Demostack Privacy & Security

May 20, 2022

demostack

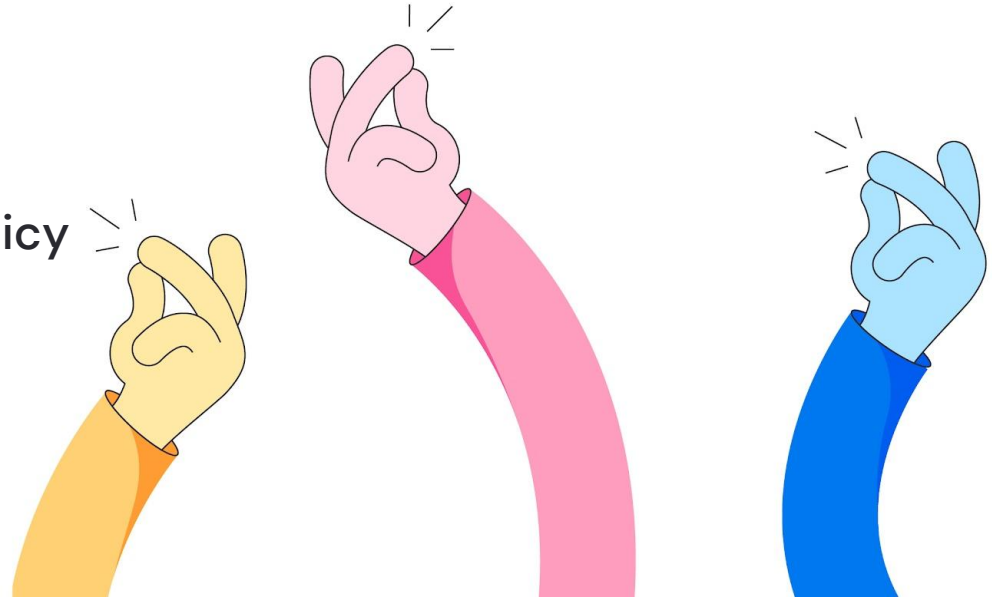
Agenda

01 Demostack Commitment to Privacy and Security

02 Security and the SOC 2

03 Privacy, GDPR and HIPAA

04 Security Assurance and Policy



demostack

Demostack Commitment to Privacy and Security

Demostack is committed to Privacy and Security as core values, and competitive differentiators.

Security is very much part of our DNA

Broad security experience and skills within staff

Head of GRC was employee #6 in the US

Strategic Priorities

Security and the SOC 2

Privacy, GDPR and HIPPA

We don’t sell or transfer customer data / personal information to any third party.

demostack

Security and the SOC 2

Earned SOC 2 Type 1 with PWC April 14, 2022

- “Unqualified” Attestation; no control gaps identified
- Type 2 assessment begins July, continues through December

Security “defense in depth” strategy

- Data center and network security
- App security and data security
- Pen testing and Responsible Disclosure Program

Data Center and Network Security

We run in Google Cloud Platform, in US

Kubernetes Engine (GKE)
Cloud CDN (Content Delivery Network)
Data stores: Cloud Datastore, MongoDB, Cloud Storage
Key Management, Secret Manager
Nothing “on-prem”
Environments separation (dev, testing, production)

We use Google Security Command Center to monitor assets, identify vulns/misconfigurations, detect threats, and assess compliance against security standards.

Application and Data Security

All customer data is encrypted at rest and in transit

Authenticate with Okta Identity Providers-support SAML, SSO, OID

Use a variety of external security services to monitor and alert

- Snyk for Vulnerability detection and mgmt
- OneTrust for Continuous Compliance Monitoring
- Security Scorecard rates us on 10 dimensions, an “A”

Domain security and Email security implemented - full DMARC
(Domain-based Message Authentication, Reporting and Conformance)

Roles-based security awareness and training for Engrs, All Hands

Application and Data Security (continued)

Substantial Security expertise and certifications among engineers (CISSP, CISM, OWASP, etc.)

Deployed Test-driven development (TDD) methodology

Active, weekly security team meetings - conducted and reported to highest levels in Org

External Pen tests at least semi-annually, with HackerOne

We support a Vulnerability Disclosure (“bug bounty”) Program

Privacy by Design

Thinking strategically about how privacy practices fit into Demostack's overall business strategy is making privacy a core part of the business model.

Competitive differentiator.

Privacy and Data Protection Frameworks

GDPR

EU-UK Data Processing Agreement and SCCs complete

Working with Privacy Consultancy to audit, continually improve Policy processes and tools

HIPAA

Compliant with HIPAA Privacy and Security Rules

CCPA/CPRA

Not yet subject to CCPA, but working toward compliance

Expanding capability to remove PII *before* being stored –"PII Shield"

PII Shield - Overview (roadmap)

PII Shield anonymizes PII in real time when recording, so sensitive data is not captured or stored.

How it works

PII is filtered before the recording is stored in Demostack, using filtering rules like:

- In these locations in the app, replace the real name with a random name
- In these locations in the app, replace the SSN with asterisks (***)
- In these locations in the app, replace the address with a generated address

Rules are usually pairs of (where in the page, what to put there)

Technical details

Filtering rules are defined with you and implemented by Demostack

There's no current UI for defining these rules, this is done by Demostack

We can filter text in HTML files and in JSON files (API responses)

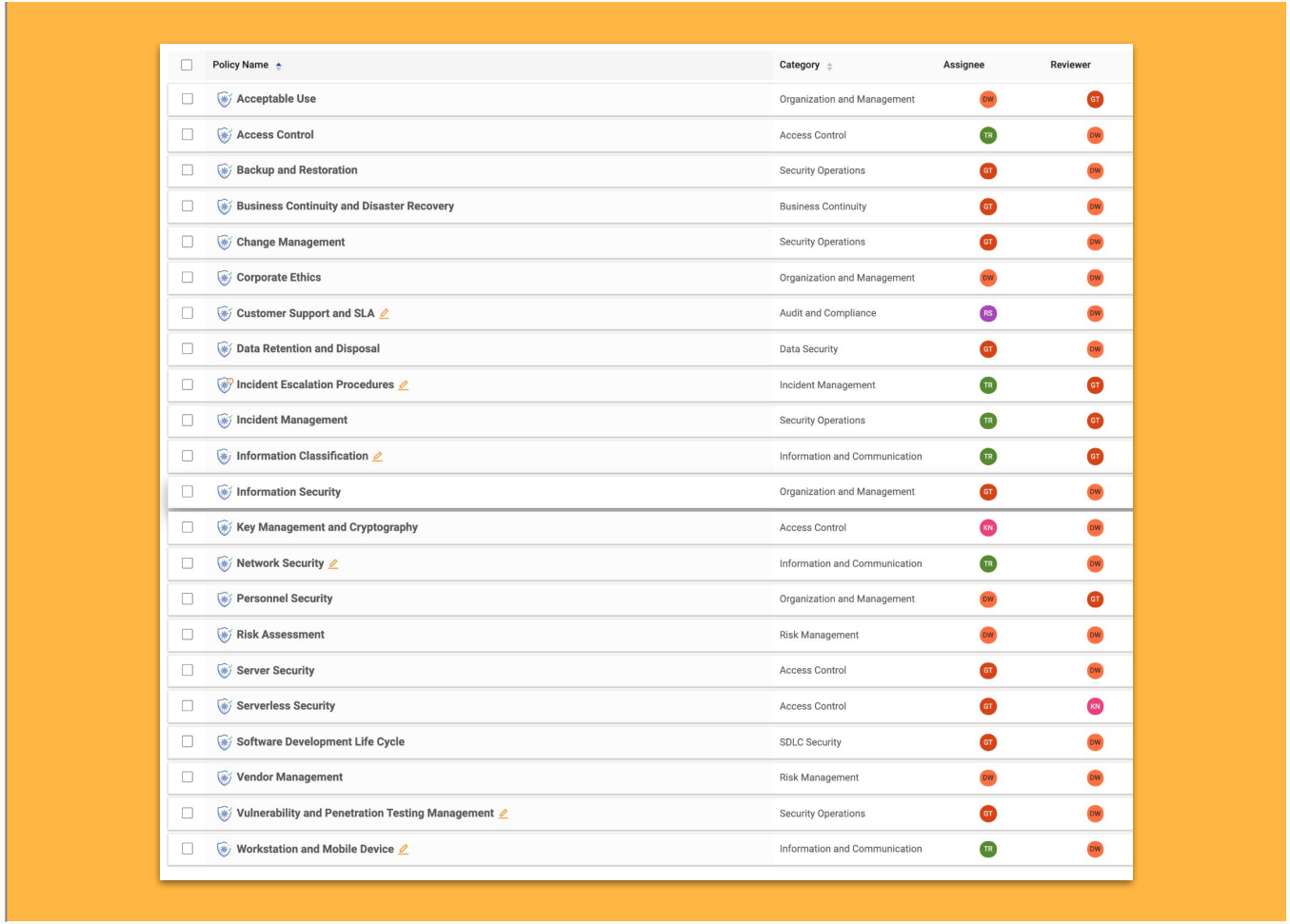
We currently do not automatically detect names in large blocks of text, just in preset fields/locations

Security Assurance with OneTrust and Tugboat Logic

- Deployed Continuous Monitoring and Assurance
  - Example: GCP Integration
  - Integration supports automated evidence collection for many security controls: cloud IAM configuration, cloud firewall rules, cloud data at rest encryption, system event logging, and system performance and capacity monitoring.
- InfoSec Policy Mgmt and Controls
- Vendor Risk Management
- Security Awareness and Training

Information Security Policies

.



Policy Name	Category	Assignee	Reviewer
Acceptable Use	Organization and Management	DW	GT
Access Control	Access Control	TR	DW
Backup and Restoration	Security Operations	GT	DW
Business Continuity and Disaster Recovery	Business Continuity	GT	DW
Change Management	Security Operations	GT	DW
Corporate Ethics	Organization and Management	DW	DW
Customer Support and SLA	Audit and Compliance	RS	DW
Data Retention and Disposal	Data Security	GT	DW
Incident Escalation Procedures	Incident Management	TR	GT
Incident Management	Security Operations	TR	GT
Information Classification	Information and Communication	TR	GT
Information Security	Organization and Management	GT	DW
Key Management and Cryptography	Access Control	KN	DW
Network Security	Information and Communication	TR	DW
Personnel Security	Organization and Management	DW	GT
Risk Assessment	Risk Management	DW	DW
Server Security	Access Control	GT	DW
Serverless Security	Access Control	GT	KN
Software Development Life Cycle	SDLC Security	GT	DW
Vendor Management	Risk Management	DW	DW
Vulnerability and Penetration Testing Management	Security Operations	GT	DW
Workstation and Mobile Device	Information and Communication	TR	DW

Contacts

David Williamson
Head of GRC / DPO

CISSP, CRISC, CGEIT, Member IAPP
Former Head of Information Security Policy for Visa Inc.
privacy@demostack.com

Gonen Tiberg
CISO and Director of Engineering

CISM, CDPSE, Member ISACA
Reports to CTO, member of Leadership team.
Former Security Officer for FCA-regulated fintech startup Covercy
security@demostack.com

Thank You!

demostack