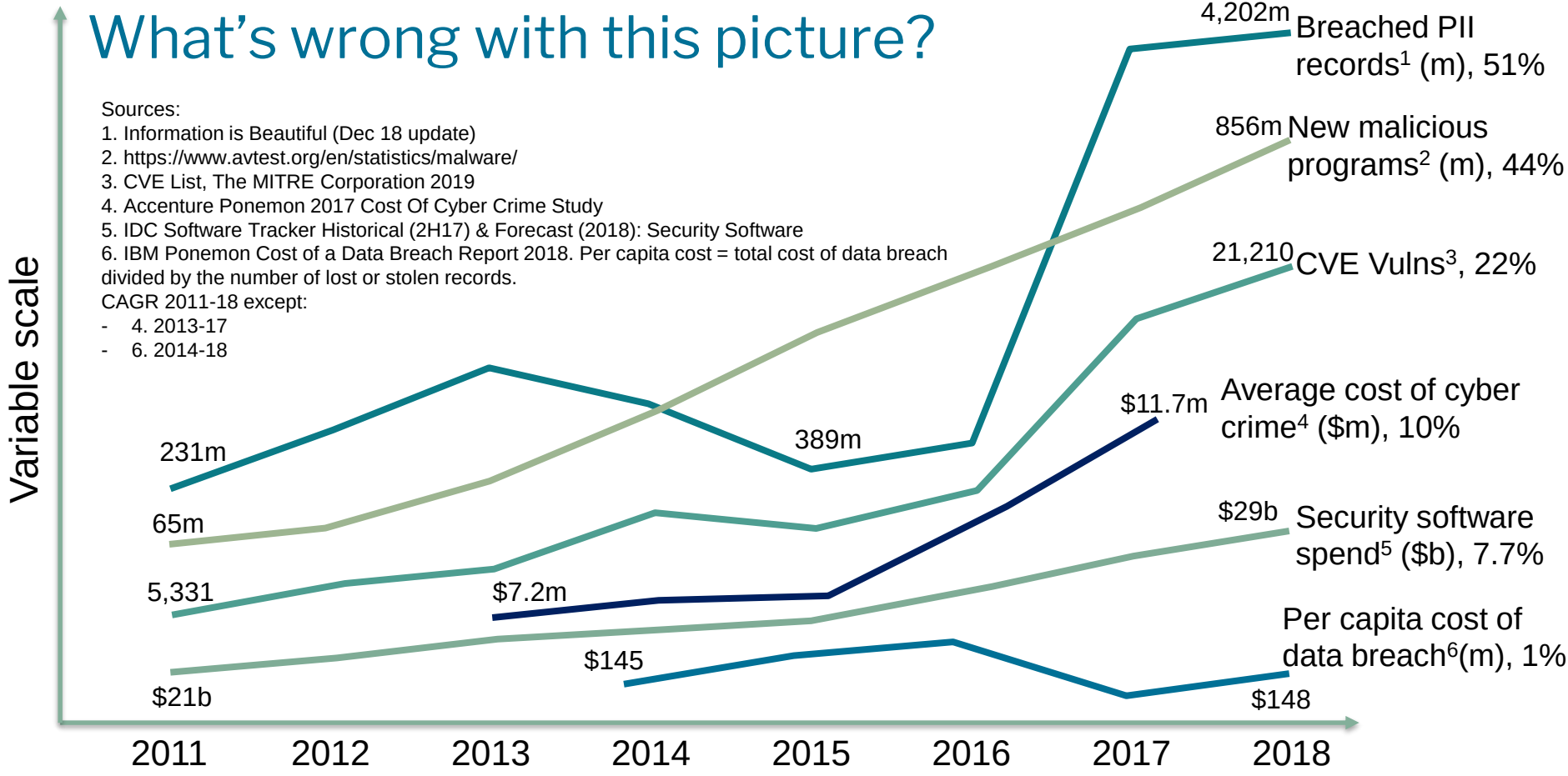
Human-Centric Security For The Era Of Digital Transformation

Duncan Brown
EMEA Chief Security Strategist

FORCEPOINT

Data Protection | Web Security | CASB | NGFW | Advanced Malware Detection | Behavioral Analytics | Insider Threat | Email Security | Data Guard | Cross Domain

What's wrong with this picture?



Sources:
1. Information is Beautiful (Dec 18 update)
2. https://www.avtest.org/en/statistics/malware/
3. CVE List, The MITRE Corporation 2019
4. Accenture Ponemon 2017 Cost Of Cyber Crime Study
5. IDC Software Tracker Historical (2H17) & Forecast (2018): Security Software
6. IBM Ponemon Cost of a Data Breach Report 2018. Per capita cost = total cost of data breach divided by the number of lost or stolen records.

CAGR 2011-18 except:
- 4. 2013-17
- 6. 2014-18

$1 Trillion has been spent over the past 7 years on Cybersecurity, and yet…

46% say they can't prevent attackers from breaking into internal networks each time it is attempted.

Source: CyberArk Global Advanced Threat Landscape Report 2018

100% of CIOs believe a breach will occur through a successful phishing attack in next 12 months.

Enterprises have seen a 26% increase in security incidents despite increasing budgets by 9% YoY.

Sources: Verizon 2018 Data Breach Investigations Report.

Digital Transformation Will Unlock Tremendous Value… If Cybersecurity Challenges Can Be Addressed

$100 trillion

The value that the World Economic Forum estimates will be created from digitalization over the next 10 years.

Source: Digital Transformation Initiative, World Economic Forum, May 2018.

"What are the greatest challenges in digital transformation?"

Security	**31%**
Technology strategy	24%
Company culture	23%
Lack of technology skills	20%

Source: Forrester: The Sorry State Of Digital Transformation in 2018.

Four Elements Of Digital Transformation That Create Advantage And Risk

box workday. salesforce Office 365

"Your IT infrastructure is going to the cloud, driven by business need and speed."

- Cloud IT creates security blind spots and fragmented security management and accountability.

"Data is the new oil and artificial intelligence the new engine of the digital economy."

- More critical data is being created than properly protected.
- Data should flow freely across the business.

"Workforce, devices, and business processes are globally hyperconnected."

- Network transformation to support cloud-centric IT breaks existing security architectures.
- Personal and IoT devices are security vulnerabilities.

"Employees and partners collaborate using all of a company's assets."

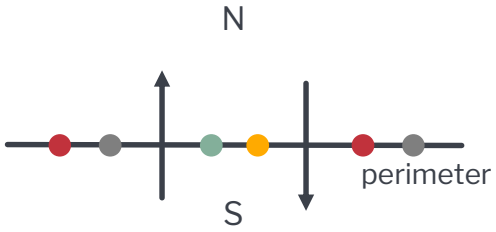
- A critical need is created to ensure trusted interactions across the extended enterprise.

What is the best way to reduce risk and secure an environment you increasingly don't own or fully manage?

Humans and Data

Users And Data Must Be At The Center Of Your Design Thinking

User and data interactions are distributed, diverse and dynamic – this breaks traditional security architectures and increases business risk



Network-Centric

User & Data Centric

Pre-2000 → Infrastructure-centric → **2010** → Behavioral-centric → **2020**

Users And Data Must Be At The Center Of Your Design Thinking

User and data interactions are distributed, diverse and dynamic – this breaks traditional security architectures and increases business risk

Traditional Security

One-to-many enforcement of static, generic policies, producing high false positive rates.

User & Data Centric

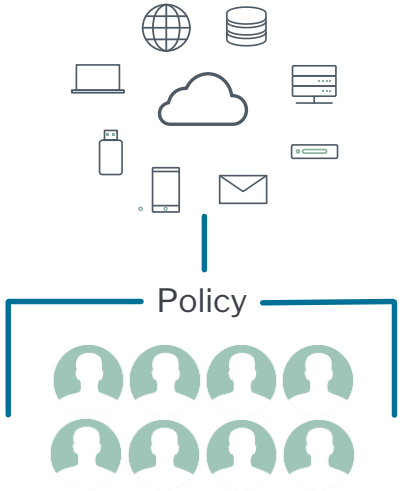
Degree of Digital Transformation

IT Complexity & Risk

Pre-2000 → Infrastructure-centric → 2010 → Behavioral-centric → 2020

Human-Centric Cybersecurity Changes Everything

Traditional Security



One-to-many enforcement of static, generic policies, producing high false positive rates.

Human-Centric Security

One-to-one enforcement of different policies based on the risk, enabling automation.

Risk-Adaptive In Action

Senior sales rep,
Copenhagen, DK

Monday
January 21 @ 10am

Working while on PTO

+ Additional Context

Risk Score: 30

Risk-Adaptive Protection

No enforcement action

Thursday
January 24 @ 1pm

Downloads customer records to Excel

+ Additional Context

Risk Score: 50

Risk-Adaptive Protection

Enhanced auditing activated

Evidence available for investigation later

Wednesday
January 30 @ 9pm

Copy multiple files to staging area

+ Additional Context

Risk Score: 80

Risk-Adaptive Protection

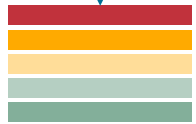
Copy allowed but file encrypted

No corporate data at risk

Saturday
February 9 @ 6am

Bulk copy to USB drive

+ Additional Context



Risk Score: 95

Risk-Adaptive Protection

Action is blocked & account is locked

Avoided $10M breach and forensic proof of the attack is available

Do privacy concerns outweigh security objectives?

You’re tracking my what???!!!

Processing personal data for security is a legitimate interest

“The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security … constitutes a legitimate interest of the data controller concerned.”

GDPR Recital 49

We already “monitor” our users

- Logins & Failed login attempts
- Application access
- Presence (Skype, WhatsApp, Chatter, Slack, etc)
- Cloud apps (sanction, blocked, tolerated, etc)
- Web filtering
- White- and black-listing
- Endpoint process monitoring
- Phishing awareness campaigns
- Physical card swipes for office access

We often don’t…

- Join these dots to create an overall risk profile for each user
- Have a framework for transparency that protects our users, customers and partners

https://www.forcepoint.com/blog/insights/behaviour-analysis-privacy-preserving-technology

OUR BLOG

Behaviour analysis is a privacy-preserving technology

TUESDAY, MAY 07, 2019

Duncan Brown

The positioning of privacy versus security with behavioural analysis is a false dichotomy, based on several misconceptions. You ought to be able to have both security and privacy. Indeed, behavioural analysis can enhance privacy, rather than threaten it. Here's why.

Gartner's Continuous Adaptive Risk and Trust Assessment (CARTA)

"We need security infrastructure and security decisions to become continuous and adaptive – enabling real-time decisions that balance risk, trust and opportunity and the speed of digital business."

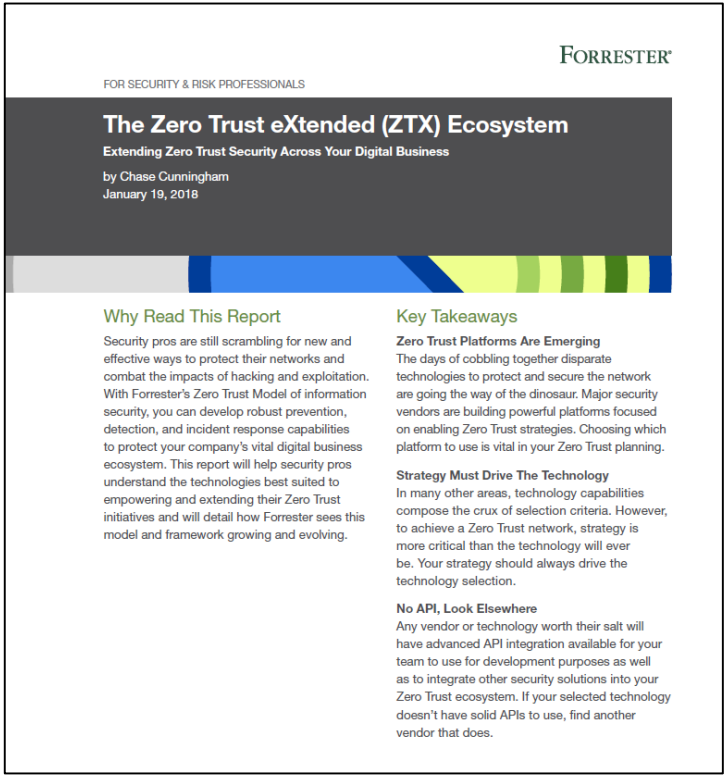
"We must have visibility into what the entity – the user – is doing once it gains access. How is it behaving? Does the entity or its behaviors represent excessive risk? If so, then we should have the ability to detect this, confirm that it is real, prioritize it and take action."

Neil MacDonald, Gartner Research Note G00351017, April 10th 2018

Forcepoint is a Zero Trust platform notable vendor

“The last line of any Zero Trust strategy is limiting and strictly enforcing the access of users and securing those users as they interact with the internet. This encompasses all the technologies necessary for authenticating users and continuously monitoring and governing their access and privileges.”

Chase Cunningham
The Zero Trust eXtended (ZTX) Ecosystem
Extending Zero Trust Security Across Your Digital Business
January 19, 2018



FORRESTER®

FOR SECURITY & RISK PROFESSIONALS

The Zero Trust eXtended (ZTX) Ecosystem

Extending Zero Trust Security Across Your Digital Business

by Chase Cunningham
January 19, 2018

Why Read This Report

Security pros are still scrambling for new and effective ways to protect their networks and combat the impacts of hacking and exploitation. With Forrester's Zero Trust Model of information security, you can develop robust prevention, detection, and incident response capabilities to protect your company's vital digital business ecosystem. This report will help security pros understand the technologies best suited to empowering and extending their Zero Trust initiatives and will detail how Forrester sees this model and framework growing and evolving.

Key Takeaways

Zero Trust Platforms Are Emerging
The days of cobbling together disparate technologies to protect and secure the network are going the way of the dinosaur. Major security vendors are building powerful platforms focused on enabling Zero Trust strategies. Choosing which platform to use is vital in your Zero Trust planning.

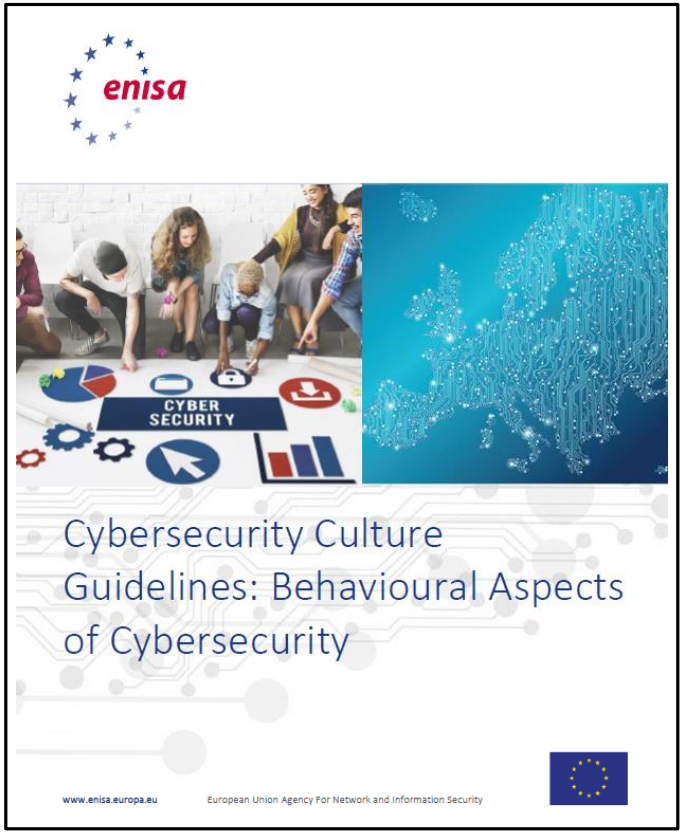
Strategy Must Drive The Technology
In many other areas, technology capabilities compose the crux of selection criteria. However, to achieve a Zero Trust network, strategy is more critical than the technology will ever be. Your strategy should always drive the technology selection.

No API, Look Elsewhere
Any vendor or technology worth their salt will have advanced API integration available for your team to use for development purposes as well as to integrate other security solutions into your Zero Trust ecosystem. If your selected technology doesn't have solid APIs to use, find another vendor that does.

Industry awareness is growing…

“It is evident that the industry must shift from the technology and process centric view to a human centric view and adopt the knowledge from behavioural theories to be successful in the digital age of cybersecurity.”

Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity
European Union Agency For Network and Information Security (ENISA)
Published April 16, 2019



Thank you

duncan.brown@forcepoint.com