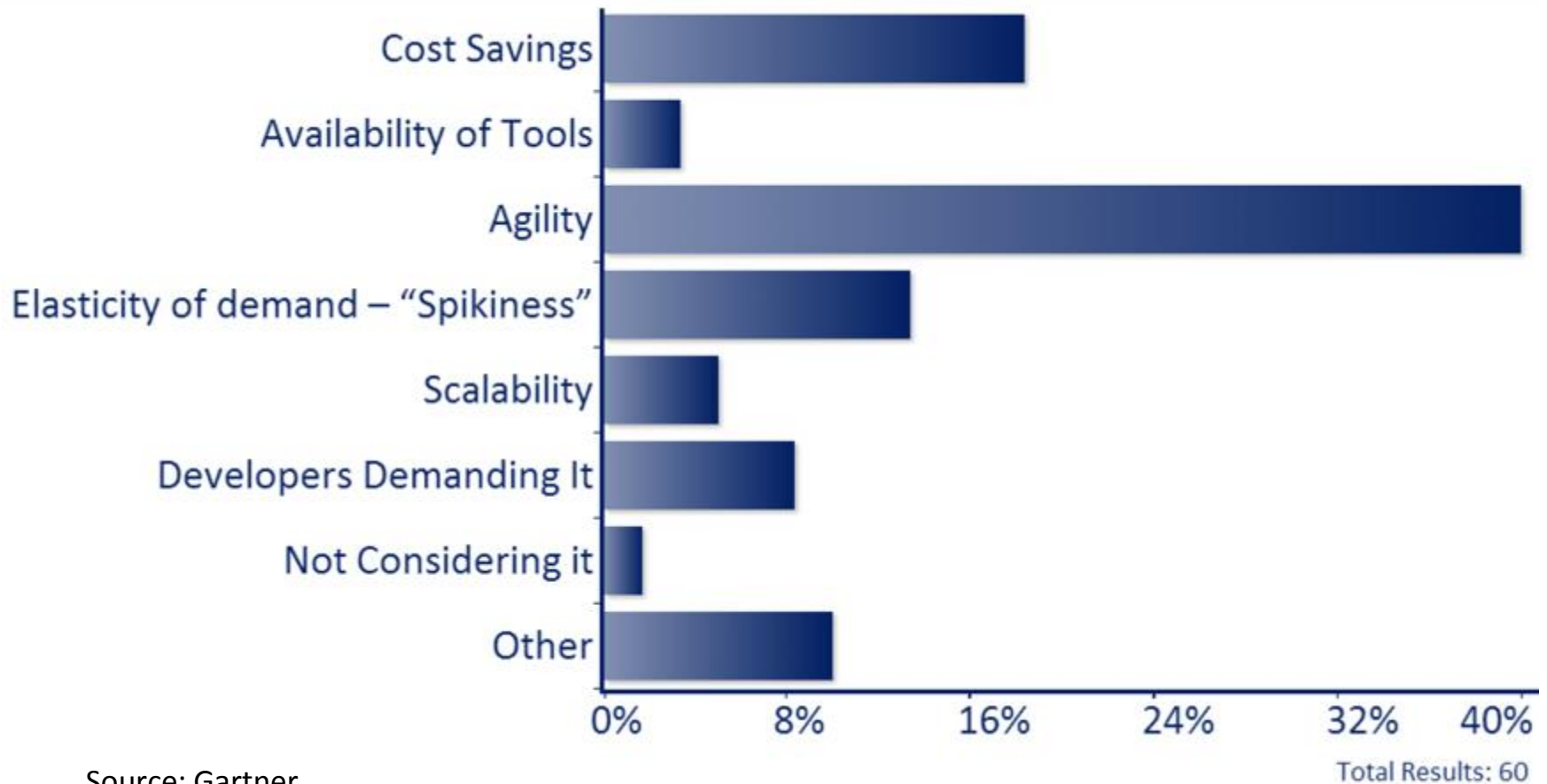
*Trust in, and value from, information systems*

**San Francisco Chapter**











The "CyberSizeIT" logo is rendered in a large, stylized font with a red-to-white gradient and a thick white outline. The background of the slide features a stylized illustration of the San Francisco skyline, including the Golden Gate Bridge and various city buildings, in a muted color palette of yellows, greys, and reds.



# CyberSizeIT

# Primary Motivation for Deploying Public Cloud IaaS



# Shared Responsibility of Security

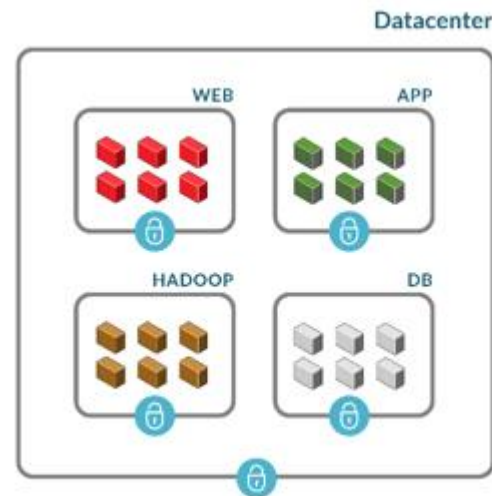
Control Category	Responsibility	
	IaaS Provider	Subscriber
Application Security		
Instance		
Network		
IaaS Infrastructure		
Physical facilities		

Low Responsibility   
 High Responsibility 

Source: Gartner

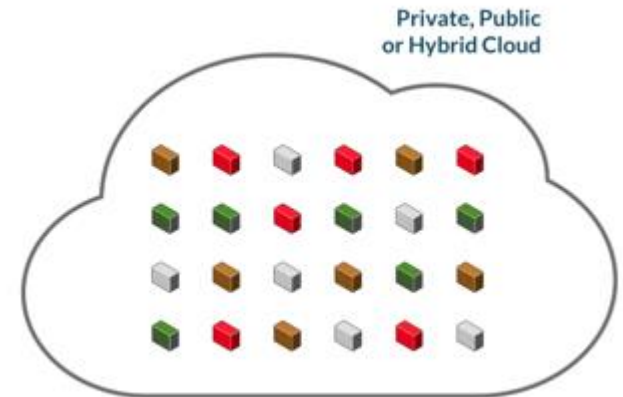
# Traditional Security

- Perimeter
- Network segmentation
- Strict change controls
- Slower rate of change
- Dedicated security hardware



# Agile Security Needed

- Shared responsibility needed
- No natural perimeter
- No network segmentation
- Elastic and on-demand
- No dedicated security hardware




# OVERVIEW OF TOP 20 SECURITY CONTROLS



The "CyberSizelT" logo is rendered in a large, stylized, red font with a white outline. The letters are slightly irregular, giving it a hand-drawn or artistic feel. In the background, there is a silhouette of the San Francisco skyline, including the Golden Gate Bridge and various skyscrapers, set against a light yellow and orange gradient sky.



# What are the Top 20 Critical Controls?

- 
- A prioritized, risk-based approach to cybersecurity
  - In 2008, the NSA led a consortium of security professionals from government and experts from the private industry, who were asked: “In practice, what works and where do you start?”
  - The Critical Controls have become a blueprint to help CISOs deploy controls that have the greatest impact in improving risk posture
  - Organizations should focus first on securing the business, then documenting the process to show compliance second

# Five Critical Tenets Used to Develop the Controls

1. Offense informs defense

2. Prioritization

3. Metrics

4. Continuous monitoring

5. Automation

# Five Critical Tenets:

## #1 – Offense Informs Defense

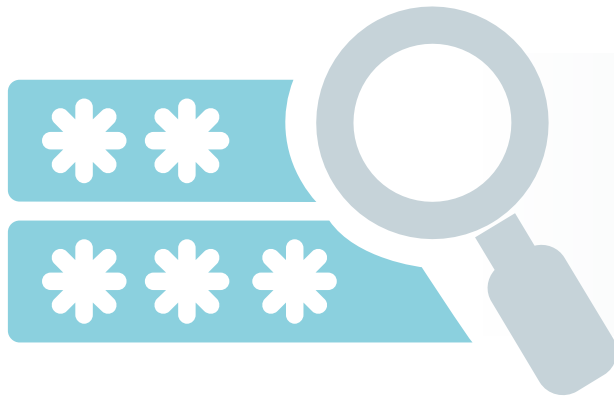
Intelligence agencies have performed  
thousands of investigations



Controls are derived from the most  
common attack patterns

# Five Critical Tenets:

## #2 – Prioritization



Some controls have  
greater impact on security  
risk than others

Should I focus on  
configuration  
or awareness  
training?

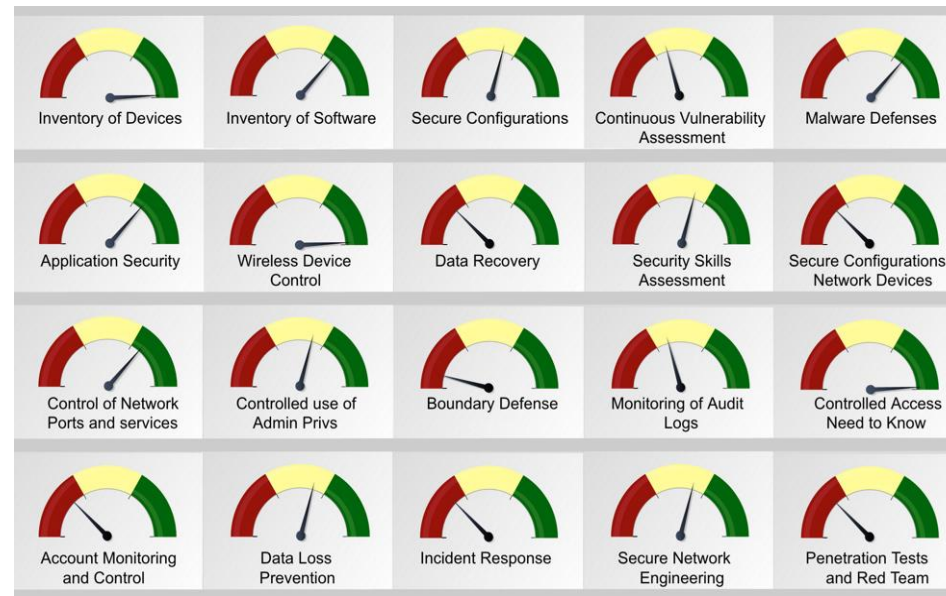
monitoring



# Five Critical Tenets:

## #3 – Metrics

- How many servers are out of compliance with policy?
- What percentage of my servers have critical vulnerabilities?



# Five Critical Tenets:

## #4 – Continuous Monitoring

Understand the state of systems at any given time



Critical for rapid response

A continuous feedback loop to **validate your security controls** is essential

# Five Critical Tenets:

## #5 – Automation

Security teams need to find ways  
to do more with less

Managing workloads in elastic  
cloud environments requires  
automation

# 184 Sub-Controls Grouped into Four Categories

1

■ Quick wins

2

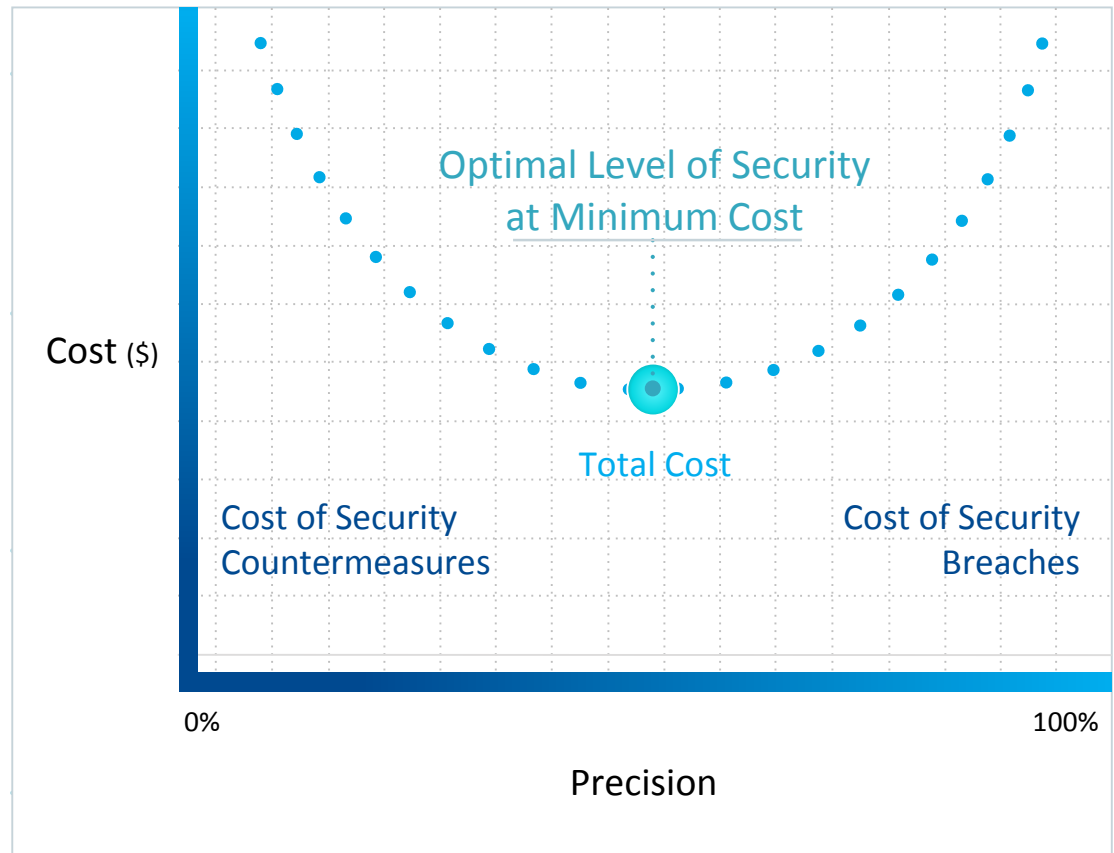
■ Visibility and Attribution

3

■ Configuration and Hygiene

4

■ Advanced





# ADAPTING CONTROLS TO THE CLOUD



The CyberSizeIT logo is rendered in a large, stylized, red font with a white outline. It is positioned over a graphic of the San Francisco skyline, which includes the Golden Gate Bridge and various city buildings. The background of the slide is a dark silhouette of the city's outline.

# The Top 20 Critical Controls

	Critical Control	Effect on Attack Mitigation
1	Inventory of Authorized and Unauthorized Devices	Very High
2	Inventory of Authorized and Unauthorized Software	Very High
3	Secure configurations	Very High
4	Continuous Vulnerability Assessment and Remediation	Very High
5	Malware Defenses	High
6	Application Software Security	High
7	Wireless Device Control	High
8	Data Recovery Capability	Moderately High
9	Security Skills Assessment and Appropriate Training to fill Gaps	Moderately High
10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Moderately High
11	Limitation and Control of Network Ports, Protocols, and Services	Moderately High
12	Controlled Use of Administrative Privileges	Moderately High
13	Boundary Defense	Moderate
14	Maintenance, Monitoring, and Analysis of Audit Logs	Moderate
15	Controlled Access Based on the Need to Know	Moderate
16	Account Monitoring and Control	Moderate
17	Data Loss Prevention	Moderately Low
18	Incident Response Capability	Moderately Low
19	Secure Network Engineering	Low
20	Penetration Tests and Red Team Exercises	Low

# #1: Inventory of Authorized and Unauthorized Devices

Control	Description	Category
CSC1-1	Deploy an <b>automated asset discovery tool</b> . Employ both active and passive tools.	Quick Win
CSC1-4	Record network address, system name, purpose and asset owner.	Visibility/ Attribution
CSC1-5	Deploy network level via <b>802.1x</b> to limit and control which devices can be connected to the network. Must be tied to inventory.	Configuration/ Hygiene
CSC1-6	Deploy <b>Network Access Control</b> . Systems must comply with business defined policy.	Configuration/ Hygiene

In the public cloud, use host-based firewalls to keep unauthorized or unmanaged systems off your network

Standardize across public, private or hybrid cloud deployments

## #2: Inventory of Authorized and Unauthorized Software

Control	Description	Category
CSC2-2	Devise a list of authorized software and use <b>file integrity checking</b> to validate that the software has not been modified.	Quick Win
CSC2-3	<b>Scan for unauthorized software</b> and version and generate alerts.	Quick Win
CSC2-4	Deploy a <b>software inventory tool</b> . Track OS, applications, version info, patch levels.	Visibility
CSC2-5	The software inventory systems must be <b>integrated</b> with the hardware asset inventory so that all devices and associated software are tracked from a single location.	Visibility

Maintaining a real-time inventory of software enables rapid response

## #3: Secure Configurations for Hardware and Software

Control	Description	Category
CSC3-3	<b>Limit administrative privileges</b> to very few users who can modify the configuration of the underlying operating system.	Quick Win
CSC3-8	Utilize <b>file integrity checking tools</b> to ensure that critical system files (including sensitive system and application executables, libraries and configurations) have not been altered.	Configuration /Hygiene
CSC3-9	Implement and test an automated <b>configuration monitoring system</b> . This includes detecting new listening ports, new administrative users, changes to group and local policy objects, (where applicable) and new services running on a system.	Advanced

Developing initial configuration settings is a complex task and systems must be continually managed to avoid security “decay”

In the cloud, control costs using lightweight security solutions which provide breadth

## #4: Continuous Vulnerability Assessments & Remediation

Control	Description	Category
CSC4-1	Run <b>automated vulnerability scanning tools</b> against all systems on the network on a weekly (or more frequent) basis.	Quick Win
CSC4-6	<b>Monitor logs</b> for unapproved scanning activity.	Visibility
CSC4-9	Evaluate critical patches in a test environment before pushing them into production on enterprise systems.	Configuration/ Hygiene
CSC4-10	Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability.	Configuration/ Hygiene

Continuous monitoring of vulnerabilities enables rapid response

Host based scanners provide great visibility, efficiency and speed

## #5: Malware Defenses

Control	Description	Category
CSC5-1	Employ automated tools to continuously monitor workstations, servers and mobile devices with anti-virus, anti-spyware, personal firewalls and <b>host-based IPS functionality</b> . All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.	Quick Win
CSC5-8	Ensure that automated monitoring tools use <b>behavior-based anomaly detection</b> to complement traditional signature-based detection.	Visibility/ Attribution
CSC5-11	Enable <b>DNS query logging</b> to detect hostname lookup for known malicious C2 domains.	Advanced

As malware becomes more evasive, re-assess NIDS vs. HIDS

Monitor logs, file changes, firewall connections and policy violations

## #6: Application Security

Control	Description	Category
CSC6-1	For all acquired application software, check that the version you are using is still supported by the vendor. If not, update to the most current version and install all relevant patches and vendor security recommendations.	Quick Win
CSC6-4	Test in-house-developed and third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to deployment.	Visibility/ Attribution
CSC6-9	For applications that rely on a database and use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.	Configuration/ Hygiene

Modern web applications are distributed, dynamic and lack a perimeter

Real-time assessment into an application's security posture is critical for defending against new attacks



# The Top 20 Critical Controls: #7-8

	Critical Control	Effect on Attack Mitigation
1	Inventory of Authorized and Unauthorized Devices	Very High
2	Inventory of Authorized and Unauthorized Software	Very High
3	Secure configurations	Very High
4	Continuous Vulnerability Assessment and Remediation	Very High
5	Malware Defenses	High
6	Application Software Security	High
7	Wireless Device Control	High
8	Data Recovery Capability	Moderately High
9	Security Skills Assessment and Appropriate Training to fill Gaps	Moderately High
10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Moderately High

## #9: Security Skills Assessment and Appropriate Training

Control	Description	Category
CSC9-2	Deliver training to fill the skills gap. If possible, use more senior staff to deliver the training. A second option is to have outside teachers provide training onsite so the examples used will be directly relevant.	Quick Win
CSC9-3	Implement an online security awareness program that (1) focuses only on the methods commonly used in intrusions that can be blocked through individual action, (2) is delivered in short online modules convenient for employees and (3) is updated frequently (at least annually) to represent the latest attack techniques.	Quick Win

Security professionals must make security processes more embedded, faster and more continuous

The cloud accelerates DevOps because it offers scalable environments to develop and test code

# The Top 20 Critical Controls: #10

	Critical Control	Effect on Attack Mitigation
1	Inventory of Authorized and Unauthorized Devices	Very High
2	Inventory of Authorized and Unauthorized Software	Very High
3	Secure configurations	Very High
4	Continuous Vulnerability Assessment and Remediation	Very High
5	Malware Defenses	High
6	Application Software Security	High
7	Wireless Device Control	High
8	Data Recovery Capability	Moderately High
9	Security Skills Assessment and Appropriate Training to fill Gaps	Moderately High
10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Moderately High

# The Top 20 Critical Controls: #11-12

	Critical Control	Effect on Attack Mitigation
11	Limitation and Control of Network Ports, Protocols, and Services	Moderately High
12	Controlled Use of Administrative Privileges	Moderately High
13	Boundary Defense	Moderate
14	Maintenance, Monitoring, and Analysis of Audit Logs	Moderate
15	Controlled Access Based on the Need to Know	Moderate
16	Account Monitoring and Control	Moderate
17	Data Loss Prevention	Moderately Low
18	Incident Response Capability	Moderately Low
19	Secure Network Engineering	Low
20	Penetration Tests and Red Team Exercises	Low

## #13: Boundary Defense

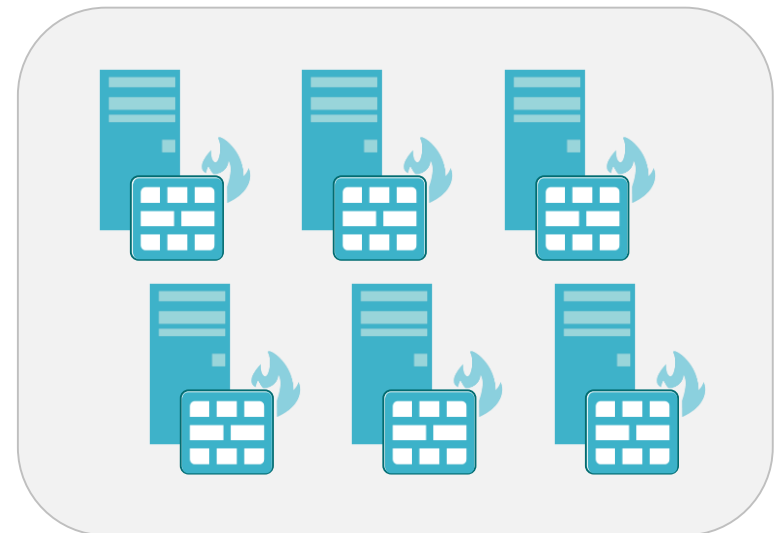
Control	Description	Category
CSC13-2	On DMZ networks, configure monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) to record at least packet header information, and preferably <b>full packet header and payloads of the traffic</b> destined for or passing through the network border.	Quick Win
CSC13-4	Deploy <b>network-based IDS sensors</b> on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems.	Visibility/ Attribution

In the public cloud, use host-based firewalls to keep unauthorized systems off your network

Re-evaluate intrusion detection deployment

## #13: Boundary Defense

- Adopt a Least Privilege strategy
- Eliminate “soft and chewy” networks
- Host based firewalls provide the **highest level of micro segmentation**



## #14: Monitoring & Analysis of Audit Logs

Control	Description	Category
CSC14-5	Have security personnel and/or system administrators run biweekly reports that <b>identify anomalies in logs</b> . They should then actively review the anomalies, documenting their findings.	Quick Win
CSC14-6	Configure network boundary devices, including firewalls, <b>network-based IPS</b> , and inbound and outbound proxies, to verbosely log all traffic (both allowed and blocked) arriving at the device.	Visibility
CSC14-8	Deploy a SIEM (Security Incident and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for <b>log correlation and analysis</b> .	Visibility

Create whitelists and blacklists and report/alert on anomalies

Automate the daily log review process

# The Top 20 Critical Controls: #15-18

	Critical Control	Effect on Attack Mitigation
11	Limitation and Control of Network Ports, Protocols, and Services	Moderately High
12	Controlled Use of Administrative Privileges	Moderately High
13	Boundary Defense	Moderate
14	Maintenance, Monitoring, and Analysis of Audit Logs	Moderate
15	Controlled Access Based on the Need to Know	Moderate
16	Account Monitoring and Control	Moderate
17	Data Loss Prevention	Moderately Low
18	Incident Response Capability	Moderately Low
19	Secure Network Engineering	Low
20	Penetration Tests and Red Team Exercises	Low



## #19: Secure Network Engineering

Control	Description	Category
CSC19-1	Design the network using a minimum of a <b>three-tier architecture</b> (DMZ, middleware, and private network). Any system accessible from the Internet should be on the DMZ, but DMZ systems should never contain sensitive data.	Quick Win
CSC19-4	Segment the enterprise network into multiple, separate <b>trust zones</b> to provide more granular control of system access and additional intranet boundary defenses.	Configuration/ Hygiene

In the public cloud, use host-based firewalls to build multi-tiered networks

# The Top 20 Critical Controls: #20

	Critical Control	Effect on Attack Mitigation
11	Limitation and Control of Network Ports, Protocols, and Services	Moderately High
12	Controlled Use of Administrative Privileges	Moderately High
13	Boundary Defense	Moderate
14	Maintenance, Monitoring, and Analysis of Audit Logs	Moderate
15	Controlled Access Based on the Need to Know	Moderate
16	Account Monitoring and Control	Moderate
17	Data Loss Prevention	Moderately Low
18	Incident Response Capability	Moderately Low
19	Secure Network Engineering	Low
20	Penetration Tests and Red Team Exercises	Low

# LEVERAGE CONTROLS TO BUILD A HIGHLY SECURE CLOUD INFRASTRUCTURE



The CyberSizeIT logo is rendered in a large, stylized, red font with a white outline. It is positioned over a background illustration of the San Francisco skyline, which includes the Golden Gate Bridge and various city buildings. The illustration is in a muted, painterly style with a warm color palette.

# Moving to the Cloud Securely

- Use the Top 20 Controls as a guide to bake security into your cloud deployment
- Develop repeatable processes
- Implement strong technology
  - Lightweight / provides breadth
  - Automated / scalable / API / SaaS
  - Works across clouds
  - Continuous monitoring
- Benchmark yourself!



# Thank You!

Learn more:

[www.cloudpassage.com](http://www.cloudpassage.com)

[info@cloudpassage.com](mailto:info@cloudpassage.com)