ON2IT
ZERO TRUST INNOVATORS

ZERO TRUST STRATEGY: THE WHY, WHAT & HOW

ZERO TRUST AS A SERVICE
ISACA NL CHAPTER WEBINAR

MAY 22, 2024 • TIM TIMMERMANS

Classification: Public

TLP:AMBER

TIM TIMMERMANS

CISO NETHERLANDS
ON2IT CYBERSECURITY

Tim.Timmermans@on2it.net

linkedin.com/in/Tim-Timmermans

Classification: Public

Perspectives from 50+ Years' Practical Zero Trust Experience and Learnings on Buyer Expectations and Industry Promises

Yuri Bobbert[1,2(✉)], Jeroen Scheerder[2], and Tim Timmermans[2]

{yur

Abstract. Eve
issued an Exe
manufacturers
ZT focuses on
segmenting the
strict access ar
to systems. Th
Zero Trust app
causes Inform
implementatio
continue with
with a collecti
settings. The p
practitioners ca

Keywords: Ze
security · Lem

How Zero Trust as a Service (ZTaaS) Reduces the Cost of a Breach

A Conceptual Approach to Reduce the Cost of a Data Breach

Yuri Bobbert(✉) and Tim Timmermans

Abstra
society.
encing
proven
ditional
the envi
reducin
traditio
tion, te
Compa
financia
Zero Tr
It concl
age to r
Insurer

Keywo
Manage

Zero Trust and Compliance with Industry Frameworks and Regulations

A Structured Zero Trust Approach to Improve Cybersecurity and Reduce the Compliance Burden

Yuri Bobbert(✉) and Tim Timmermans

ON2IT, Zaltbommel, Netherlands

{yuri.bobbert,tim.timmermans}@on2it.net

Abstract. In 2021, the United States president released an Executive Order directing the implementation of Zero Trust to protect federal institutes from cyber incidents. Organisations, not limited to government agencies, find it challenging to translate Zero Trust from strategy to operational implementation. At the same time, regulatory and industry requirements on cybersecurity skyrocketed. This paper deals with this dual complexity of both implementing Zero Trust and, at the same time, ensuring compliance with regulatory standards and frameworks. We start this paper by presenting the challenging situation of organisations in the current cyber threat landscape when facing increasingly stringent regulatory requirements. Next, we will introduce the core principles of Zero Trust, followed by the five-step model for Zero Trust implementation, including security measures, presented as an architectural repository. We explain how an exhaustive mapping of the Zero Trust-based repository measures to all major current frameworks and standards supports compliance with regulatory and industry frameworks. This paper

TLP:AMBER

ZERO TRUST

A **strategy** designed to stop data breaches and make other cyberattacks unsuccessful by eliminating trust from digital systems.

WHY
IS ZERO TRUST RELEVANT

WHY

±70

SECURITY TOOLS INSTALLED

WHY

CYBER THREATS ARE INCREASING

Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom

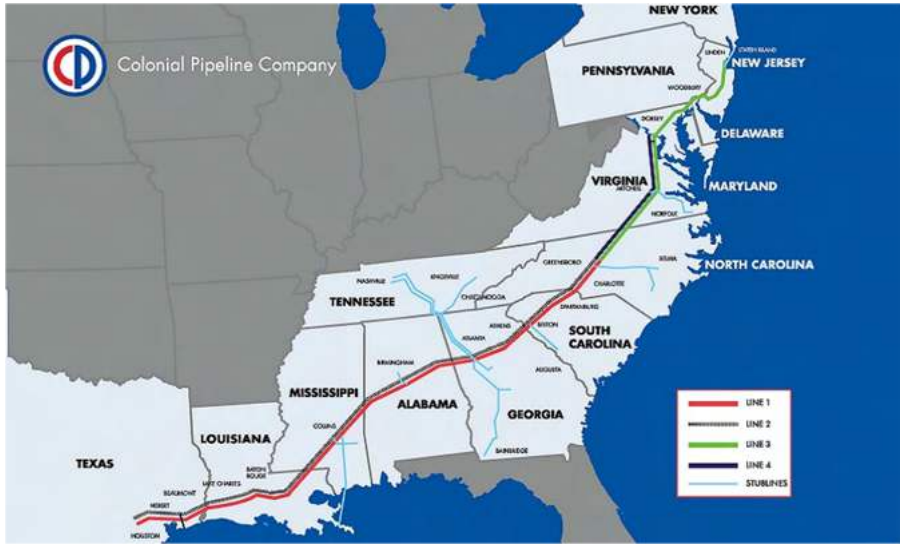
WSJ wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

May 19, 2021

A cyberattack on the U.S.'s largest fuel pipeline on May 7 forced a shutdown that triggered a spike in gas prices and shortages in parts of the Southeast. WSJ explains just how vulnerable the nation's critical energy infrastructure is to attack. Photo illustration: Liz Ornitz/WSJ

By Collin Eaton

and Dustin Volz



Colonial Pipeline Co. now faces at least two lawsuits seeking class action status in the aftermath of a ransomware attack in May that led the firm to shut down the operations of a 5,500-mile pipeline for nearly a week.

WHY

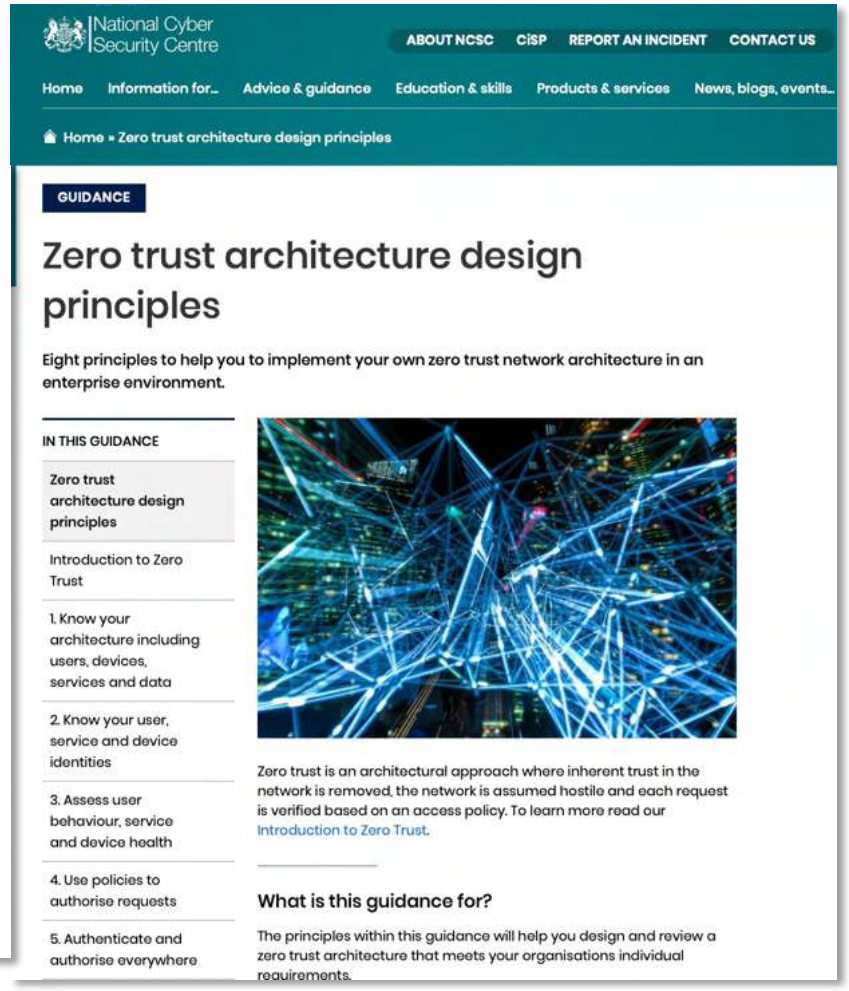
NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY



National Cyber Security Centre

ABOUT NCSC CiSP REPORT AN INCIDENT CONTACT US

Home Information for... Advice & guidance Education & skills Products & services News, blogs, events...

Home » Zero trust architecture design principles

GUIDANCE

Zero trust architecture design principles

Eight principles to help you to implement your own zero trust network architecture in an enterprise environment.

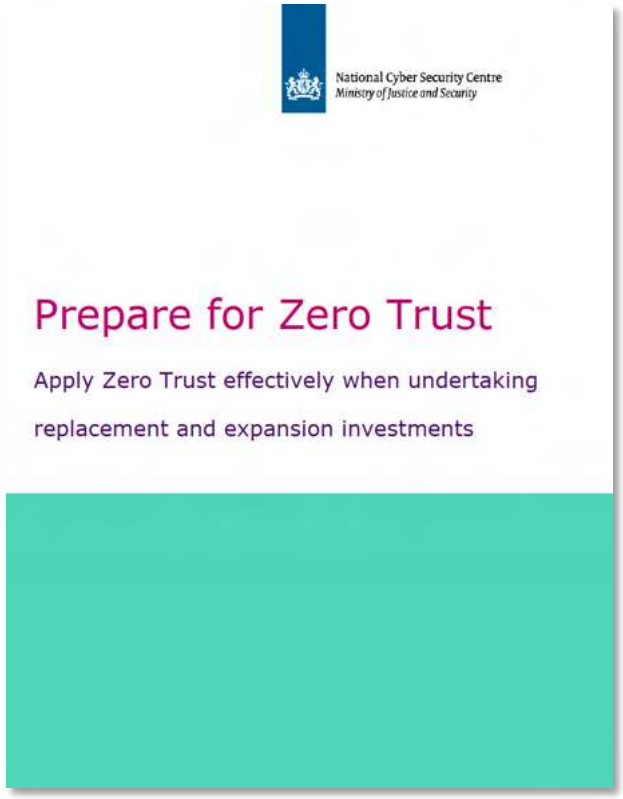
IN THIS GUIDANCE

- Zero trust architecture design principles
- Introduction to Zero Trust
- 1. Know your architecture including users, devices, services and data
- 2. Know your user, service and device identities
- 3. Assess user behaviour, service and device health
- 4. Use policies to authorise requests
- 5. Authenticate and authorise everywhere

Zero trust is an architectural approach where inherent trust in the network is removed, the network is assumed hostile and each request is verified based on an access policy. To learn more read our Introduction to Zero Trust.

What is this guidance for?

The principles within this guidance will help you design and review a zero trust architecture that meets your organisations individual requirements.



National Cyber Security Centre
Ministry of Justice and Security

Prepare for Zero Trust

Apply Zero Trust effectively when undertaking replacement and expansion investments

(89) Essential and important entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness, organise training for their staff and raise awareness concerning cyber threats, phishing or social engineering techniques. Furthermore, those entities should evaluate their own cybersecurity capabilities and, where appropriate, pursue the integration of cybersecurity enhancing technologies, such as artificial intelligence or machine-learning systems to enhance their capabilities and the security of network and information systems.

on2IT
ZERO TRUST INNOVATORS

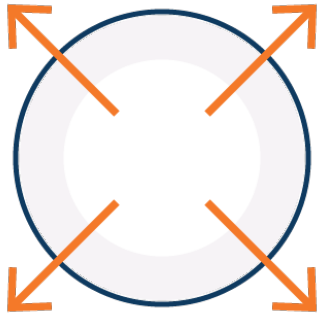
WHAT ARE ZERO TRUST CORE PRINCIPLES

TLP:AMBER

WHAT

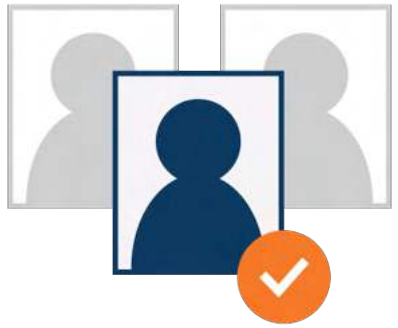
FOCUS ON BUSINESS OUTCOMES

WHAT



DESIGN FROM THE INSIDE OUT

WHAT



DETERMINE WHO/WHAT NEEDS ACCESS

WHAT

INSPECT AND LOG ALL TRAFFIC

HOW

TO IMPLEMENT ZERO TRUST

HOW

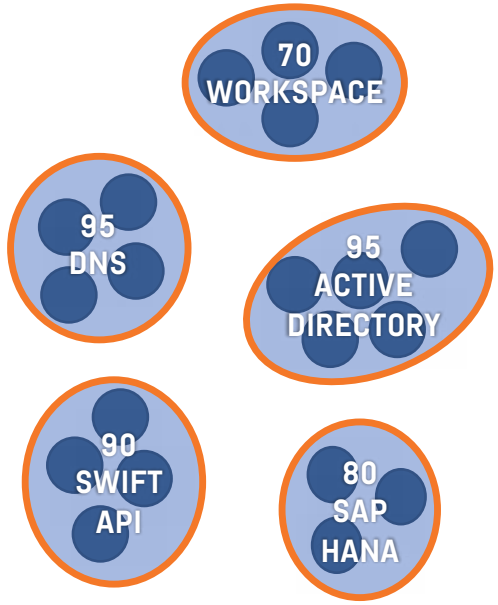
1 DEFINE THE PROTECT SURFACE

HOW

ATTACK SURFACE

PROTECT SURFACE

HOW

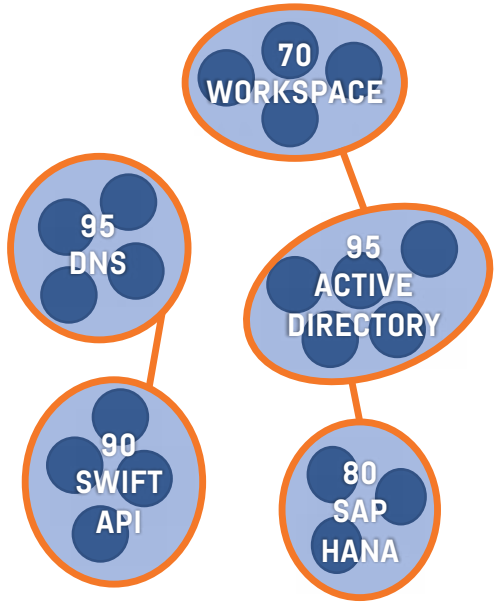

70
WORKSPACE
95
DNS
95
ACTIVE
DIRECTORY
90
SWIFT
API
80
SAP
HANA

HOW

2

MAP THE TRANSACTION FLOWS

HOW

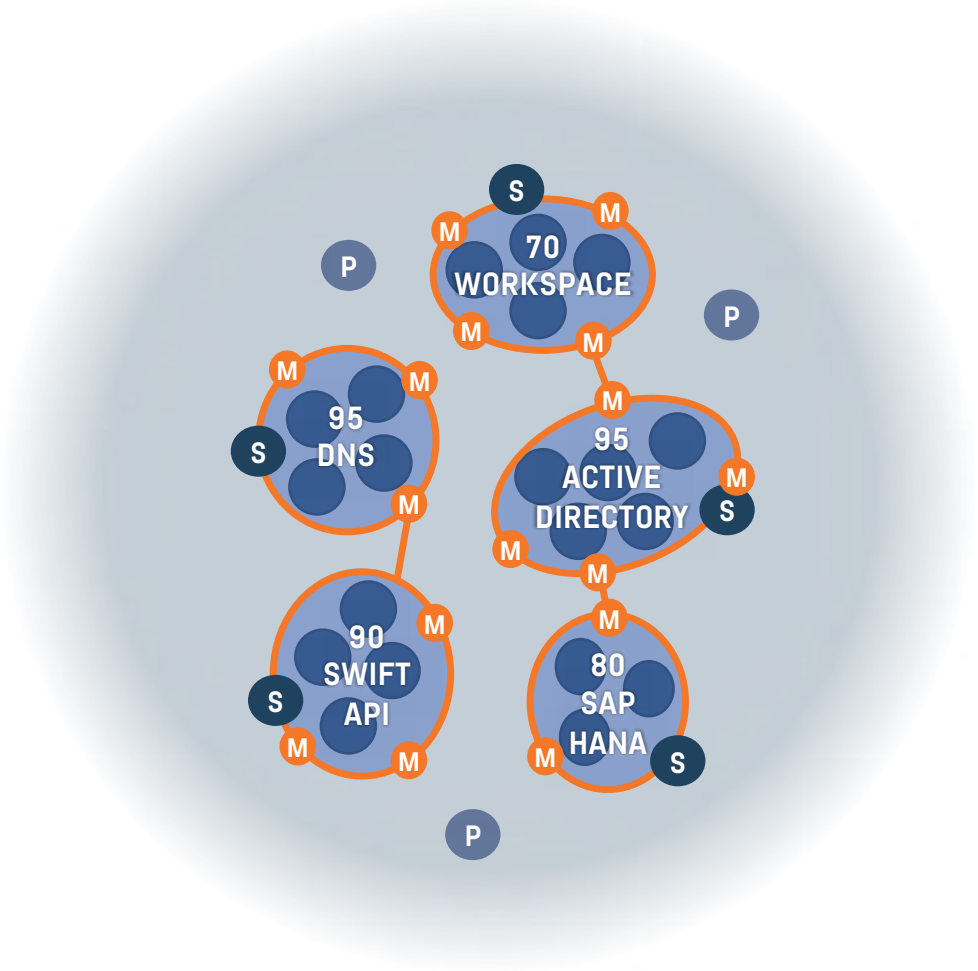

70
WORKSPACE
95
DNS
95
ACTIVE
DIRECTORY
90
SWIFT
API
80
SAP
HANA

HOW

3

BUILD A ZERO TRUST ARCHITECTURE

HOW



P **CORPORATE POLICY**

S **STANDARD**

M **MEASURE**

TLP:AMBER

HOW

ZERO TRUST		COMPLIANCE FRA			
CATEGORY (1-12)	PROTECT SURFACE MEASURE (1-33)	MITRE MITIGATIONS	ISO/IEC 27001:2022	FEDRAMP 2021BASELINE	DNB GOOD PRACTICE 2019/2022
1. Encryption	1.1 SSL Inspection M	M1020	A.8.21	AC-17 (2)	16.1 & 18.3 & 18.4 & 18.5 & 19.1
	1.2 Encryption at rest M	M1041	A.5.33 & A.8.24	AC-17 (2) & SC-28	2.2 & 10.4 & 11.3 & 11.4 & 12.1 & 12.2 & 12.3 & 18.5
	1.3 Encryption in Transit M	M1041	A.5.14 & A.5.33 & A.8.24	AC-17 (2)	12.3 & 18.5
2. Identity & Access Management	2.1 Centrally managed IAM M	M1036 & M1015 & M1018	A.5.16 & A.5.17	AC-2	6.1 & 7.1 & 17.1 & 17.2
	2.2 Restrict Control M	M1027 & M1026 & M1017	A.5.15 & A.5.18 & A.8.3	AC-6	2.2 & & 6.1 & 7.1 & 10.3 & 17.1 & 20.1
	2.3 Multi Factor Authentication (MFA) M	M1032	A.5.17 & A.8.5	IA-2 (11)	7.1 & 10.5 & 17.1
	2.4 Logging on Deviations M		A.8.15 & A.8.16	IA-2	1.2 & 16.1 & 17.1 & 17.2 & 18.4 & 19.1
...	...	...	...	...	...

ZERO TRUST		COMPLIANCE FRAMEWORKS AND STANDARDS
CATEGORY (1-12)	PROTECT SURFACE MEASURE (1-33)	ISO/IEC 27001:2022
1. Encryption	1.1 SSL Inspection	A.8.21
	1.2 Encryption at rest	A.5.33 & A.8.24
	1.3 Encryption in Transit	A.5.14 & A.5.33 & A.8.24
2. Identity & Access Management	2.1 Centrally managed IAM	A.5.16 & A.5.17
	2.2 Restrict Control	A.5.15 & A.5.18 & A.8.3
	2.3 Multi Factor Authentication (MFA)	A.5.17 & A.8.5
	2.4 Logging on Deviations	A.8.15 & A.8.16

P **CORPORATE POLICY**

S **STANDARD**

M **MEASURE**

TLP:AMBER

HOW

4

CREATE ZERO TRUST POLICY

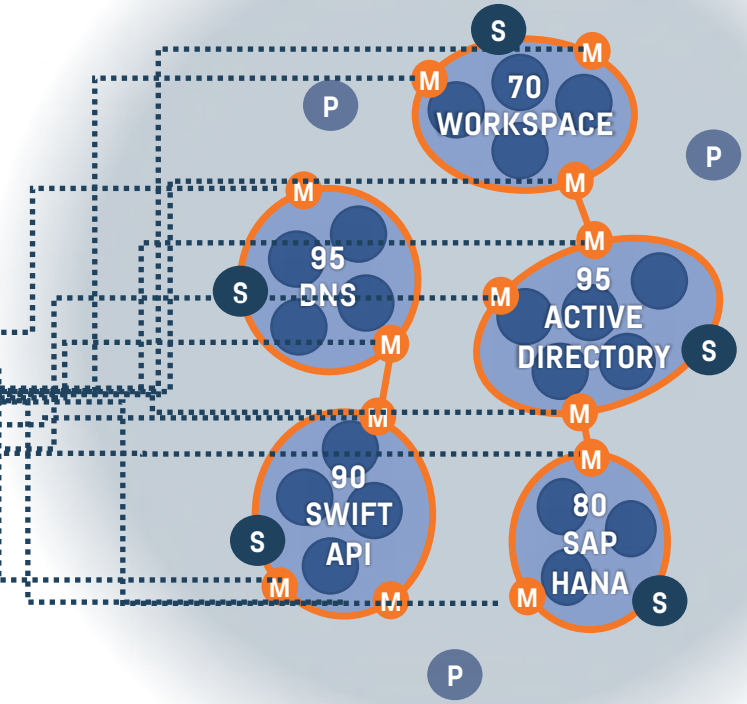
HOW

5

MONITOR & MAINTAIN THE NETWORK

HOW

MONITOR & MAINTAIN THE NETWORK



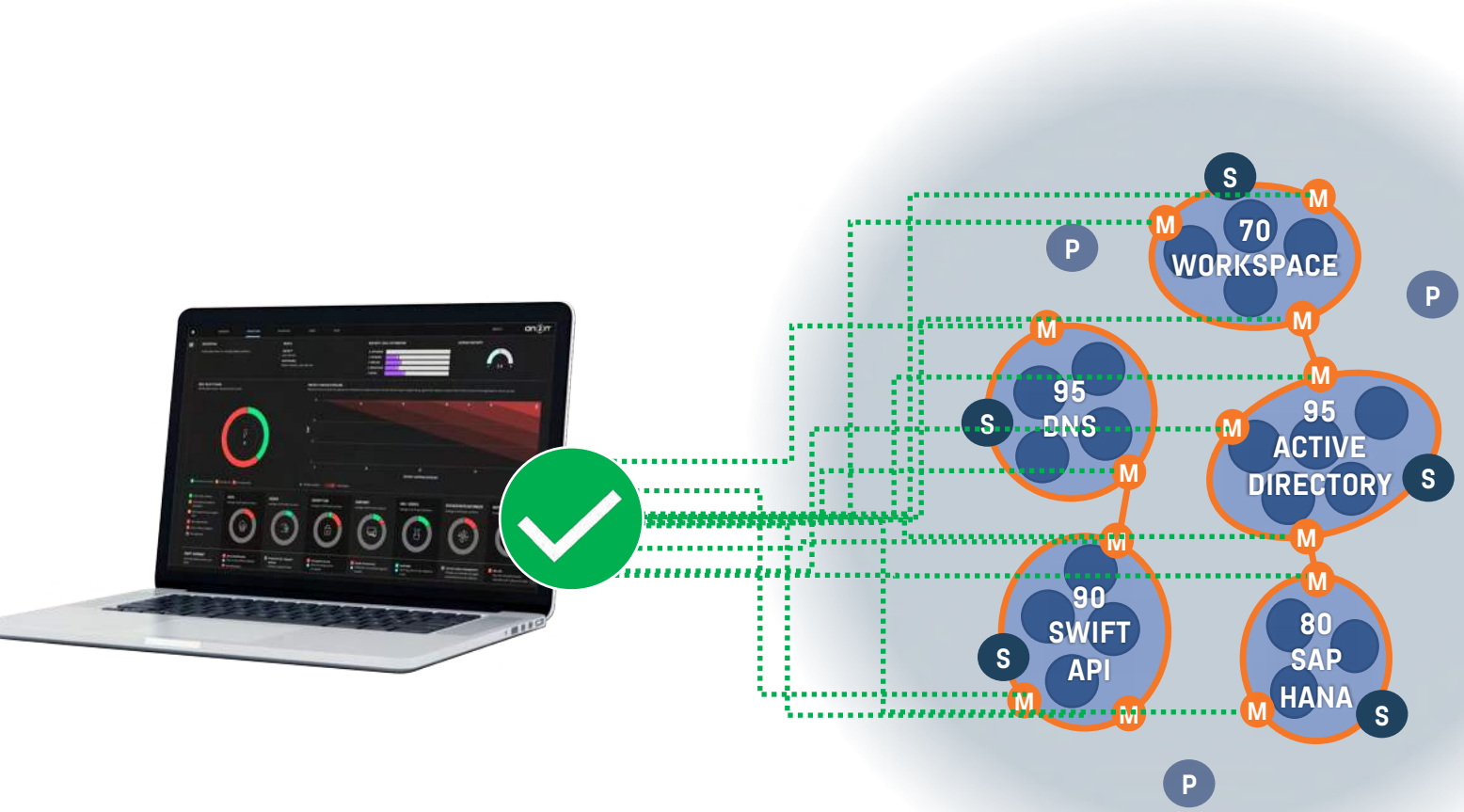
P CORPORATE POLICY

S STANDARD

M MEASURE

HOW

MONITOR & MAINTAIN THE NETWORK



- P CORPORATE POLICY
- S STANDARD
- M MEASURE
- V VALIDATION

ZERO TRUST

WHY
3 DRIVERS

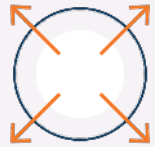
STRONGER CYBERSECURITY

MORE EFFECTIVE INVESTMENTS

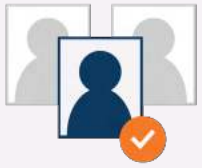
EASE COMPLIANCE

WHAT
4 PRINCIPLES

FOCUS ON BUSINESS OUTCOMES



DESIGN FROM THE INSIDE OUT



DETERMINE WHO/WHAT NEEDS ACCESS

INSPECT AND LOG ALL TRAFFIC

HOW
5 STEPS

1. DEFINE THE PROTECT SURFACE
2. MAP THE TRANSACTION FLOWS
3. BUILD A ZERO TRUST ARCHITECTURE
4. CREATE ZERO TRUST POLICY
5. MONITOR AND MAINTAIN THE NETWORK

TLP:AMBER

ZERO TRUST AS A SERVICE

CONTROLS MANAGEMENT	PROTECT SURFACE MANAGEMENT	EVENT MANAGEMENT	INCIDENT MANAGEMENT	IMPROVEMENT MANAGEMENT	COMPLIANCE MANAGEMENT

ON2IT
ZERO TRUST INNOVATORS

THANK YOU

ZERO TRUST AS A SERVICE
ISACA NL CHAPTER WEBINAR

MAY 22, 2024 • TIM TIMMERMANS

● Classification: Public