# Cyber Security Investing 101

Vincenzo Iozzo

# Topics

1. Industry structure and growth trajectory
2. Funding and exits stats + players in the sector
3. InfoSec-specific DD questions
4. A few gotchas learned the wrong way
5. Historical and future “Why now” in InfoSec
6. A couple of examples
7. Open questions I’m trying to find answers to

# About

## How it started

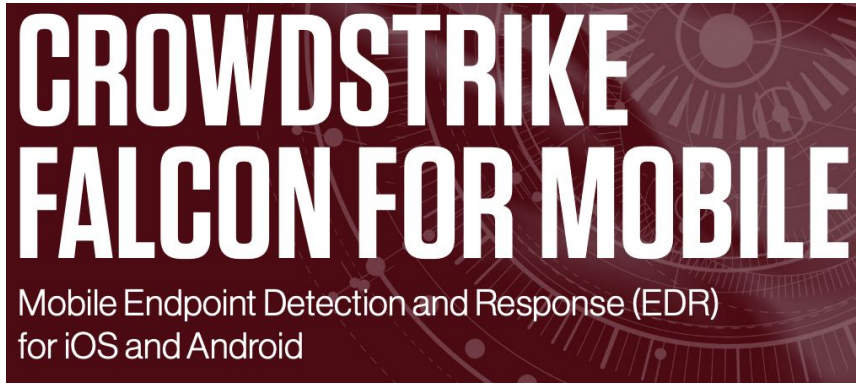
### iPhone Hacked at Pwn2Own; SMS Database Stolen

Using an exploit against a previously unknown vulnerability, the duo – Vincenzo Iozzo and Ralf Philipp Weinmann – lured the target iPhone to a rigged Web site and exfiltrated the SMS database in about 20 seconds.

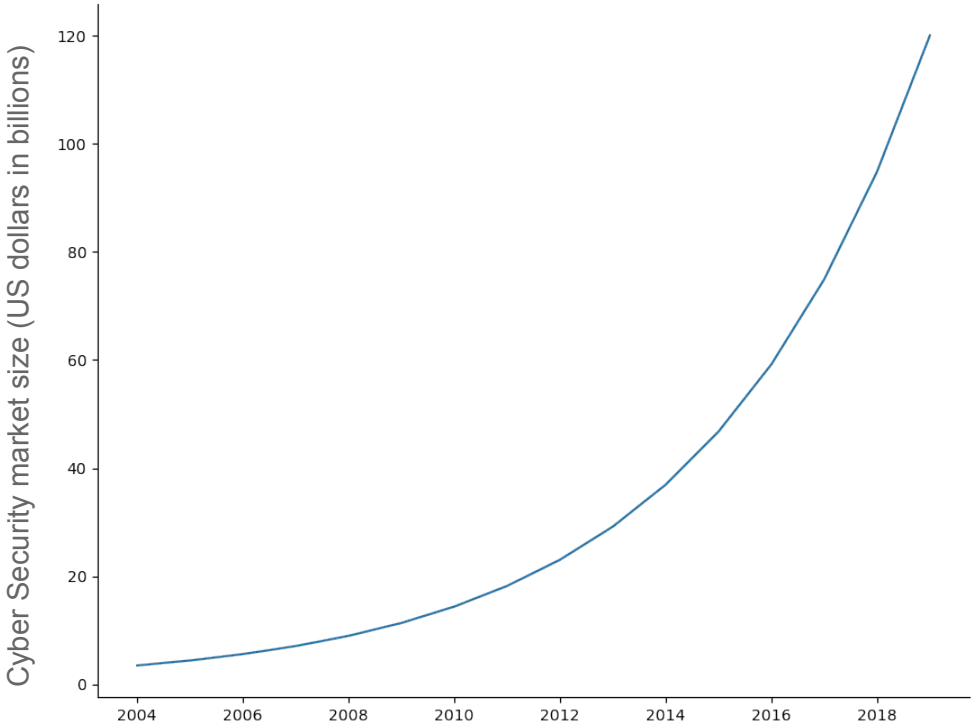
## How it's going

### CrowdStrike and Accel launch Falcon Fund

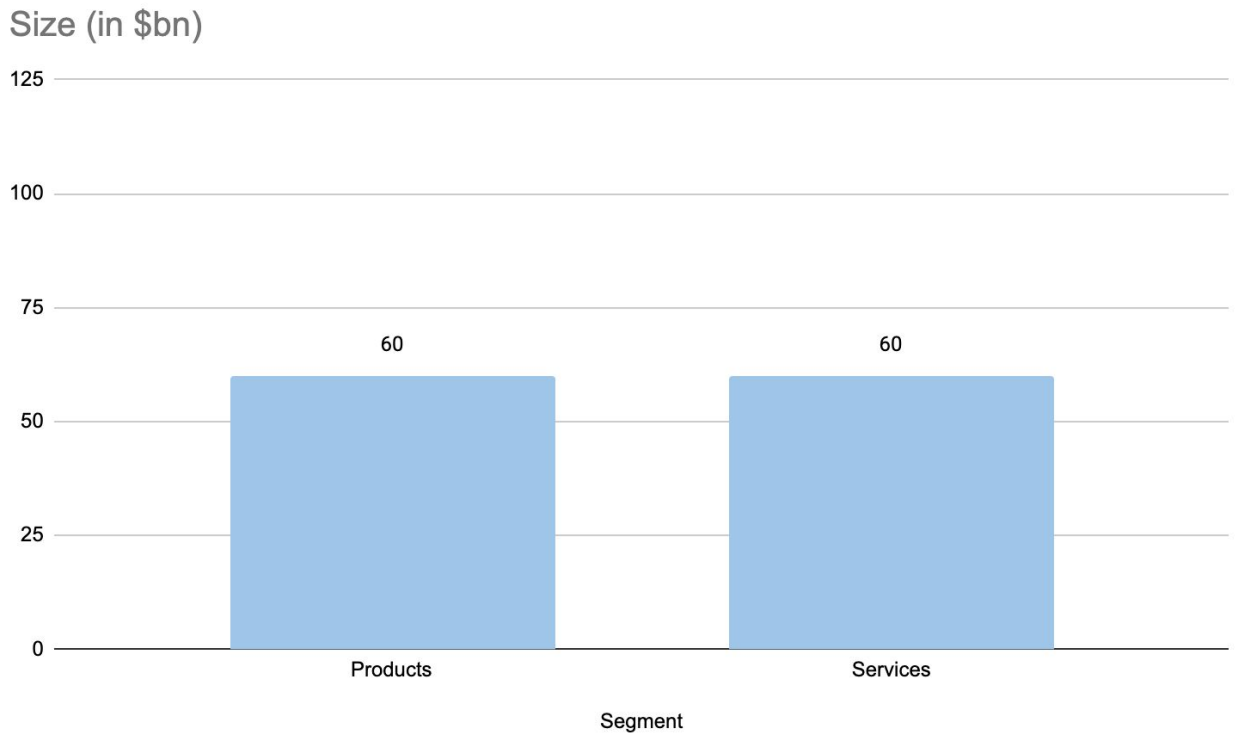
**CrowdStrike Completes Acquisition of Preempt Security**



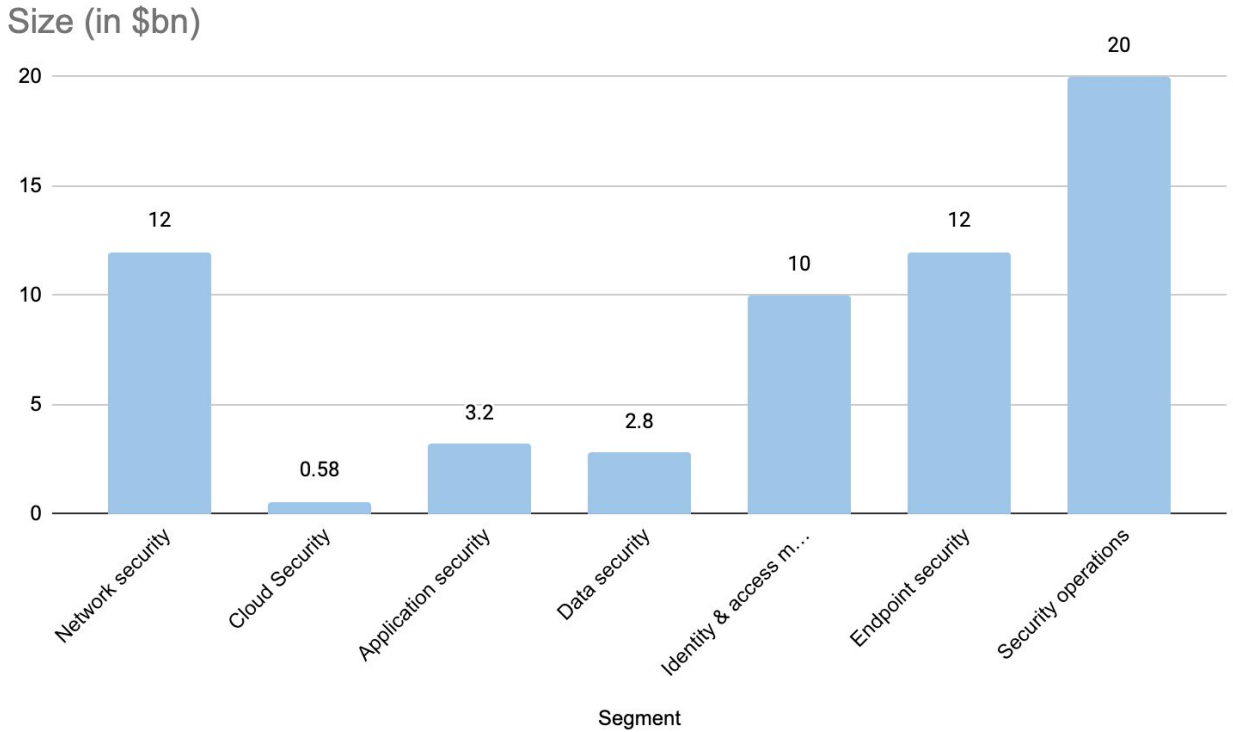
# Industry growth



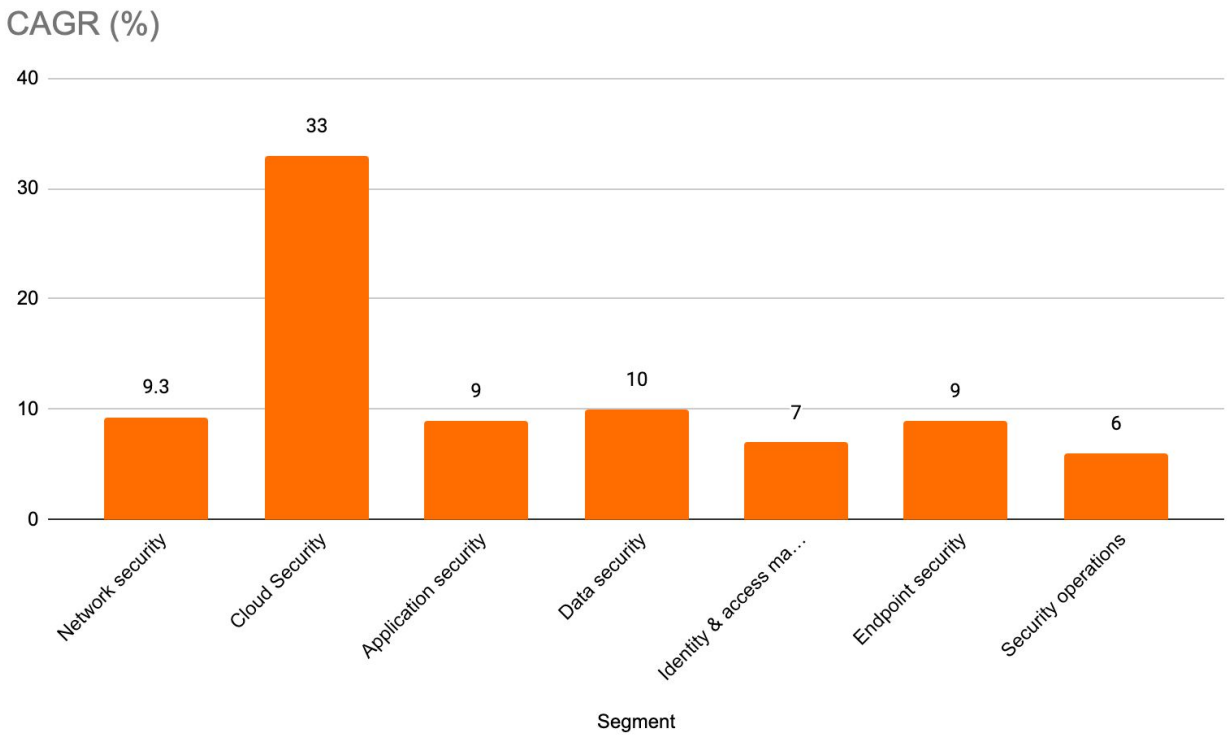
# The market today - A tale of two universes



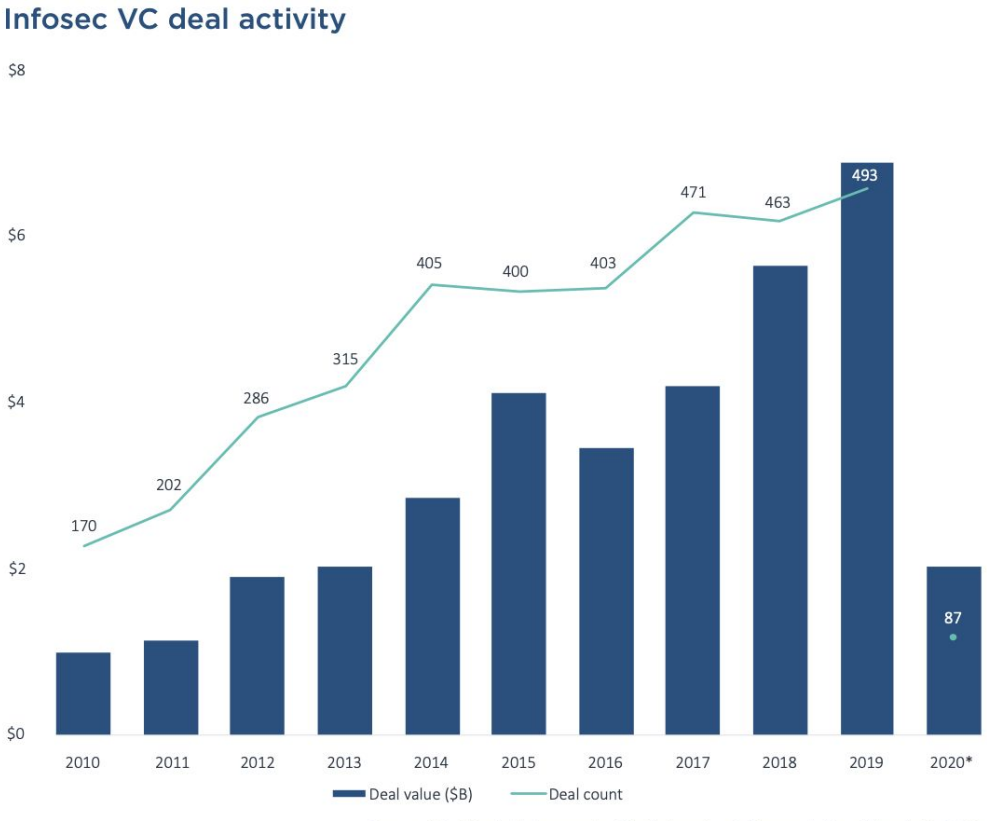
# Market Structure - Macro segments



# 3-Year growth

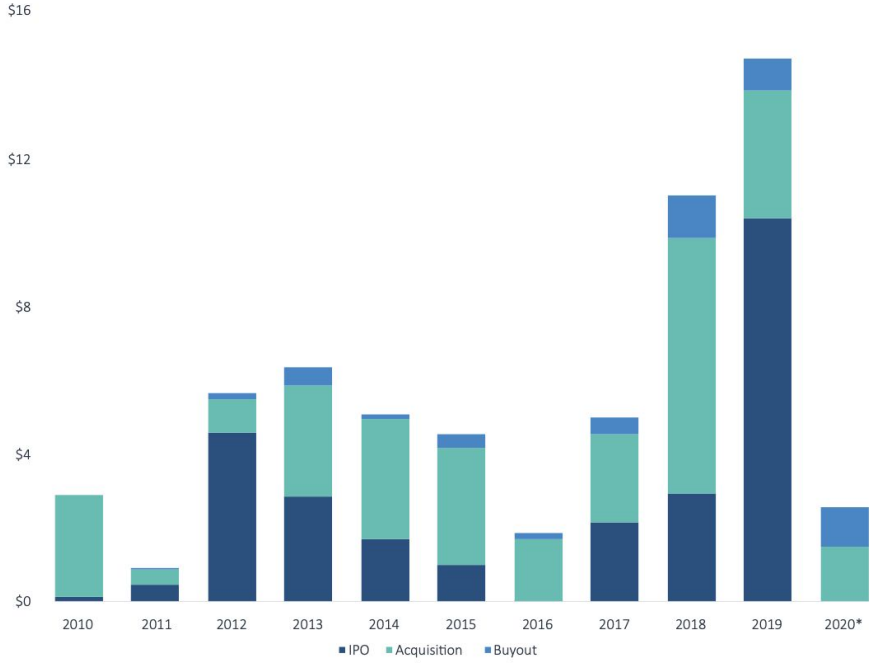


# Number of deals



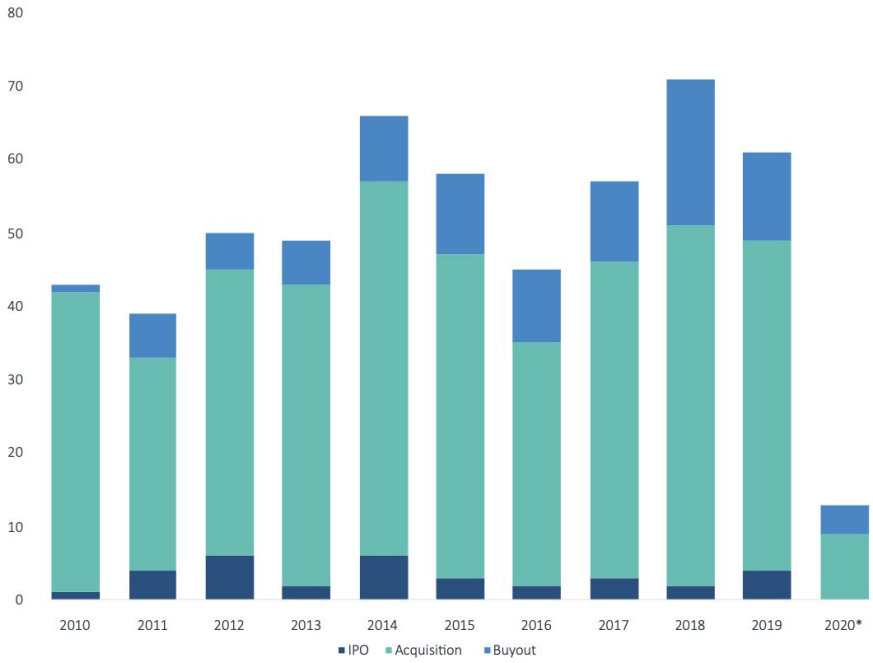
# Exits

## Infosec VC exits ($) by type




Source: PitchBook | Geography: North America & Europe | *As of March 31, 2020

## Infosec VC exits (#) by type




Source: PitchBook | Geography: North America & Europe | *As of March 31, 2020

# Players to know

## VC

- Accel
- NEA
- ClearSky
- Greylock
- Dell Technologies Capital
- Bain Capital Ventures
- ForgePoint Capital
- Ten Eleven Ventures
- YL Ventures
- Battery Ventures
- Jerusalem Venture Partners
- Elron
- CapitalG
- Redpoint

## PE

- Thoma Bravo
- Insight Partners
- H.I.G. Capital
- TA Associates Management
- Marlin Equity Partners
- KKR

# Two types of blueprints in InfoSec

**Disrupting product incumbents via a platform/threat shift**

CrowdStrike
Palo Alto Networks
Okta

**Budget shift from Services to Products***

Demisto
OneTrust
Splunk (partially)

*This comes with quite a bit of risk in terms of market adoption, revenue quality, gross margins and exit scenarios

# Three types of products in Product InfoSec

| **Protect*** | **Manage** | **Automate** |
| --- | --- | --- |
| CrowdStrike | Okta | Demisto |
| Palo Alto Networks | Sumo Logic | Expel |
| Zscaler | Anchorage | Coalition |
| Duo | CyberArk | Immersive Labs |

*Most of these are one or more pieces of the “Observe, Detect, Prevent, Remediate” formula

# InfoSec-Specific investment criteria/questions

- Does this company fit one of the traditional product models? If not, why?
- What is the threat the company is protecting against? What is the right abstraction layer for this threat?
- How is the company going to win a bake-off against the incumbents? Is it measurable?
- Do customers have a budget for this?
- How difficult is it to deploy the solution? Is it interfering with performance or any IT/Eng requirements?
- Do founders have a background/connections in InfoSec or enterprise software? NSA/Unit 8200 is not enough

# Lessons learned

- Platform & threat shifts kill companies more than competition does
- Engineering talent matters more than Security talent in InfoSec companies
- Most InfoSec companies are features vs standalone businesses, 85% of the exits are below $300m
- If Thoma Bravo is in the space, it likely means that there's a sector transition in progress
- Governments are generally not a great first customer
- Adoption of the canonical tech stack is an insurance policy (increases odds of early acquisition)
- Gartner&co influence large companies decisions more than you'd imagine
- **Often startups in the space attack a problem at the wrong level of abstraction just to differentiate themselves vs the market**

# The “Why Now” of InfoSec - Platform shifts & politics

Web-based apps (move from Layer 3 to 7) → Palo Alto Networks

Nation state-backed attacks, move to the cloud → CrowdStrike

Cloud-based Enterprise Apps → Okta, Zscaler, NetSkope

OSS and DevOps → Snyk

Regulation (GDPR, CCPA) → OneTrust

# The “Why Not Anymore”

Code signing and App Store distribution model → Much less malware on iOS

Certificate pinning → Deep packet inspection no longer possible

Microservices & “Cloud OSes” → Firewalls become code

“Malware-less” attacks → EDR replaces traditional AV

# An example of Services->Product: Immersive Labs

**History**: Started in mid-2017. First round end of 2017, Series B in 2019. 8-figure revenue today

**Why Now**: Flood of new people in InfoSec who need to be skilled-up continuously

**Business model**: Traditional training is an unscalable services business. Productize the whole process, make it continuous

**Founder background**: Long-time InfoSec Instructor

IMMERSIVELABS

# An example of product disruption: Snyk

**History**: Started in 2015. First round end of 2015, Series D in 2020. 8/9-figure revenue today

**Why Now**: OSS and Cloud are taking over AppSec

**Business model**: Traditional AppSec tools are not built for an OSS-first world, offer a freemium model bottom-up (developers first)

**Founders background**: Long-time InfoSec practitioners. The CEO/Co-founder was the CTO of Akamai

snyk

# Ongoing shifts

DevOps and OSS → Increase shift of InfoSec to developers

More Cloud Computing → Who owns security here? How does IAM work in this world? Are traditional firewalls redundant?

Move to serverless/JAM/APIs → Data protection and endpoint protection shift

Way too many tools and companies → Opportunity to bundle security (SOAR, SIEM)?

# Open questions

How big will the shift from other security verticals to AppSec be?

What does a modern security platform/aggregator look like?

Where’s the line between Security vendors and Cloud/OS vendors in the long run?

How much of the Services TAM can be productized?