

# Managing Cyber Risk through Macro Economic Trends



**Sean Duca**Vice President & Chief Security Officer
JAPAC, Palo Alto Networks

#### **CYBERSECURITY MEGATRENDS**



Work is now an activity, not a place.



Cloud adoption has accelerated dramatically.



Software supply chains are more interconnected and complex.



The cyber talent gap has widened.



Attackers are increasingly emboldened and automated.

**76%** of global workers now want the option to work remotely.

Gallup

Remote Workplace Report, 2021

**59%** of all workloads were running in the cloud in 2022, up from 46% in 2021.

Gartner

State of Cloud Security Report, 2022

"Hundreds of millions of devices likely impacted by Log4i"

Jay Gazlay

CISA Vulnerability Management Office

**76%** of organizations say it's difficult to recruit and hire cybersecurity staff.

ISS

Cybersecurity Skills Report, 2022

**35** new ransomware groups emerged in 2022 and **ransomware** as a service is thriving.

Unit 42

Threat Research Report, 2022

#### **CYBERCRIME EXPECTED TO RISE**

10+

Publicly attributed cyber attacks per month



Increase in Nation State cyber incidents

#### Cybercrime worsens during economic downturn

**JBS** ransomware - US, CN, AU facilities shut down

Fujitsu hack

Ireland's national health service ransomware

Colonial Pipeline ransomware

**DDoS** attack on **Belgium** government

May

Verizon and Microsoft hacks

NATO, UK, NL warships fake data

1,182 UK Special Forces soldiers data leak

**Department of Energy nuclear weapons** supply chain attack

Jun

**Japan Olympics** data breach

Southeast Asia APT

**South Africa** port and freight halted

Kaseya hack 1,500 SMB ransomed

Jul

Belarus. Slovak. Iranian

Aua

governments breach

Russian election back

T-Mobile breach 50 million accounts

Poly Network \$600 million heist

Italian COVID 19 vaccine site hack

#### **BOARD ROOM**

#### **RESPONSIBILITIES**

#### **DIRECTORS**

Understand your current cyber resilience / maturity baseline.
Measure yourself against respected standards. Reasonableness frames everything.

You are aware of the risk, you assess the risk, and you make an informed decision as a board about an action or no action.

Company directors should beware that failure to adequately address cybersecurity risk or comply with relevant disclosure and reporting requirements, may be a breach of their directors' duties.



Know your **data holdings** and confirm appropriate management of those.

#### **STRESS TEST**

- Incident response and business continuity plans
- **2** Cyber compliance

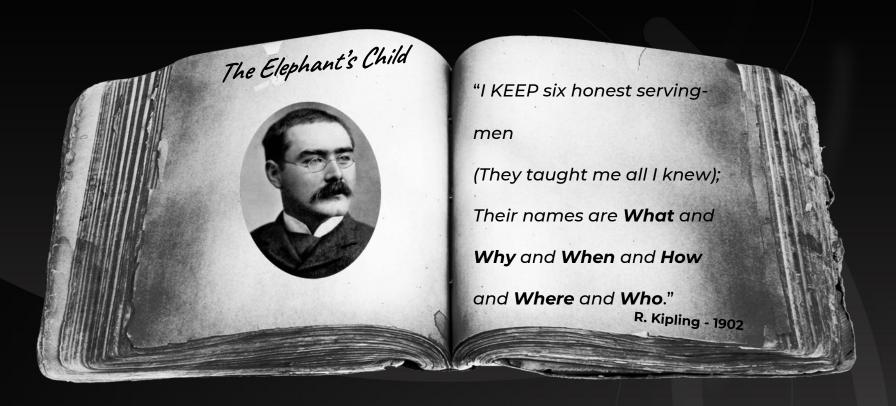


#### **DEFINING ZERO TRUST**

A strategic approach to cybersecurity that secures an organiSation by eliminating implicit trust and continuously validating every stage of a digital interaction.

# ZERO TRUST IN THE NETWORK /// paloalto

#### **REMOVING IMPLICIT TRUST**



#### **ZERO TRUST IN THE NETWORK**

slideshare-uploading

application function

slideshare

application

roadmap.pdf

file name

prodmgmt

group

**HTTP** 

protocol

confidential

data sensitivity



mjacobsen

client user

SSI

SSL protocol **R&D File Server** 

enterprise resource

172.16.1.10

source IP

TCP/443
destination port

22-05 9:30AM timestamp

64.81.2.23
destination IP

#### **ZERO TRUST IN THE NETWORK**

who

slideshare-uploading

application function

what

slideshare

application

how roadmap.pdf file name

why confidential data sensitivity

R&D File Server

enterprise resource

64.81.2.23

destination IP

prodmgmt

group

HTTP

protocol

mjacobsen

SSL protocol

client user

172.16.1.10

source IP

TCP/443

destination port

when

22-05 9:30AM timestamp

#### **ZERO TRUST IN THE NETWORK**

download

IT-admins group



172.16.1.10 source IP

web-browsing
application

HTTP

344 KB

SSL protocol

TCP/443
destination port

22-05 9:30AM timestamp

CreditCards.txt

file name

PCI data sensitivity



Finance Server

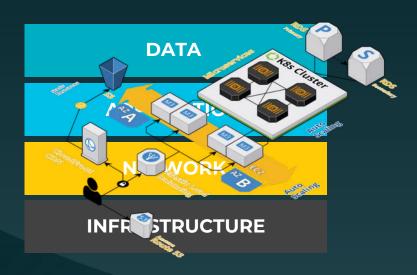
enterprise Resource

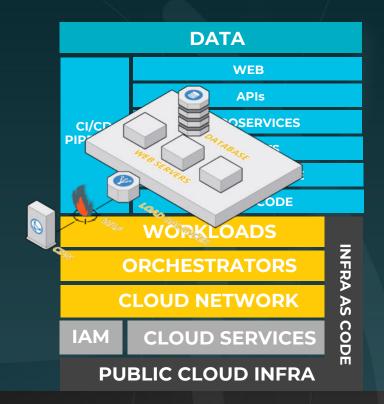
64.81.2.23
destination IP



#### **SECURING MODERN APPLICATIONS**

#### How apps werbuiltdebbeilt



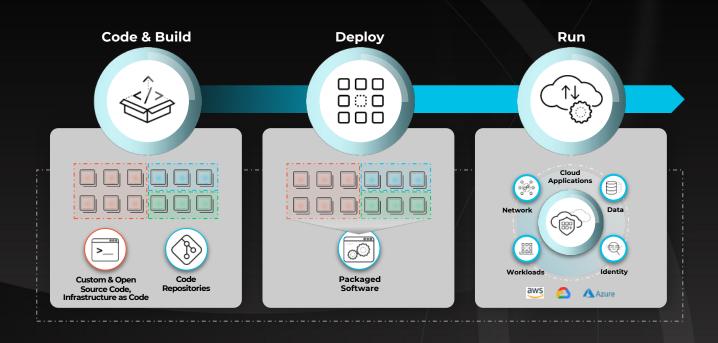


#### **HOW MANY POINT SOLUTIONS TO SECURE ONE APP?**

DATA			CLOUD DATA INVENTORY CLOUD DLP CLOUD DATA SECURITY POSTURE MANAGEMENT
CI/CD PIPELINE	WEB		WAF RASP BOT RISK MGMT. DDOS DEFENSE PAGE PROTECTION WEB CLIENT REPUTATION ACCOUNT TAKEOVER
	APIs		API PROTECTION API SECURITY TESTING API GATEWAY OPENAPI SCANNING
	MICROSERVICES		MICROSEGMENTATION
	SECRETS		SECRETS SCANNING CLOUD NATIVE SECRETS MANAGEMENT
	3RD PARTY CODE		SOFTWARE COMPOSITION ANALYSIS (SCA) SOFTWARE BILL OF MATERIALS (SBOM)
	CUSTOM CODE		DYNAMIC AST (DAST) STATIC AST (SAST) INTERACTIVE AST (IAST) APPSEC ORCHESTRATION (ASOC)
WORKLOADS			WORKLOAD CONFIG SCANNING HOST SECURITY CONTAINER SECURITY SERVERLESS SECURITY AGENTLESS SCANNING RUNTIME DEFENSE
ORCHESTRATORS		NFR.	K8S SECURITY POSTURE MGMT
CLOUD NETWORK AS		A AS	CLOUD NATIVE FIREWALL CLOUD IDS / IPS CLOUD INCIDENT RESPONSE
IAM	CLOUD SERVICES	CODE	CLOUD IDENTITY ENTITLEMENT MGMT. CLOUD ACCOUNT UEBA
PUBLIC CLOUD INFRA		Ш	CLOUD SECURITY POSTURE MGMT. INFRA-AS-CODE SECURITY

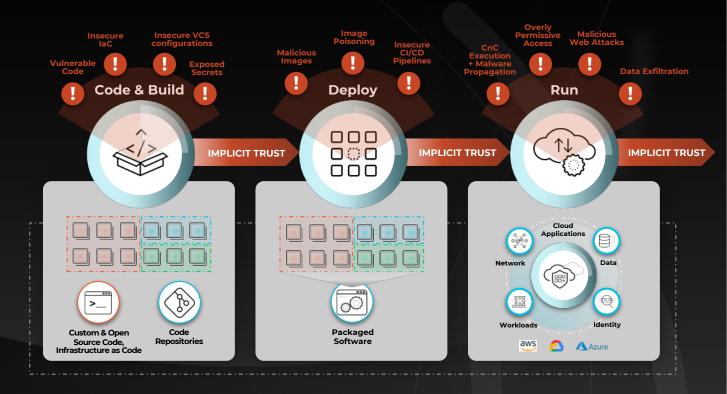
#### MAKING SENSE OF APPLICATIONS DEVELOPMENT

- Designed for rapid iteration and continuous application rollouts
- Highly automated builds to reduce time to market
- Improves app team / developer productivity



#### **ZERO TRUST WITHIN APPLICATIONS DEVELOPMENT**

The cloud application lifecycle is full of implicitly trusted components that if left unverified lead to major vulnerabilities down the line



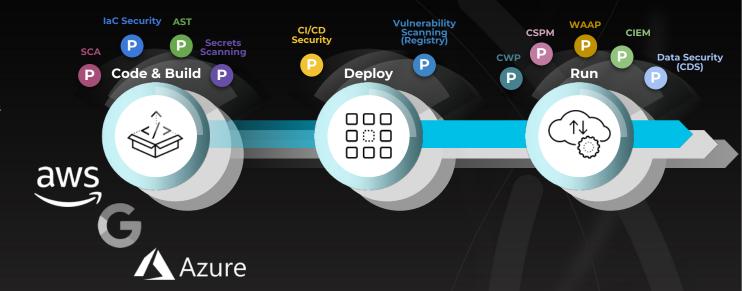
#### **HOW MANY POINT PRODUCTS DOES IT TAKE TO SECURE AN APP?**

It's typical for security teams to acquire, learn and manage over ten point product security tools from different vendors.



#### **MULTIPLE POINT PRODUCTS FOR MULTIPLE CLOUDS**

Using security services across the different cloud providers further complicates security and compliance through inconsistent capabilities, policies, and reporting.





#### THE ROLE OF THE SOC IN A ZERO TRUST FRAMEWORK

- Collects telemetry from all security tools
- Automates the fine-tuning or correction into the tools
- Re-assesses the decision making with wider context



## Our best of breed platforms enable cyber security transformation



#### **Network Security**

STRATA | PRISMA SASE

Best-in-class security delivered across hardware, software and SASE



#### **Cloud Security**

**PRISMA CLOUD** 

Comprehensive platform to secure everything that runs in the cloud



#### **Security Operations**

**CORTEX** 

A new approach to SOC with fully integrated data, analytics and automation



#### Threat Intelligence and Advisory Services

World-renowned threat intelligence, cyber risk management and advisory services

### THANKYOU