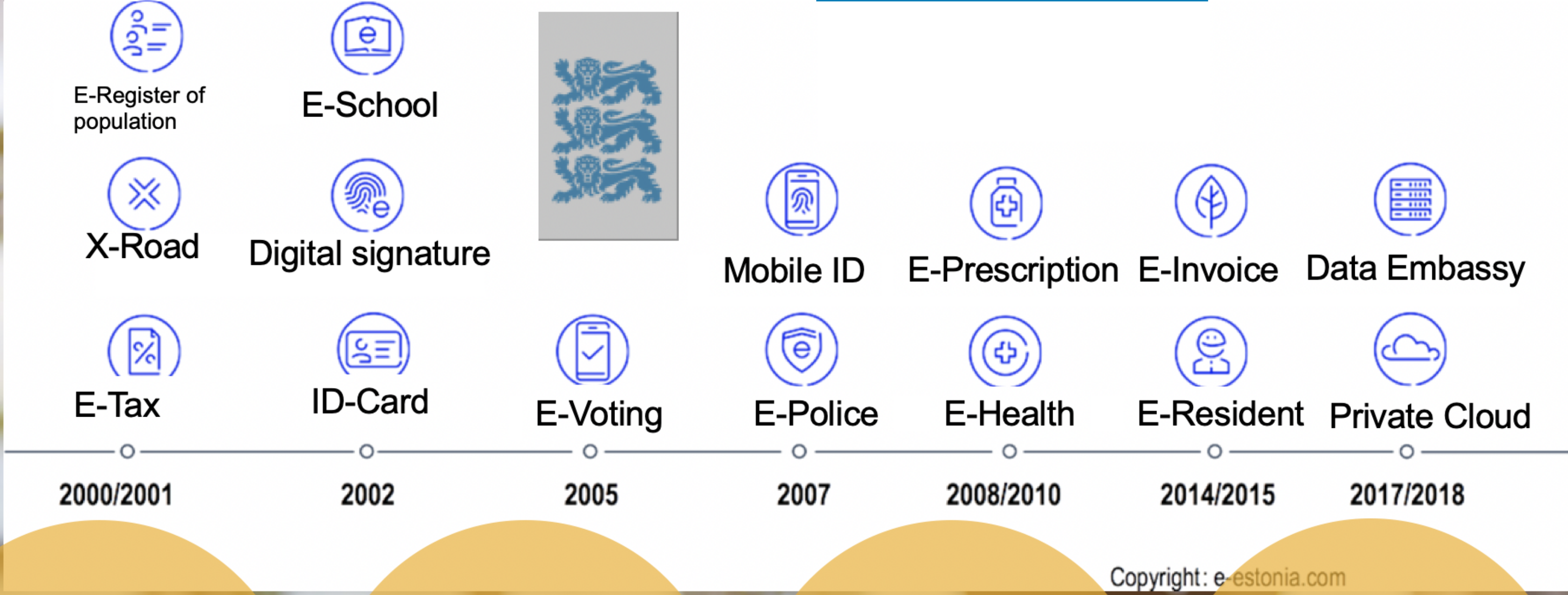
Estonian Government Cloud – way to tackle challenges

Sergei Butenko
Head of Modern Data Center division,
NEE region

Board member
Estonian Government Cloud

[redacted]



2000/2001: E-Register of population, X-Road, E-Tax

2002: E-School, Digital signature, ID-Card

2005: E-Voting

2007: Mobile ID, E-Police

2008/2010: E-Prescription, E-Health

2014/2015: E-Invoice, E-Resident

2017/2018: Data Embassy, Private Cloud

Copyright: e-estonia.com

99%

Faster VM provisioning
Vs standard Public RFP
(Municipal elections 2017)

24%

Cost savings in Capex
(Ministry of Environment '18)

61%

Reduction in 3Y Opex
(Center of Registers)

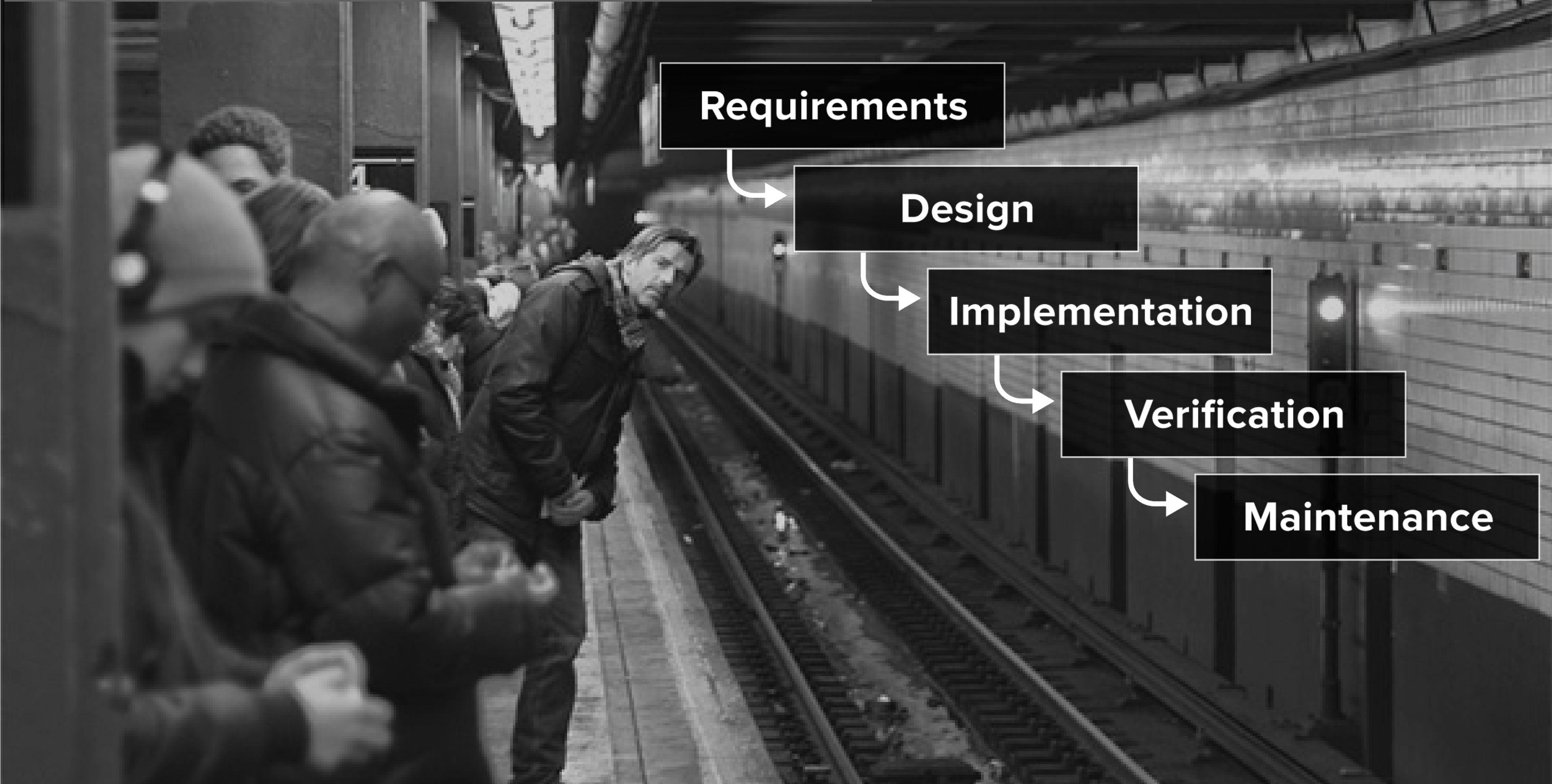
99,9999999%

Nine 9's Uptime
Vs traditional five 9's
(RIA survey & audit '18)

75% of digital business applications
will be **built** not bought by 2020

–Gartner, August 2015

From idea to production: 6-9 months



Requirements

Design

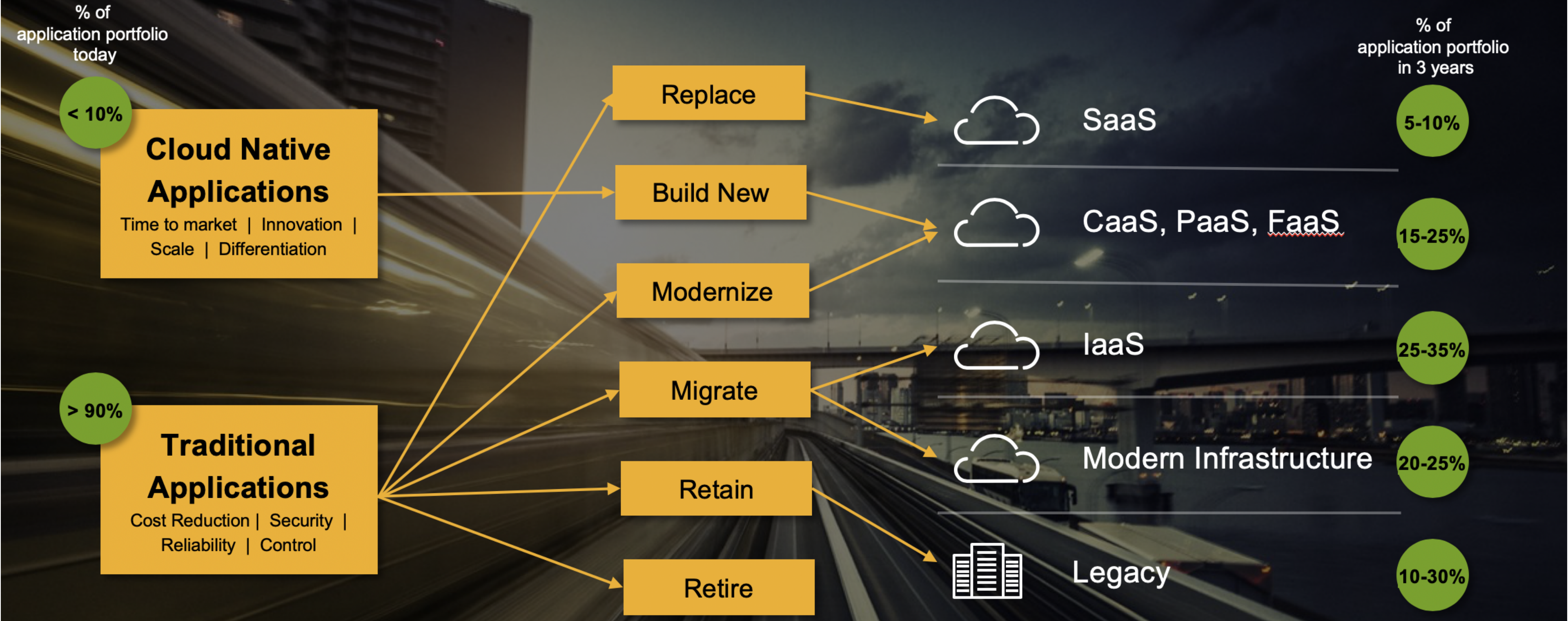
Implementation

Verification

Maintenance

Modernize Your Existing Application Portfolio

Dell Technologies Services helps you to assess, replatform, or refactor existing apps



% of application portfolio today

< 10%

Cloud Native Applications

Time to market | Innovation | Scale | Differentiation

> 90%

Traditional Applications

Cost Reduction | Security | Reliability | Control

- Replace
- Build New
- Modernize
- Migrate
- Retain
- Retire

% of application portfolio in 3 years

SaaS	5-10%
CaaS, PaaS, FaaS	15-25%
IaaS	25-35%
Modern Infrastructure	20-25%
Legacy	10-30%

Source: *Dell Technologies client analysis*

Pivotal Labs

DELL Technologies

Minimize Application Risk

Before and After

Traditional approaches to application risk aren't working

88% Growth in application vulnerabilities

197 Average number of days to identify a data breach

30+ Vulnerabilities in top Docker images

Rethinking risk to achieve **both speed and safety**

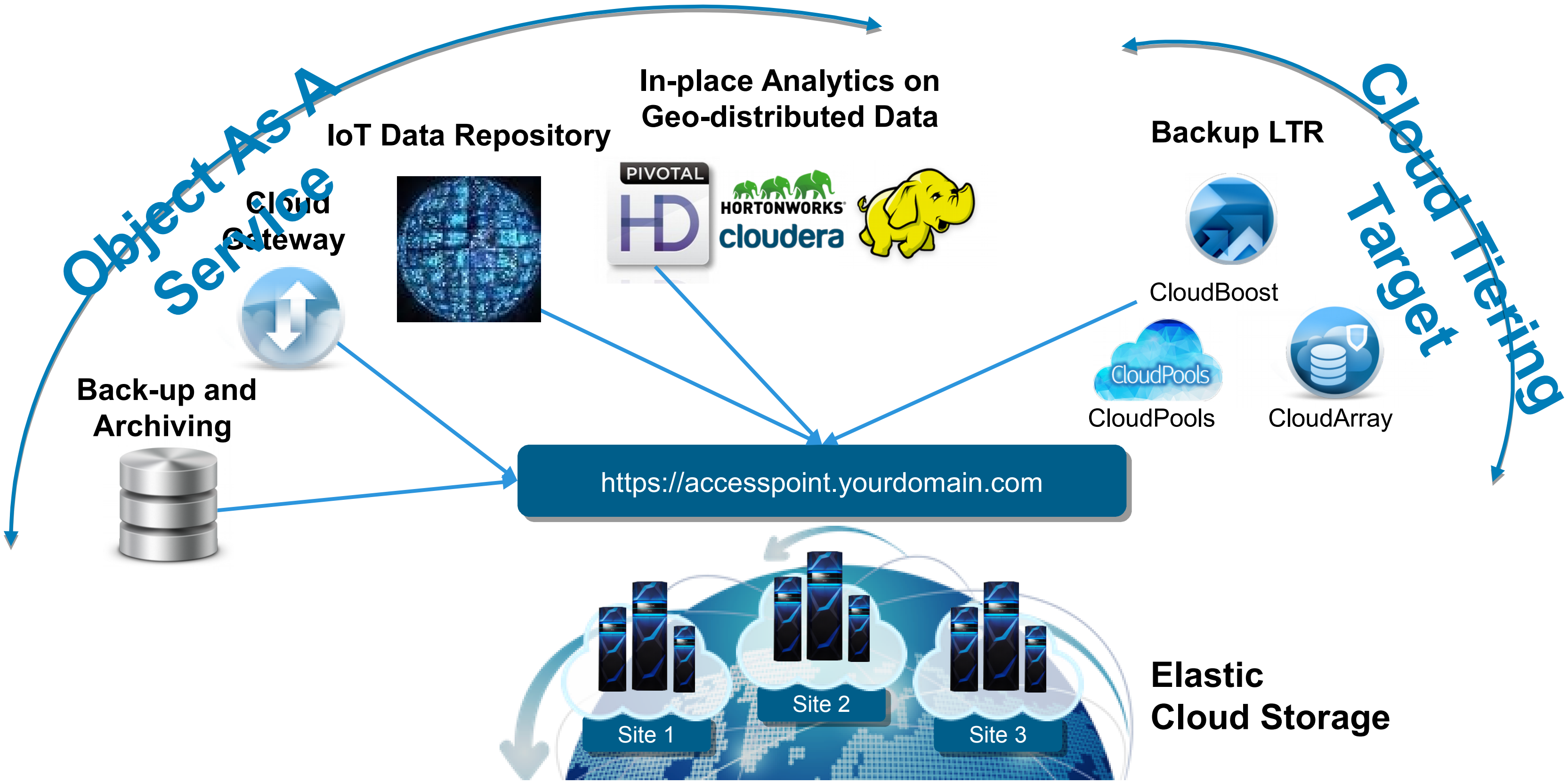
814K USD each data breach cost

50% are unprotected in the cloud

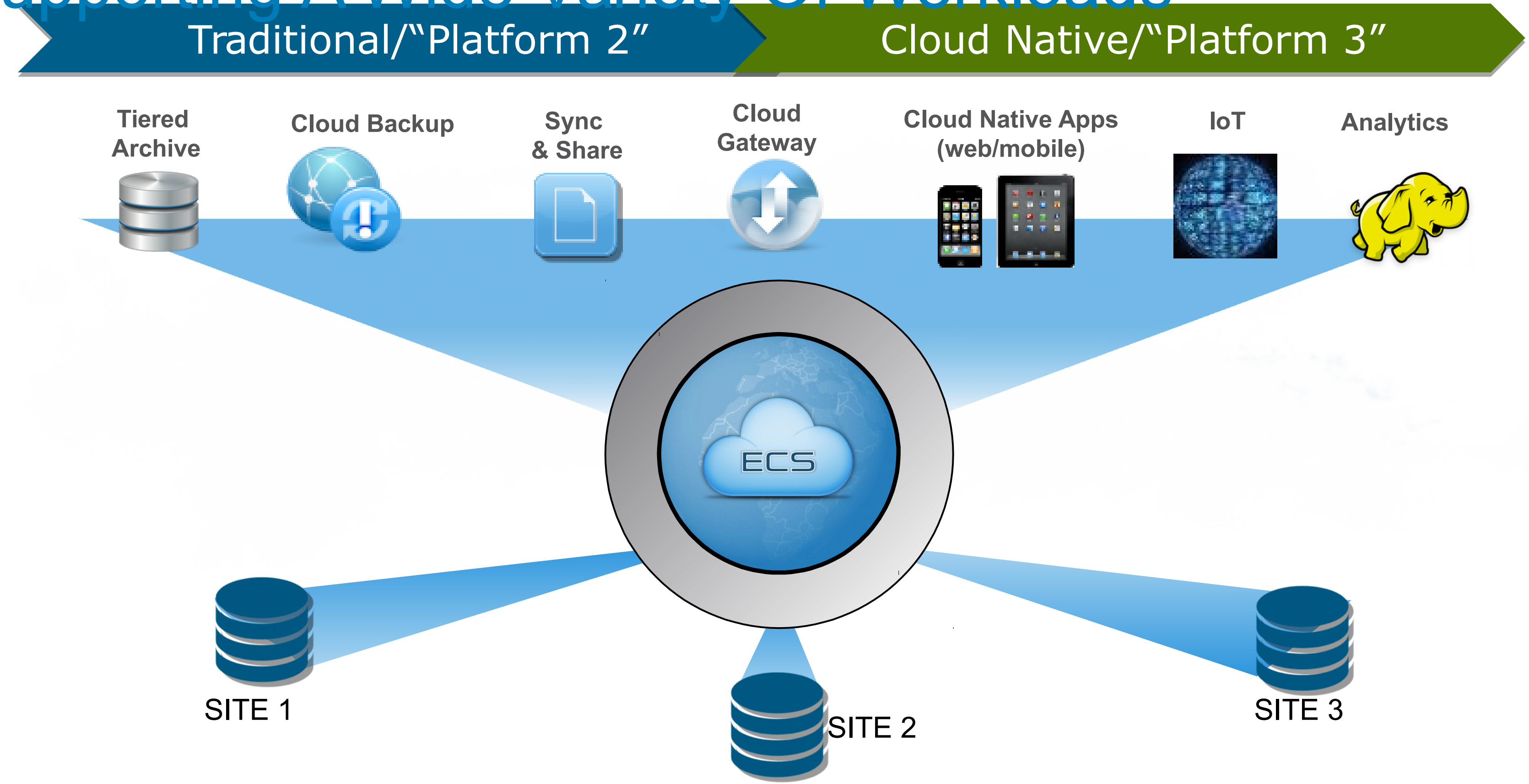
82% of responders not prepared to address future business challenges

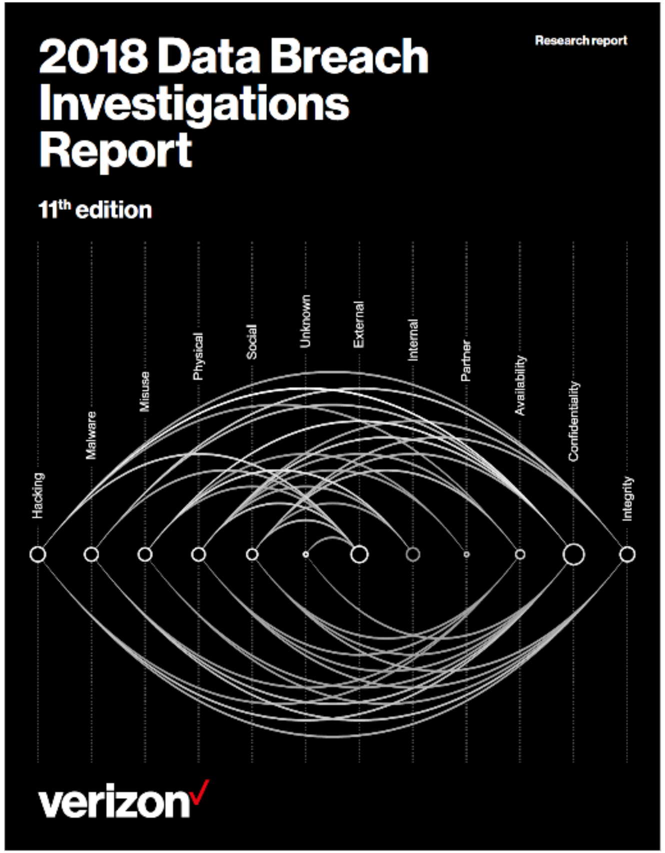
2.36T is average data loss

Data Embassy



Supporting A Wide Variety Of Workloads



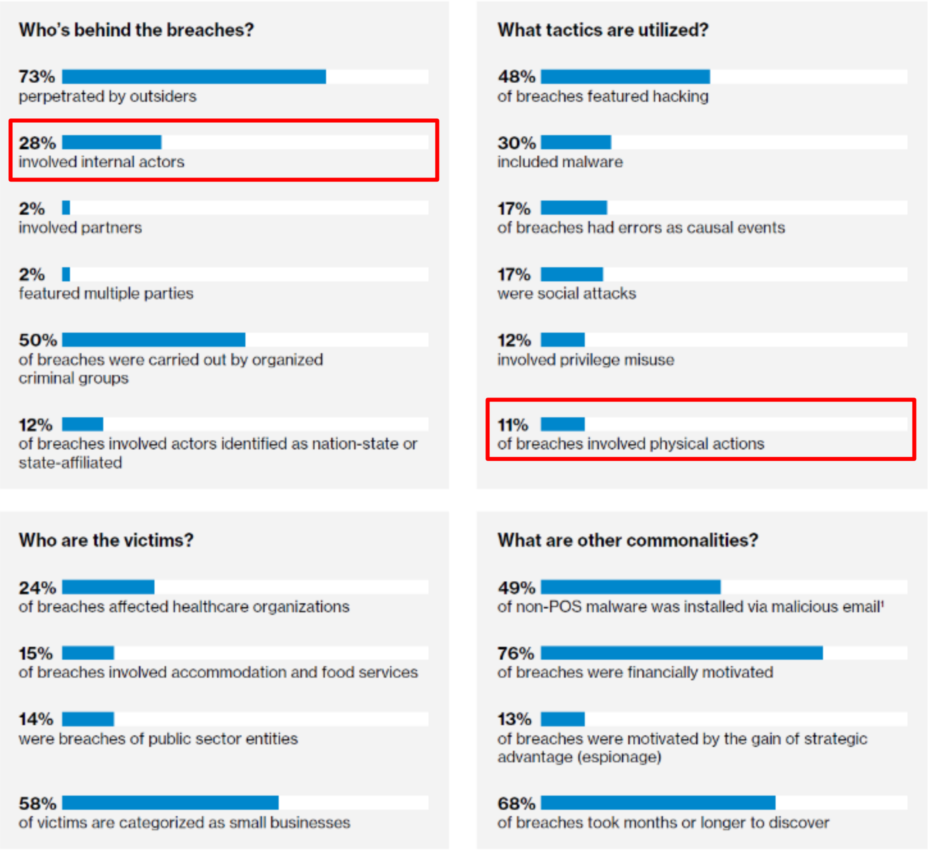


Research report

2018 Data Breach Investigations Report

11th edition

verizon✓



Who's behind the breaches?

73% perpetrated by outsiders

28% involved internal actors

2% involved partners

2% featured multiple parties

50% of breaches were carried out by organized criminal groups

12% of breaches involved actors identified as nation-state or state-affiliated

What tactics are utilized?

48% of breaches featured hacking

30% included malware

17% of breaches had errors as causal events

17% were social attacks

12% involved privilege misuse

11% of breaches involved physical actions

Who are the victims?

24% of breaches affected healthcare organizations

15% of breaches involved accommodation and food services

14% were breaches of public sector entities

58% of victims are categorized as small businesses

What are other commonalities?

49% of non-POS malware was installed via malicious email[1]

76% of breaches were financially motivated

13% of breaches were motivated by the gain of strategic advantage (espionage)

68% of breaches took months or longer to discover

Adversaries Exploiting Your Blind Spots

Adversaries are bypassing anti-malware and traditional security controls, allowing them to go **undetected for months or** sometimes even **years**.

Organizations often not prepared to respond and face prolonged data recovery times.

Breach & Dwell Time

170 Days Average

Challenges:

- Disappearing perimeter ▭ Lack of Visibility
- Cloud, Mobile, IOT ▭ More points of exposure
- Skills Shortage ▭ spread to thin, too much information

Requirements:

- Adaptive framework ▭ responds to evolving threat landscape
- Tools, knowledge, and expertise reduce breaches and dwell time

Incident & Response

28 Days Average

Challenges:

- No clear understanding of business impact
- Often delayed due to lengthy data recovery

Requirements:

- Framework for prioritized recovery of business processes
- Integrated incident response and

Role of Cyber Recovery Solution

Source: SecureWorks Targeted Threat Response Engagements

VxRail simplifies lifecycle management

Sustained and delivered as a single [illegible] testing, sequencing, and validating

		Jan	Feb	Mar	Apr	May	Jun	Jul	Aug
		● Maintenance	● Critical	● Critical	● Maintenance		● Critical		
Software	Integrated Software	4			3		6		
	SDS						3		
	Hypervisor	1		1	1		1		
	Software governance	3		2	4		2		
	Virtualization Management		1						
Hardware	BIOS				2				
	Components Firmware & Drivers	2					4		
	NIC Firmware		2				5		

● Critical Releases ● Maintenance Releases

GO FROM ONE GOOD KNOWN STATE TO THE NEXT

** Example only, not reflective of actual VxRail software packages*

Secure, Protect, Archive and Recover Your Apps – Wherever They Run

Secure APIs

DELL Boomi

Minimize Vulnerability Windows

Pivotal

Secureworks

RSA

Detect & Respond

DELL EMC

vmware

Protect & Recover