Microsoft Cloud Security Gap Analysis

Mapping Microsoft 365 to the CIS Top 20

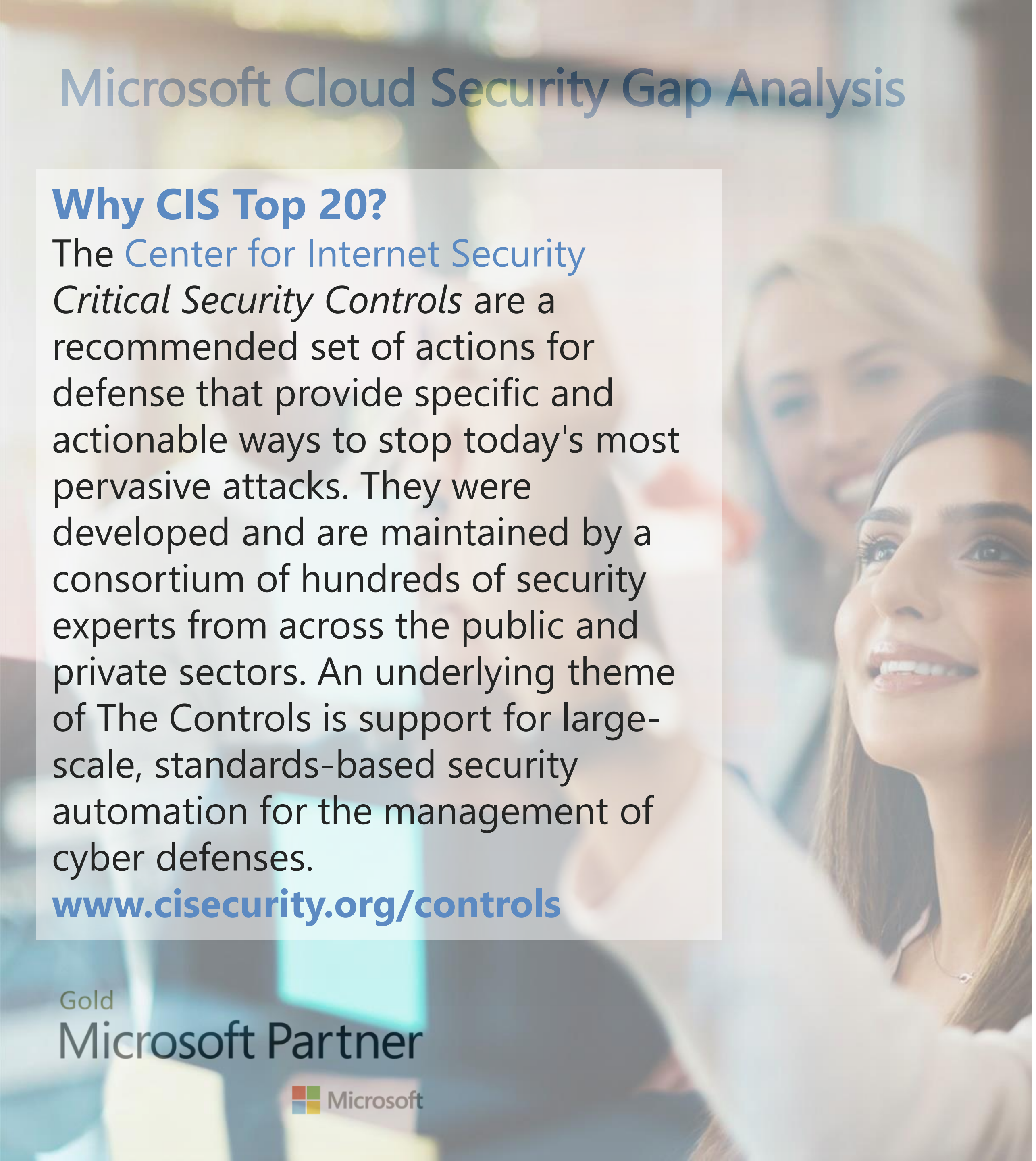
Gold
Microsoft Partner
Microsoft

CompuNet, Inc.

Having moved to the Microsoft cloud, securing your environment is one of the most important next steps to consider. The risk that organizations incur when shifting workloads to the Microsoft cloud requires new security controls to reduce the risk.

CompuNet will assist you by creating a security roadmap based on Microsoft 365 that aligns to the CIS Top 20. Use this roadmap to shift to the Microsoft cloud while maintaining your security around identity, data, applications, and workloads.

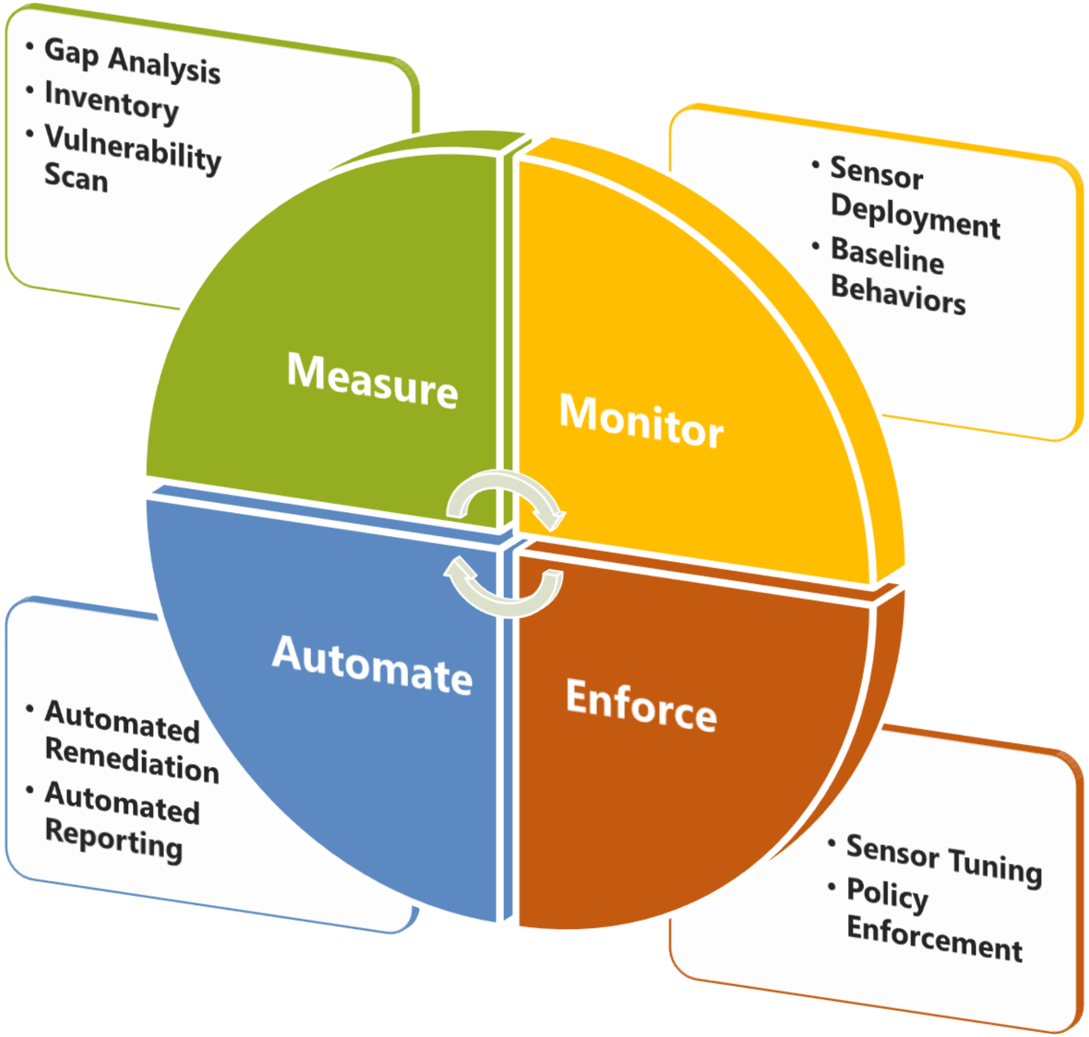
Microsoft Cloud Security Gap Analysis



Why CIS Top 20?

The Center for Internet Security *Critical Security Controls* are a recommended set of actions for defense that provide specific and actionable ways to stop today's most pervasive attacks. They were developed and are maintained by a consortium of hundreds of security experts from across the public and private sectors. An underlying theme of The Controls is support for large-scale, standards-based security automation for the management of cyber defenses.

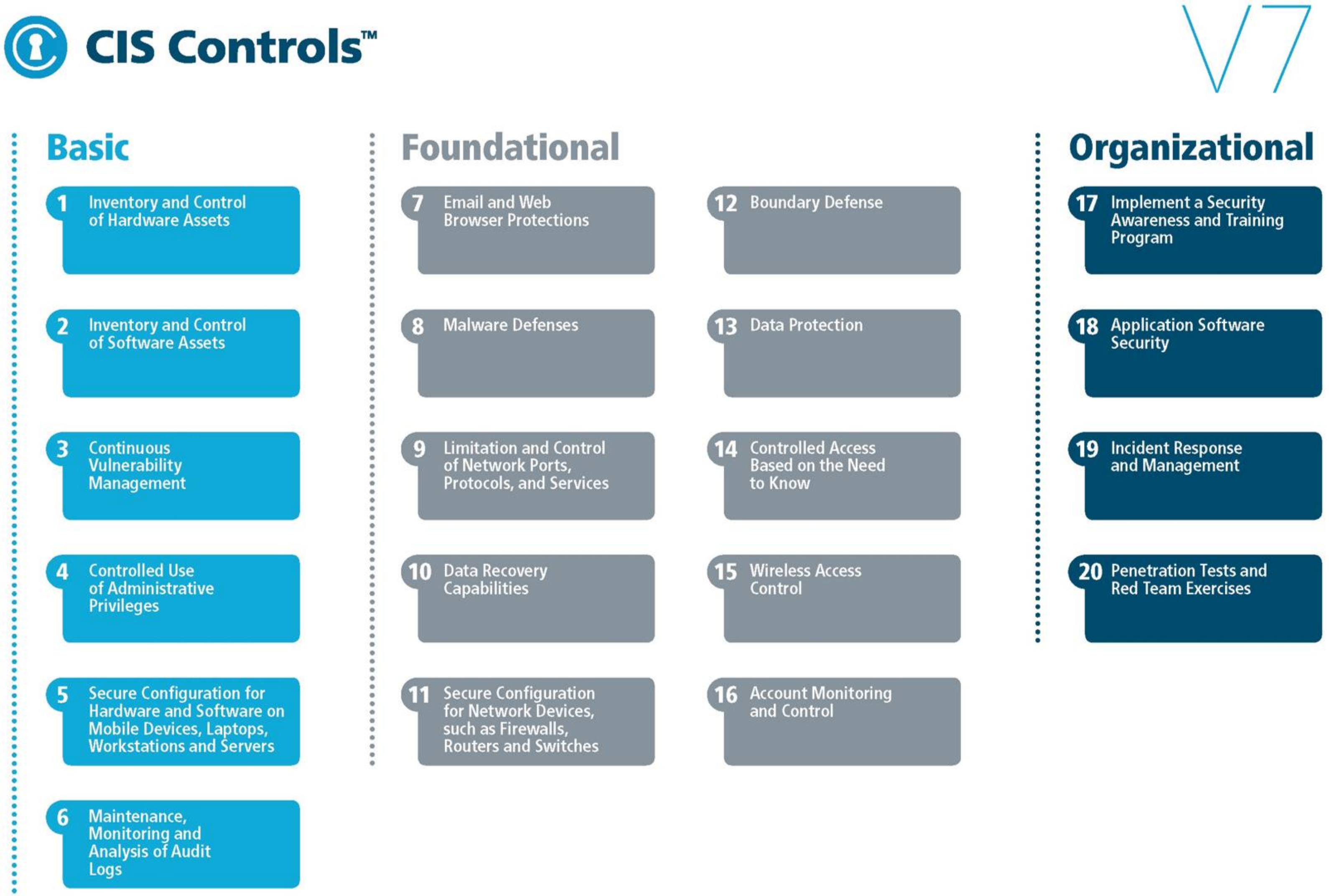
www.cisecurity.org/controls



Gold
Microsoft Partner
Microsoft

CompuNet, Inc.

Microsoft Cloud Security Gap Analysis



CIS Controls™ V7

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols, and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

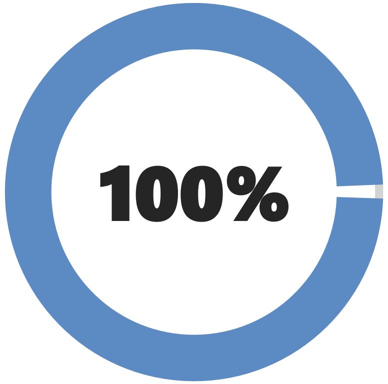
20 Penetration Tests and Red Team Exercises

Gold
Microsoft Partner
Microsoft

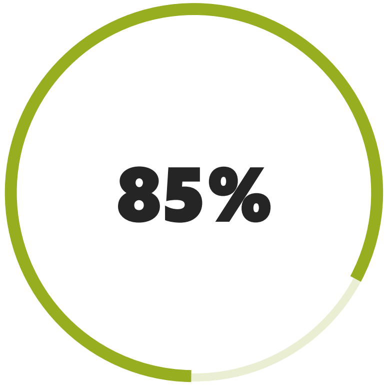
CompuNet, Inc.

Microsoft Cloud Security Gap Analysis

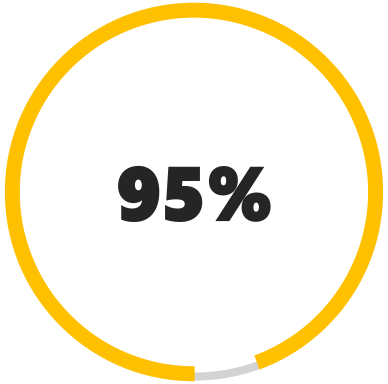
The Security Gap Analysis assesses the current state of security and identifies potential risks not currently being addressed.



The analysis will assess all CIS Top 20 categories



Applying just the first 6 CIS controls can reduce your risk of cyberattack by 85%



Implementing all 20 CIS controls increases risk reduction to 95%

Gold
Microsoft Partner
Microsoft

CompuNet, Inc.

Microsoft Cloud Security Gap Analysis

Microsoft has built a robust toolset you can use to ensure your organization complies with the Top 20 CIS controls.

These tools are integrated into the Microsoft Intelligent Security Graph that feeds into the Microsoft Secure Score and the Microsoft Compliance Score.

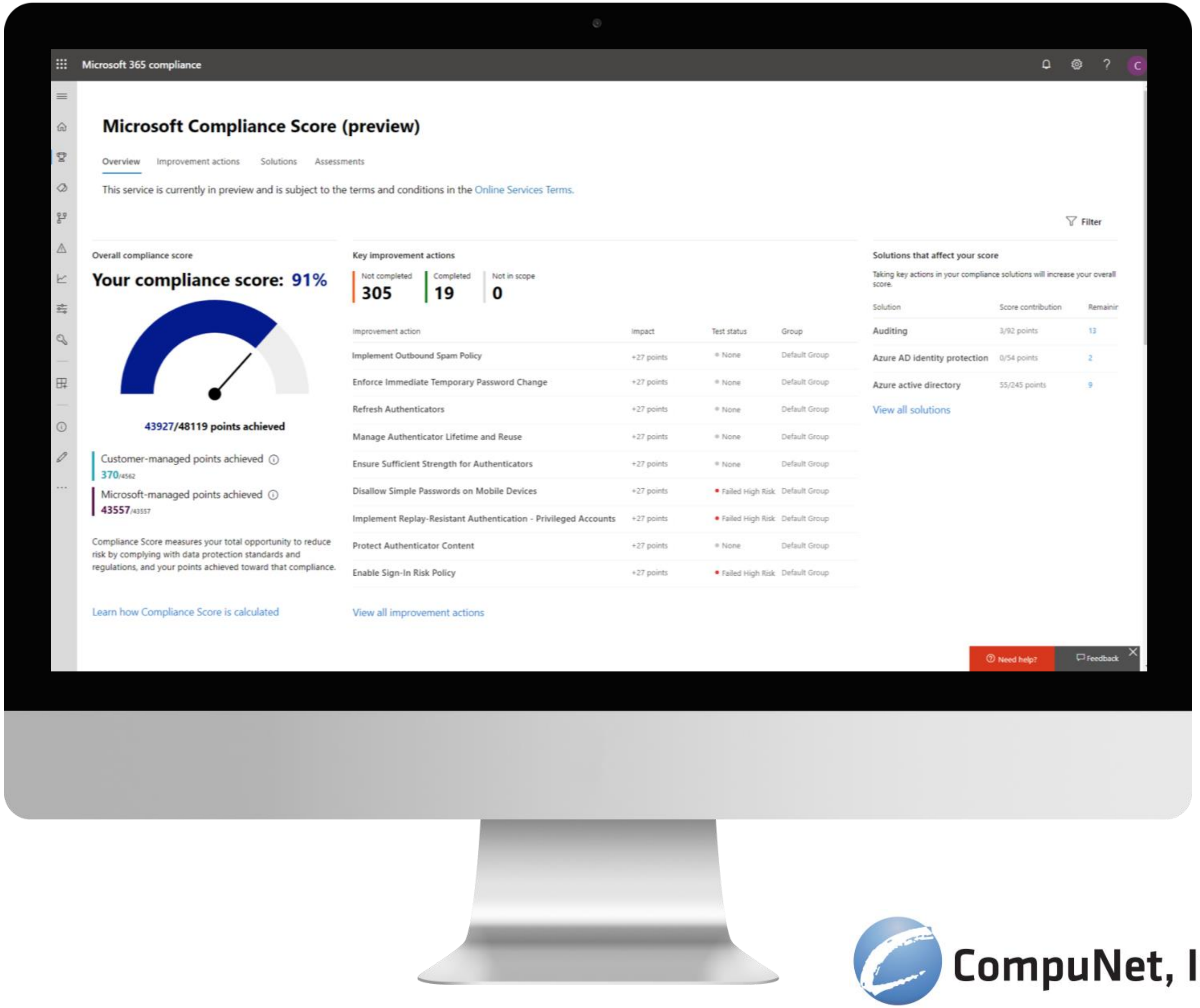
- **Azure Active Directory Premium**
- **Multi-Factor Authentication**
- **Office 365 Data Loss Prevention**
- **Microsoft Cloud App Security**
- **Azure Information Protection**
- **Office 365 Advanced Threat Protection**
- **Windows Defender Advanced Threat Protection**
- **Microsoft Intune**
- **Azure Sentinel**

Gold
Microsoft Partner
Microsoft

Microsoft Cloud Security Gap Analysis

Microsoft Compliance Score

- Simplify compliance & reduce risk.
- **Continuous assessments.** Detect and monitor control effectiveness automatically with a risk-based score
- **Recommended actions.** Reduce compliance risks with actionable guidance
- **Built-in control mapping.** Scale your compliance efforts with built-in mapping across regulations and standards



Microsoft Compliance Score (preview)

This service is currently in preview and is subject to the terms and conditions in the Online Services Terms.

Overall compliance score

Your compliance score: 91%

43927/48119 points achieved

Customer-managed points achieved
370/4562

Microsoft-managed points achieved
43557/43557

Compliance Score measures your total opportunity to reduce risk by complying with data protection standards and regulations, and your points achieved toward that compliance.

Learn how Compliance Score is calculated

Key improvement actions

Not completed	Completed	Not in scope
305	19	0

Improvement action	Impact	Test status	Group
Implement Outbound Spam Policy	+27 points	● None	Default Group
Enforce Immediate Temporary Password Change	+27 points	● None	Default Group
Refresh Authenticators	+27 points	● None	Default Group
Manage Authenticator Lifetime and Reuse	+27 points	● None	Default Group
Ensure Sufficient Strength for Authenticators	+27 points	● None	Default Group
Disallow Simple Passwords on Mobile Devices	+27 points	● Failed High Risk	Default Group
Implement Replay-Resistant Authentication - Privileged Accounts	+27 points	● Failed High Risk	Default Group
Protect Authenticator Content	+27 points	● None	Default Group
Enable Sign-In Risk Policy	+27 points	● Failed High Risk	Default Group

View all improvement actions

Solutions that affect your score

Taking key actions in your compliance solutions will increase your overall score.

Solution	Score contribution	Remainir
Auditing	3/92 points	13
Azure AD identity protection	0/54 points	2
Azure active directory	55/245 points	9

View all solutions

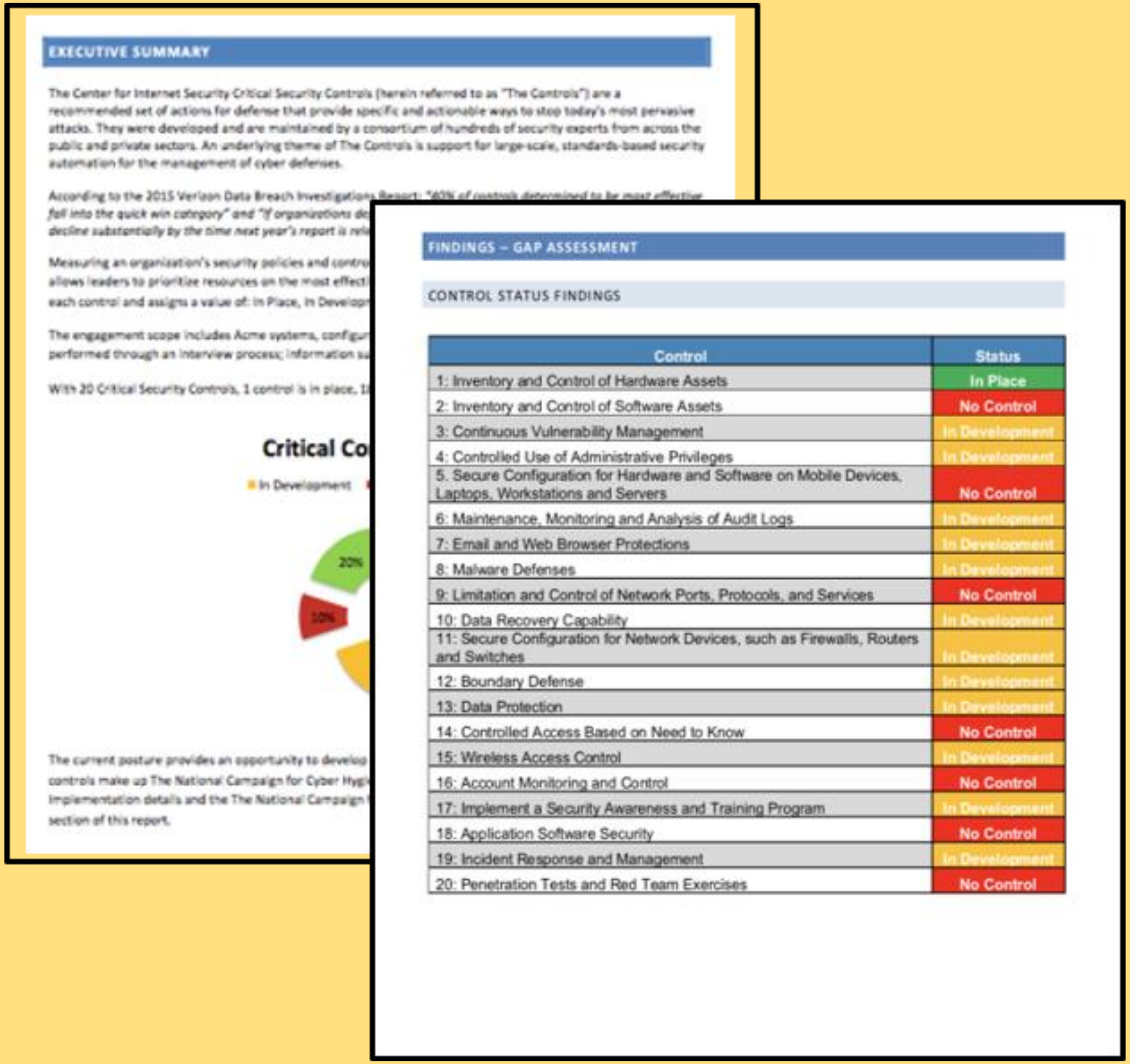
Gold
Microsoft Partner
Microsoft

CompuNet, Inc.

Microsoft Cloud Security Gap Analysis

CompuNet's Gap Analysis occurs in three phases:

1. Session 1 – Security benchmark and recommendations
2. Remediation period (self or guided)
3. Session 2 – Six months later – benchmarking and improvement analysis



EXECUTIVE SUMMARY

The Center for Internet Security Critical Security Controls (herein referred to as "The Controls") are a recommended set of actions for defense that provide specific and actionable ways to stop today's most pervasive attacks. They were developed and are maintained by a consortium of hundreds of security experts from across the public and private sectors. An underlying theme of The Controls is support for large-scale, standards-based security automation for the management of cyber defenses.

According to the 2015 Verizon Data Breach Investigations Report: *"40% of controls determined to be most effective fall into the quick win category" and "If organizations de*
decline substantially by the time next year's report is rele

Measuring an organization's security policies and contro
allows leaders to prioritize resources on the most effecti
each control and assigns a value of: In Place, In Develop

The engagement scope includes Acme systems, configur
performed through an interview process; information su

With 20 Critical Security Controls, 1 control is in place, 1

The current posture provides an opportunity to develop
controls make up The National Campaign for Cyber Hygi
implementation details and the The National Campaign
section of this report.

FINDINGS – GAP ASSESSMENT

CONTROL STATUS FINDINGS

Control	Status
1: Inventory and Control of Hardware Assets	In Place
2: Inventory and Control of Software Assets	No Control
3: Continuous Vulnerability Management	In Development
4: Controlled Use of Administrative Privileges	In Development
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	No Control
6: Maintenance, Monitoring and Analysis of Audit Logs	In Development
7: Email and Web Browser Protections	In Development
8: Malware Defenses	In Development
9: Limitation and Control of Network Ports, Protocols, and Services	No Control
10: Data Recovery Capability	In Development
11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	In Development
12: Boundary Defense	In Development
13: Data Protection	In Development
14: Controlled Access Based on Need to Know	No Control
15: Wireless Access Control	In Development
16: Account Monitoring and Control	No Control
17: Implement a Security Awareness and Training Program	In Development
18: Application Software Security	No Control
19: Incident Response and Management	In Development
20: Penetration Tests and Red Team Exercises	No Control

Gold
Microsoft Partner
Microsoft

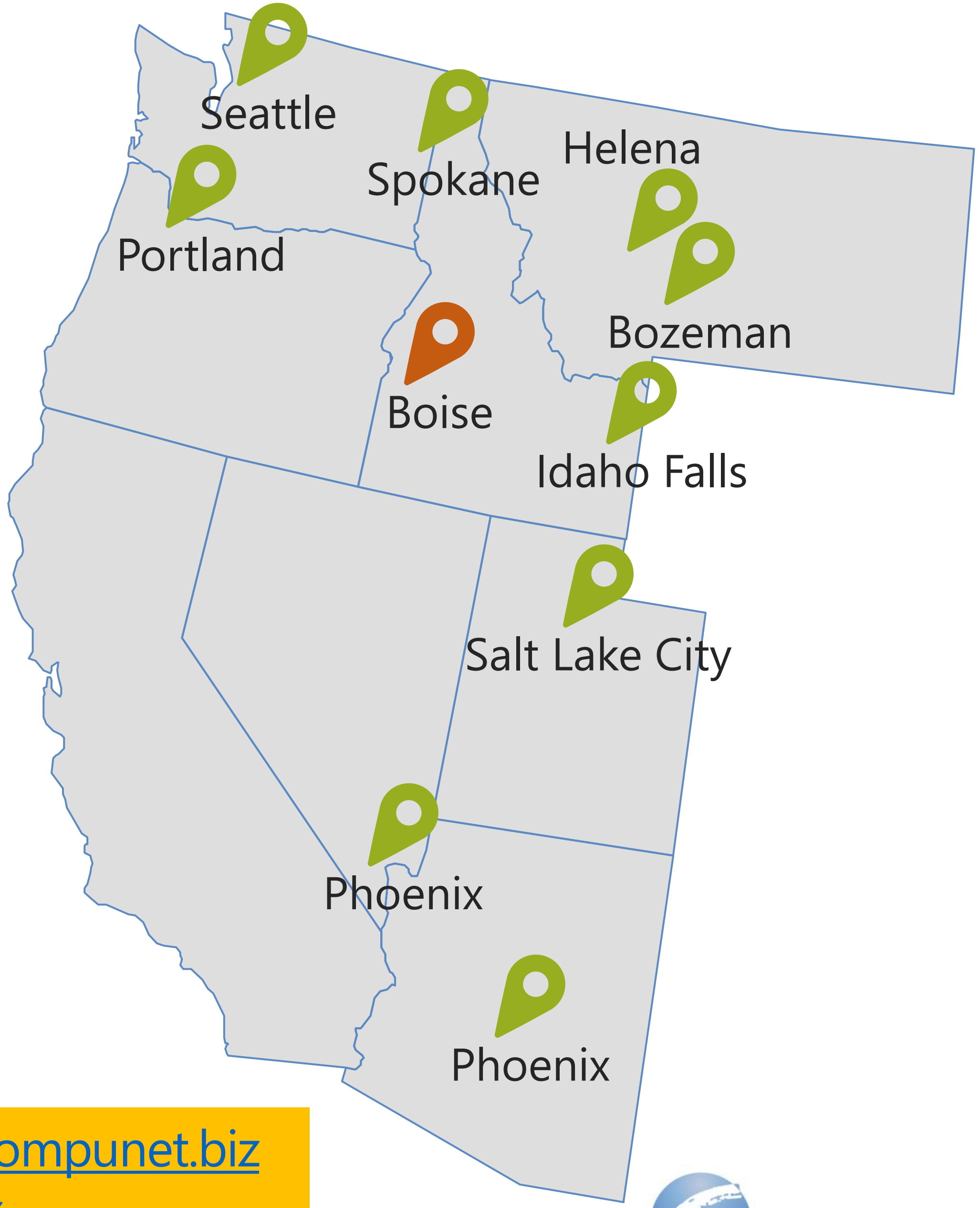
CompuNet, Inc.

About CompuNet, Inc.

CompuNet is a 'Managed Microsoft Partner' and is part of the 'One Commercial Partner' program. We work closely with Microsoft to provide the best on-site support possible while leveraging our experience with our customers' current environment.

Contact us today to protect your Microsoft Cloud environment!

- Microsoft Gold Partner
- Community-focused security practice
- Engineering-led, solutions-based approach



Gold
Microsoft Partner
Microsoft

Email: MicrosoftSales@compunet.biz
Web: www.compunet.biz

CompuNet, Inc.