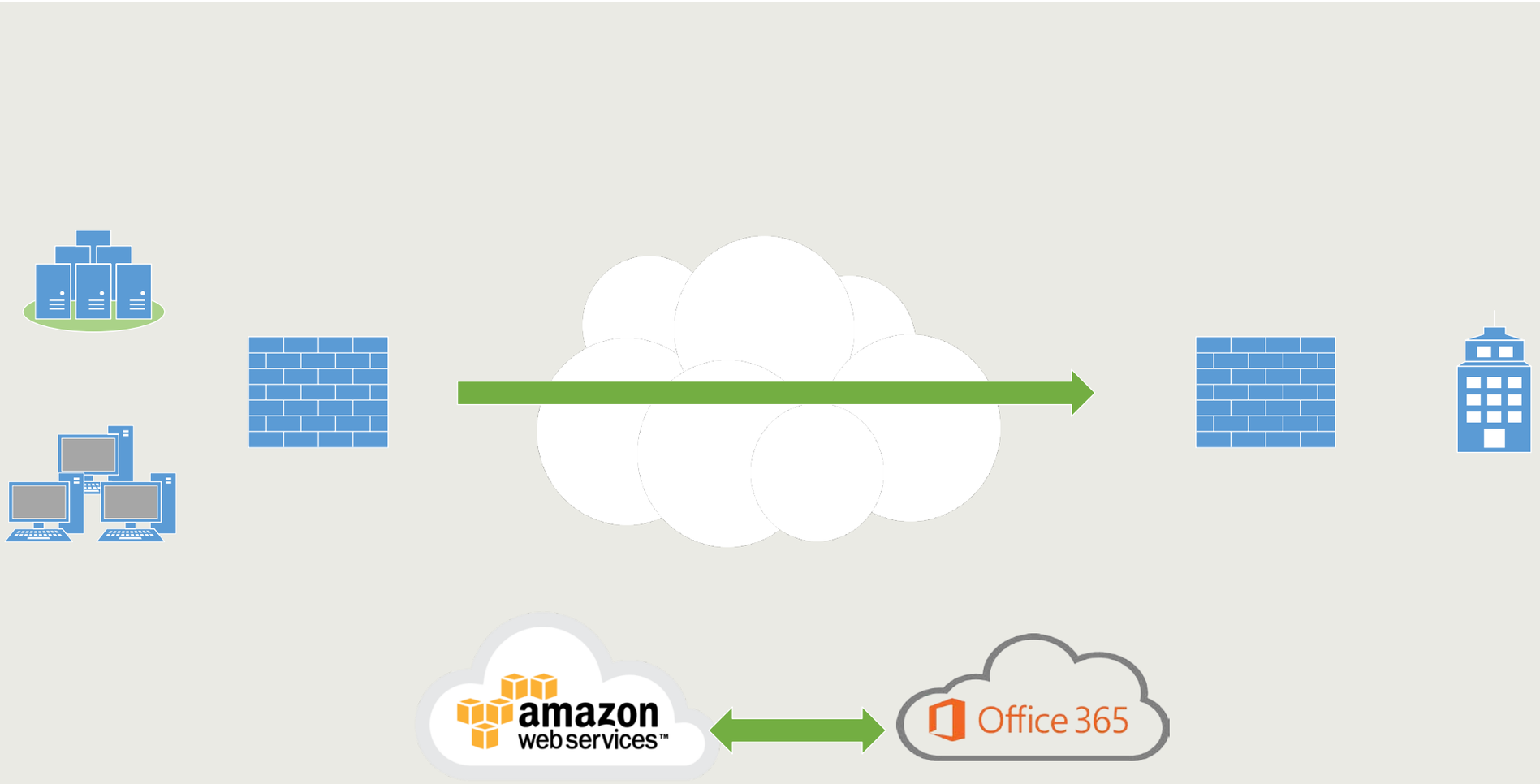
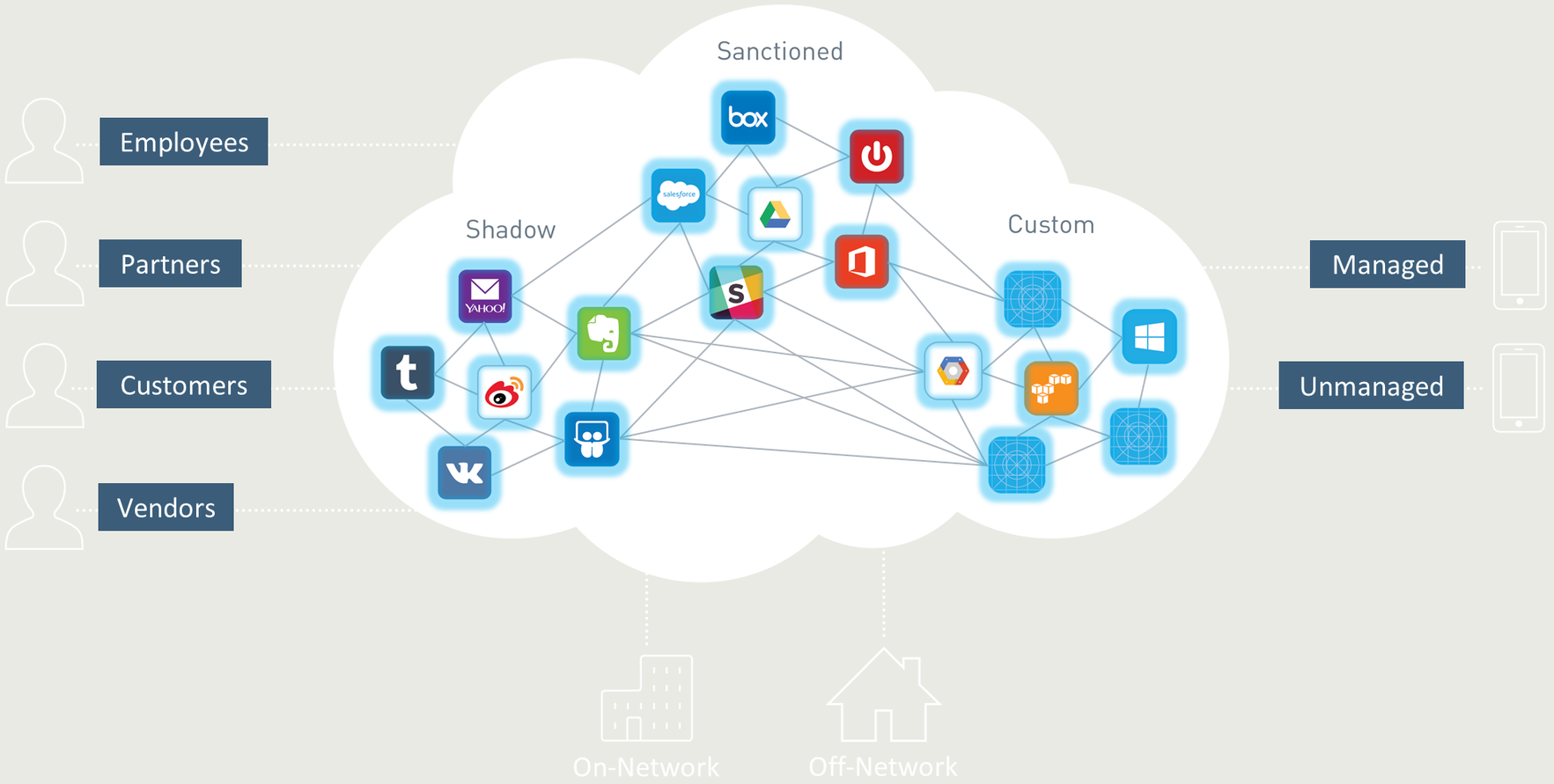
Cloud Security

Cloud Access Security Brokers

Historical Approach to Information Security

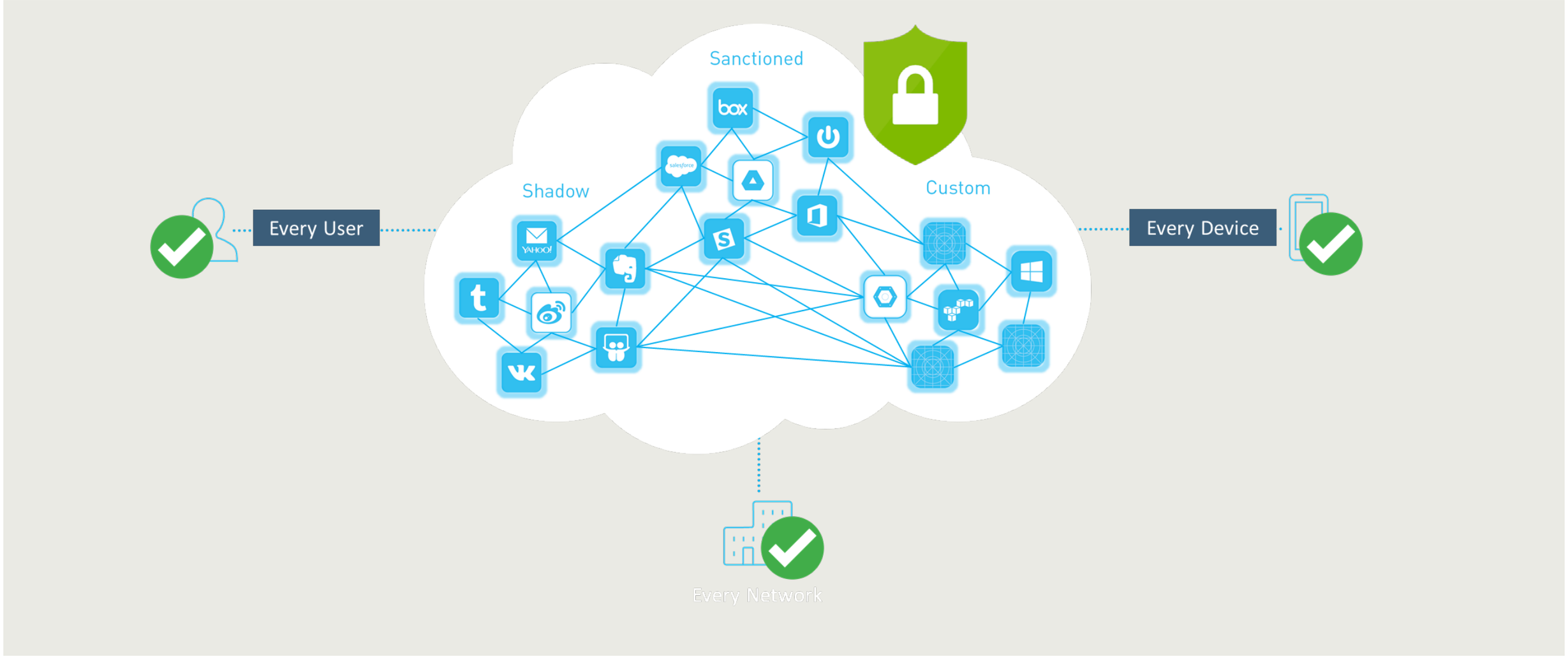


Network based controls do not work!



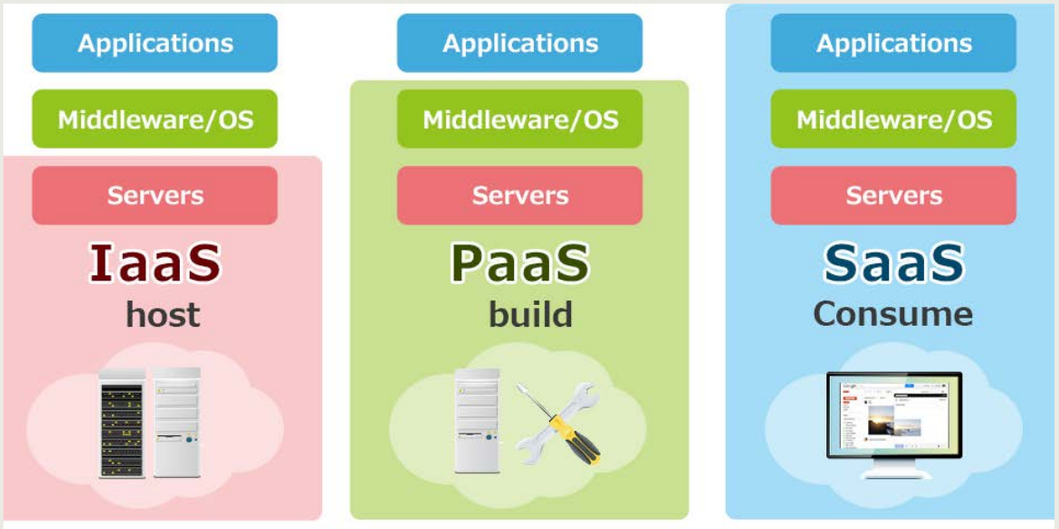
https://www.skyhighnetworks.com/

Cloud Access Security Broker: Adds Security for all apps, networks, users & devices



Cloud Services

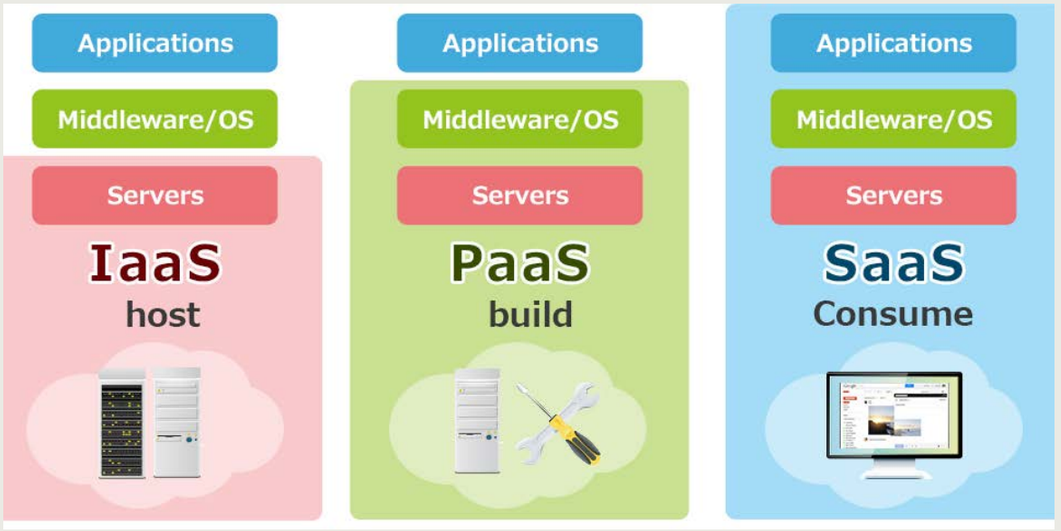
- Infrastructure as a Service (IaaS) – systems and storage (e.g. AWS, Azure)
- Platform as a Service (PaaS) – application stack (e.g. GCP)
- Software as a Service (SaaS) – business applications (e.g. Workday, O365)



https://medium.com/@Albihany/true-cloud-story-about-iaas-paas-saas-47cfea883271

Cloud Security: Who is responsible?

- Infrastructure as a Service (IaaS)
  - Network security, vulnerability management, data security, user security
- Platform as a Service (PaaS)
  - Vulnerability management, data security, user security
- Software as a Service (SaaS)
  - User security



https://medium.com/@Albihany/true-cloud-story-about-iaas-paas-saas-47cfea883271

PCI DSS Shared Responsibility of Google Cloud Platform

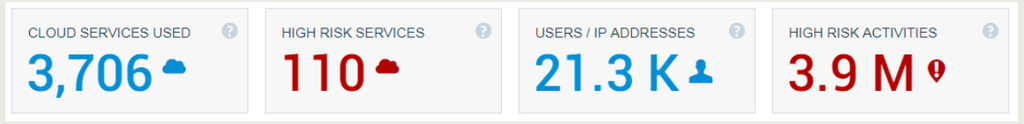
PCI DSS Requirements 3.1	Testing Procedures 3.1	GCP (Google Cloud Platform) Responsibility	Customer Responsibility
1.1 Establish and implement firewall and router configuration standards that include the following:	1.1 Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:		
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	1.1.1.a Examine documented procedures to verify there is a formal process for testing and approval of all: * Network connections and * Changes to firewall and router configurations	Google's internal production network and systems have been assessed against and comply with this requirement.	GCP customers are responsible for implementing processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on GCP comply the requirements of Section 1 of PCI DSS.
	1.1.1.b For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested.	Google's internal production network and systems have been assessed against and comply with this requirement.	GCP customers are responsible for implementing processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on GCP comply the requirements of Section 1 of PCI DSS.
	1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	Google's internal production network and systems have been assessed against and comply with this requirement.	GCP customers are responsible for implementing processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on GCP comply the requirements of Section 1 of PCI DSS.
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any	1.1.2.a Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all	Google's internal production network and systems have been assessed against and comply with this requirement.	GCP customers are responsible for implementing processes and procedures necessary to ensure that all network

Cloud Security

Cloud Access Security Brokers: Deployment Strategy

L.L.Bean’s approach to Shadow IT

- What we’re trying to accomplish:
  - Identify where L.L.Bean data is going



  - Control where L.L.Bean data goes
    - **Identify** sanctioned cloud applications: vetted by Security, Infrastructure and Procurement/IT Finance
    - **Migrate** users to corporately supported/provided cloud services (e.g. O365 Suite)
    - Deny access to ***unsanctioned*** cloud applications
  - Improve security operations:
    - Enable business processes
    - Minimize exceptions, simplify our configuration

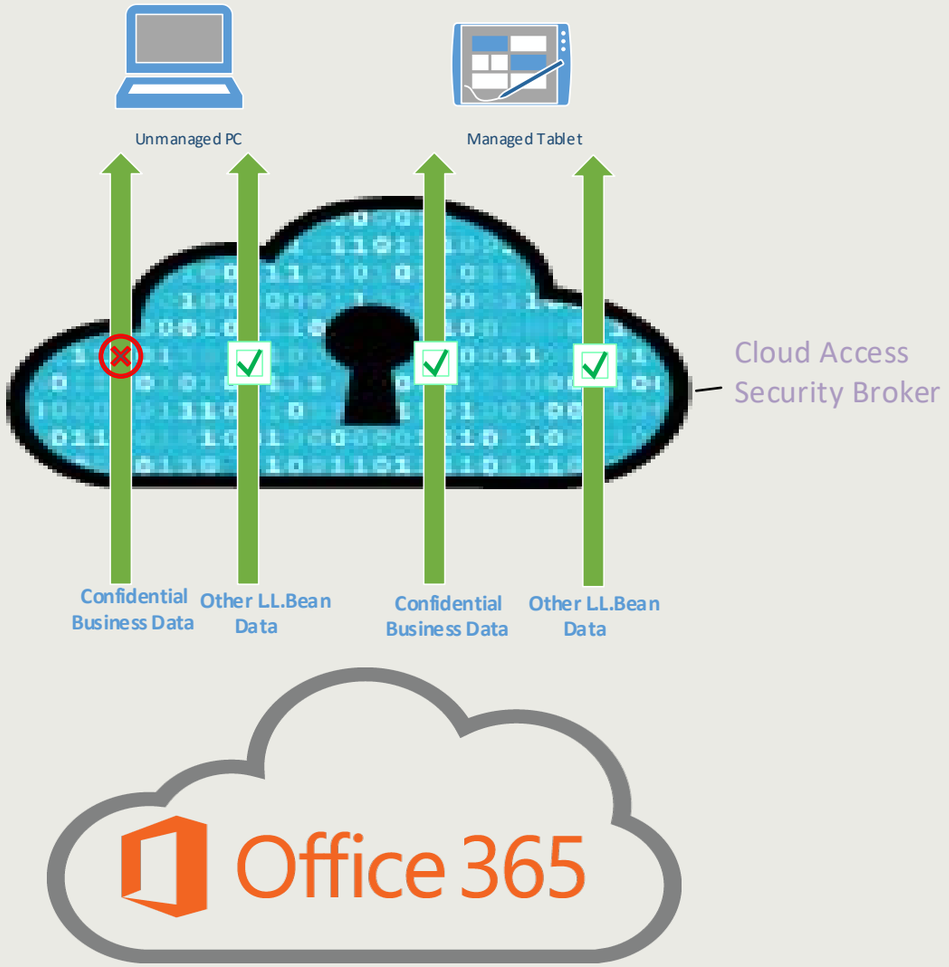
L.L.Bean: Performing DLP on data uploaded to O365

- Identify prohibited data based on company policy.
- Create policies in CASB to detect and quarantine/block data transfers.
- Test and tune policies.
- Apply policies.

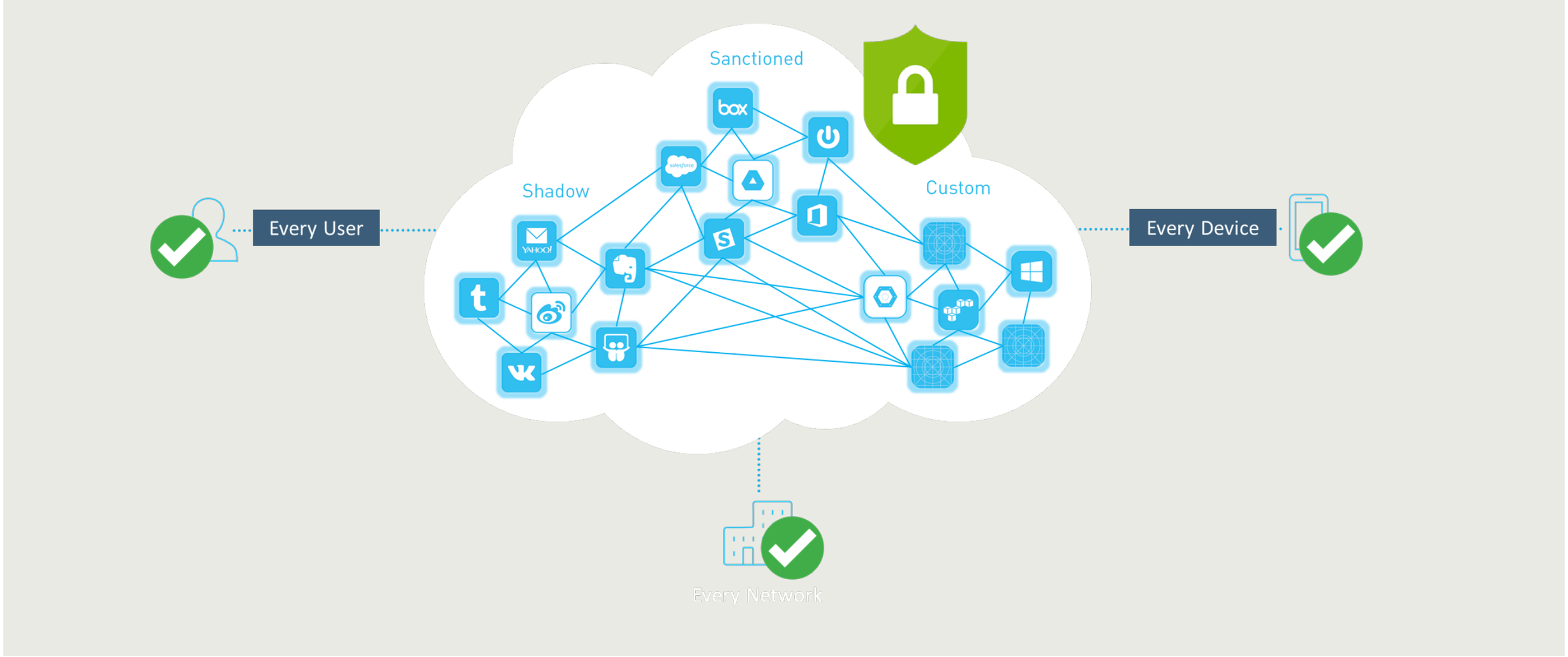
L.L.Bean

L.L.Bean: Managing personal device usage

- Managed devices
  - Use L.L.Bean issues certificate for identification
- Unmanaged devices
  - Require second factor of authentication
  - Only have access to certain classes of information



Cloud Access Security Broker: Adds Security for all apps, networks, users & devices



Questions?