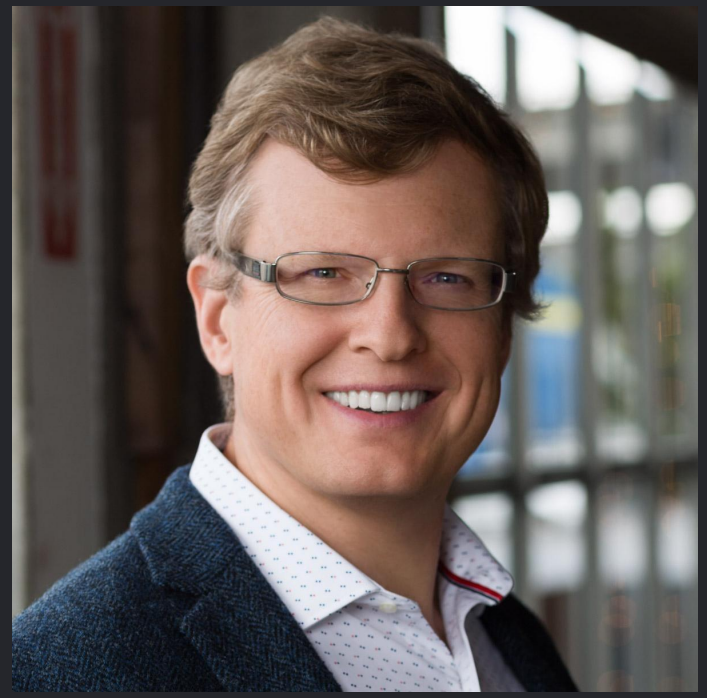
Who?



Dr. Anton Chuvakin

Security Solution Strategy
Chronicle / Google Cloud

@anton_chuvakin

https://medium.com/anton-on-security

Security: Sad History of Being a Bolt-on

- ➔ 1980: Internet without security
- ➔ 1990: Windows without security
- ➔ 2000: Mobile devices without security
- ➔ 2005: Cloud without security
- ➔ 2010: IoT without security
- ➔ 2015: ML/AI without security
- ➔ Don’t even get me started on blockchain :-)

Where Does Cloud Security Comes From?

1. **Cloud Provider** brings security tools (paid or free)
2. **Cloud customer** brings own **existing** security tools
3. **Cloud customer** purchases tools from 3rd party vendors **just for cloud**
4. Combination of the above

	Client
	CSP
	BOTH Client and CSP

PCI DSS Requirement	Example responsibility assignment for management of controls		
	IaaS	PaaS	SaaS
1: Install and maintain a firewall configuration to protect cardholder data	Both	Both	CSP
2: Do not use vendor-supplied defaults for system passwords and other security parameters	Both	Both	CSP
3: Protect stored cardholder data	Both	Both	CSP
4: Encrypt transmission of cardholder data across open, public networks	Client	Both	CSP
5: Use and regularly update anti-virus software or programs	Client	Both	CSP
6: Develop and maintain secure systems and applications	Both	Both	Both
7: Restrict access to cardholder data by business need to know	Both	Both	Both
8: Assign a unique ID to each person with computer access	Both	Both	Both
9: Restrict physical access to cardholder data	CSP	CSP	CSP
10: Track and monitor all access to network resources and cardholder data	Both	Both	CSP
11: Regularly test security systems and processes	Both	Both	CSP
12: Maintain a policy that addresses information security for all personnel	Both	Both	Both
PCI DSS Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers	CSP	CSP	CSP

Whose Fault Is It?

In fact, Gartner says...

“Through 2025, 99% of cloud security failures will be the [cloud] customer’s fault.”

What does it mean?

Question:

Is it fair to blame cloud customers for nearly all security problems?

Anton's Ideal Cloud Security Criteria

Default security	e.g. logging that just works and is always centrally collected and searchable
Opt-out security	e.g. tight permissions that loudly object to being loosened
Transparent security	e.g. encryption of data in transit and at rest
Native to the system	e.g. not sold separately and requiring integration work
Automated security	e.g. turned on after deployment via an API
Role-based security	e.g. specific roles must be granted for management and access (but without the headache!)
Obvious security	e.g. not require the failure-prone user education

Question:

Is change realistic or are we doomed to bring our pre-cloud security problems to the cloud?

Recommendations

- ➔ Migration to cloud infrastructure is a unique opportunity to dismantle the legacy security debt of the past two decades.
- ➔ Think how you can use cloud migration to actually do security from day one, not day +1 after the breach
- ➔ Push your cloud provider to make it easier to secure your assets.
- ➔ Finally, remember that joint responsibility model is forever; there will always be security tasks that a customer will own.

Further Reading

- “Move to Cloud: A Chance to Finally Transform Security?”
- “Google Security Model”
- “Psychoanalyzing Security Cloud Fears”
- “Top Threats to Cloud Computing: Deep Dive”