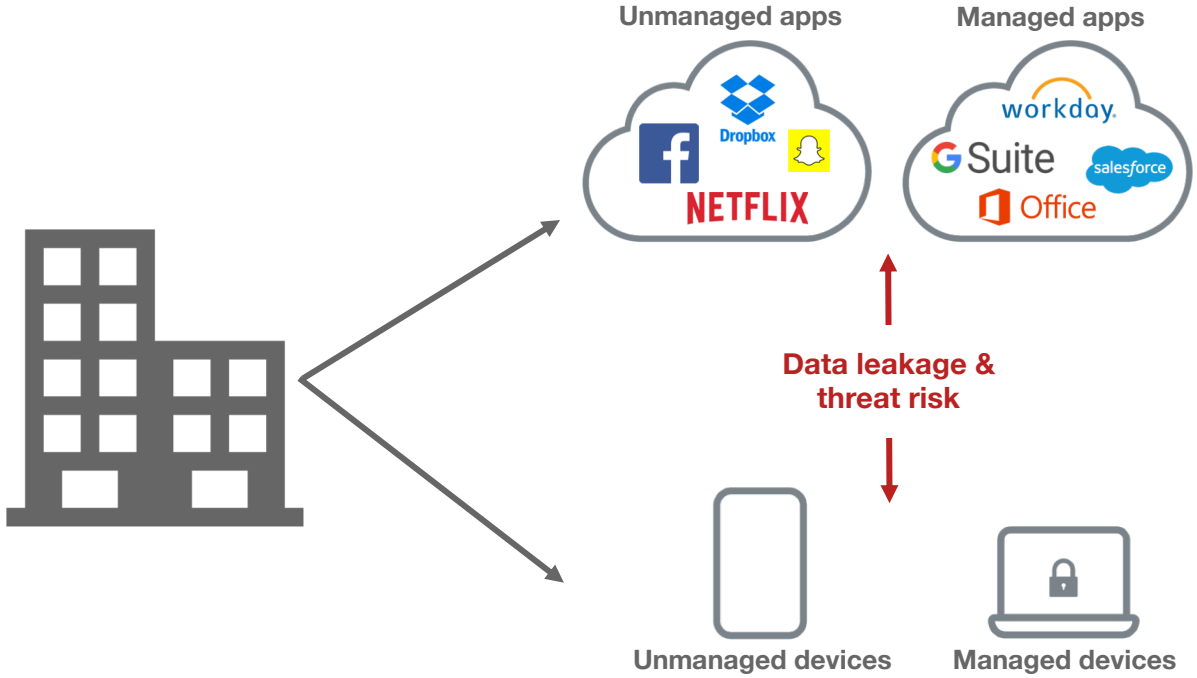
Problem

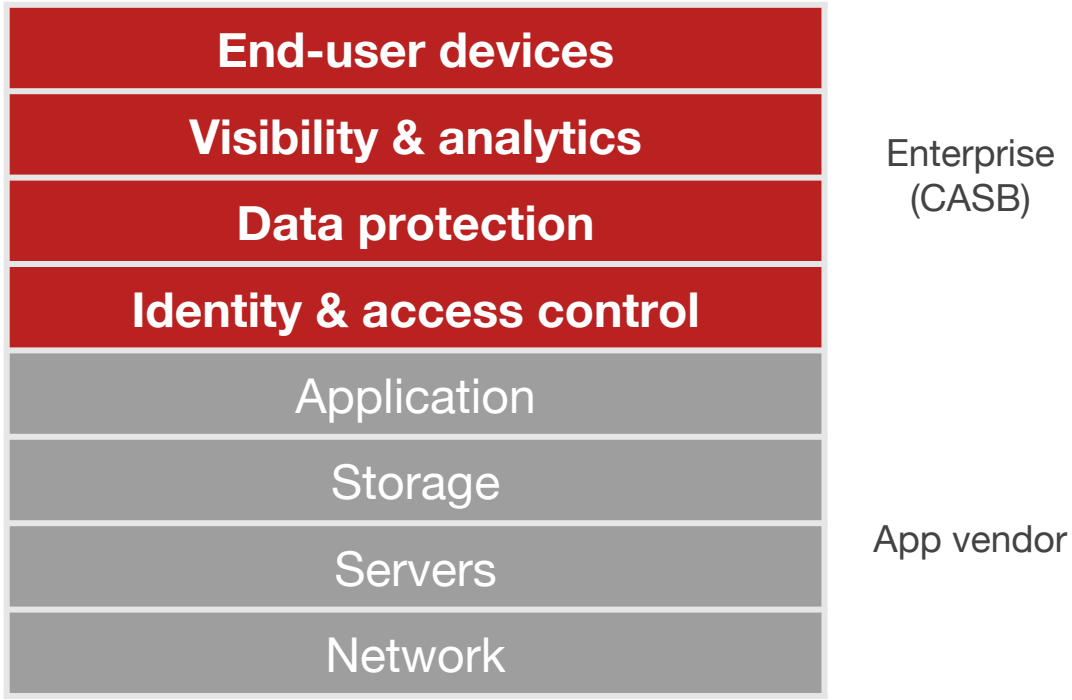
Cloud and mobile are beyond the firewall...

Legacy Tech
Firewall
Premises DLP
MDM
SSL VPN
Web Proxy



...leaving legacy security technologies obsolete.

SaaS Shared Responsibility Model



bitglass

1: Identity & Access Control

- Control access based on identity and context
  - User, role & authentication type
  - Device (managed vs unmanaged), location, app, access method, data, etc.
- Extend premises identity best practices to the cloud and across the entire session (e.g., step-up MFA)
- Example: User on unmanaged device accessing Office365
  - Force MFA for new device/location access
  - Block OneDrive sync (too much data on endpoint)
  - Restricted web/email access - encrypt downloads of sensitive data

bitglass

2: Prevent Data Leakage

- Detection
  - Native CASB or via integration with network DLP
  - Most common: sync of policy network→ CASB
- Data-at-rest
  - API integration with cloud app
  - Scanning + attribute/permission modification quarantine, encrypt, etc)
- Data-in-transit
  - Real-time, inline control via proxies
    - Agentless support required for any device control
  - Detect + remediate beyond allow or block
    - Redact, encrypt, block, watermark, more

bitglass

3: Threat Prevention

- Most cloud apps don’t have built-in malware protection
  - Signature-based malware no longer effective for new threats
  - Cloud apps a convenient malware distribution mechanism
- Unwanted user activity must be detected and stopped
  - Intra- and inter-cloud important
  - Proactive response (Step-up MFA, reauthenticate, block access)

4: Unmanaged App Control

- Automatically discover and learn new applications
  - 100k's of apps require ML-based classification and control; signatures no longer effective
- Control required - discovery no longer sufficient
  - Options: Sanction+Control, Coach, Block, Read-only, Alert/Notify

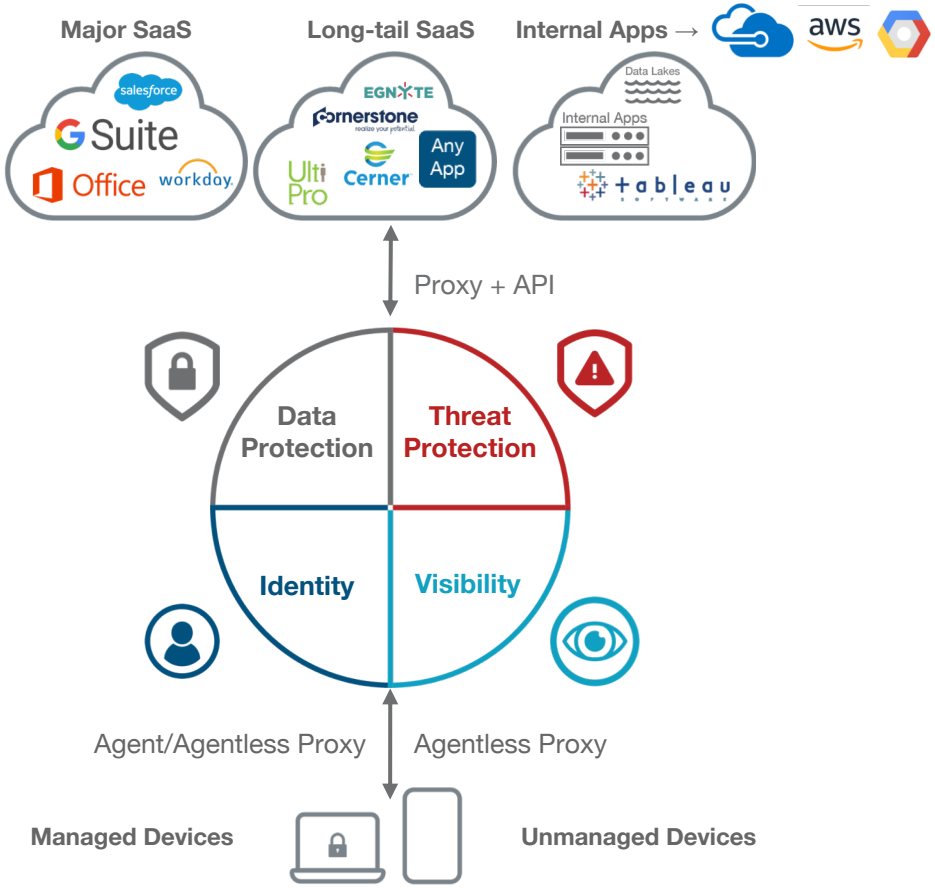
bitglass

5: Mobile Data Protection

- Cloud data doesn’t stay in the cloud - sync, download, etc., from both managed and BYOD
  - BYOD is a bigger data protection challenge than data-at-rest in cloud
- Requirements
  - Control flow of data to the device
    - Advanced DLP detection and control
  - Protect data on the device
    - MDM doesn’t work for BYOD - need alternative
    - Combine with data-centric protection (DRM, encryption, tracking, etc)

bitglass

How CASBs Work



How CASBs Work

API Integration

- Visibility and control over data-at-rest

Forward Proxy

- Managed device controls for sanctioned/unsanctioned apps

Reverse Proxy

- Agentless managed/unmanaged device controls for sanctioned apps

Protocol-specific proxies

- Purpose-built agentless proxies for common use cases (Activesync, MAPI, etc)

bitglass

Northwestern University

Over 20,000 students and 3,000 faculty members

Challenges

- Cloud deployment met with security concerns around intellectual property, research, and health data
- Unmanaged device access controls
- Compliance requirements including HIPAA and FERPA

Solution

- Granular DLP policies to identify and secure PHI
- Regular scans for zero-day malware in the cloud
- Distinguish between managed and unmanaged devices
- Technical safeguards for HIPAA compliance at Feinberg School of Medicine

JOHN MUIR HEALTH

Over 900 physicians; leading Bay Area non-profit

Challenges

- Inadequate native O365 security
- PHI leakage from unmanaged devices
- Agent-based CASB competitors and AirWatch failed to deploy

Solution

- Distinguish between managed and unmanaged devices
- Limit PHI access from risky unmanaged assets
- Real-time DLP prevents data leakage on download
- Readily deployable to all mobile devices, managed and unmanaged

WELLS FARGO

Challenges

- Encrypt sensitive data in SaaS applications
- Preserve functionality - search, sort etc.
- Incumbent solution did not perform

Solution

- Bitglass encryption for Salesforce, Box, Marketo
- Private cloud, on-premise or AWS deployment
- Encrypt/decrypt PII & email addresses
- SMTP mail relay for decryption

Only Bitglass

Zero-day security,
any app or workload

Agentless deployment,
any device

Real-time data protection,
anywhere

Global enterprise success via
sustained innovation and **scale**

www.bitglass.com
@bitglass