McAfee
Together is power.

Embracing the Cloud, Securely

Reducing Risk, Enabling Innovation

& Case Studies

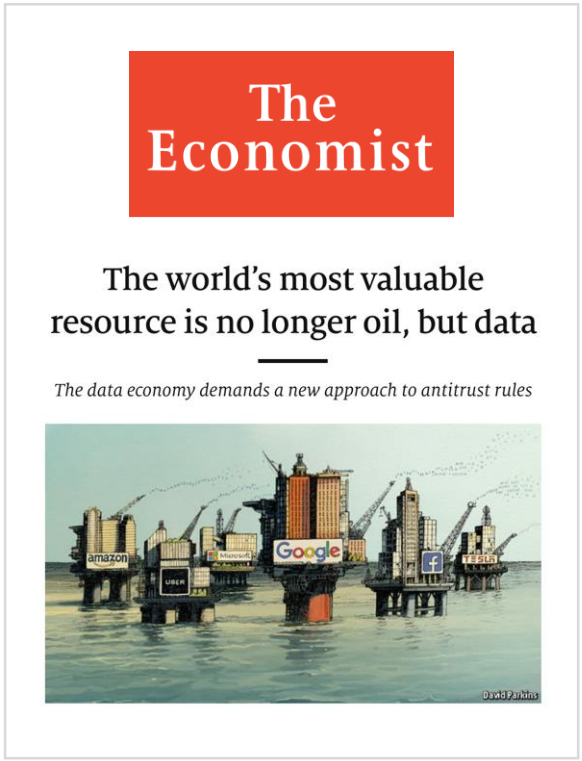
Nigel Hawthorn, EMEA Spokesperson

nigel_hawthorn@mcafee.com +44 7801 487987 @wheresnigel

Agenda

- Data: The Most Valuable Asset
- Cloud Is Taking Over, What Do The Analysts Say?
- Who Is Responsible for Cloud Security?
- Introducing Cloud Access Security Brokers
- Integration with McAfee Portfolio
- Customer Examples
- One SaaS Example - Prezi

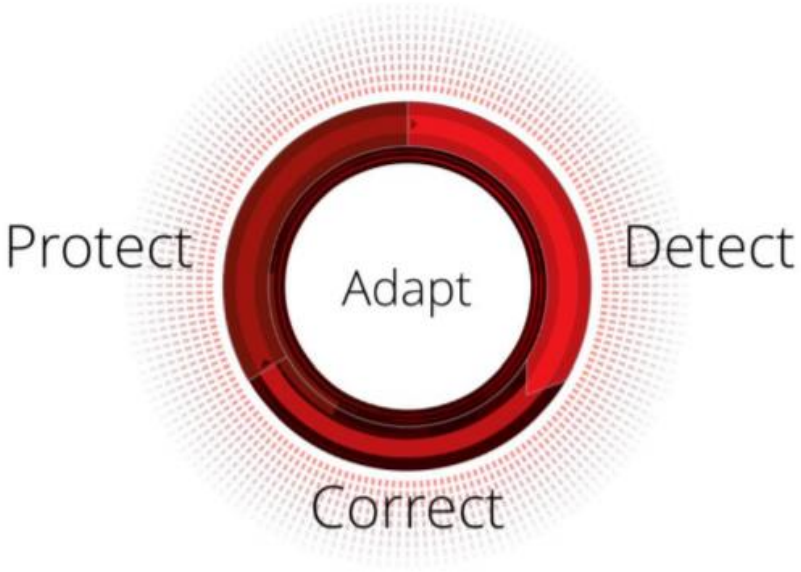
Data is the most valuable asset for organizations across industries

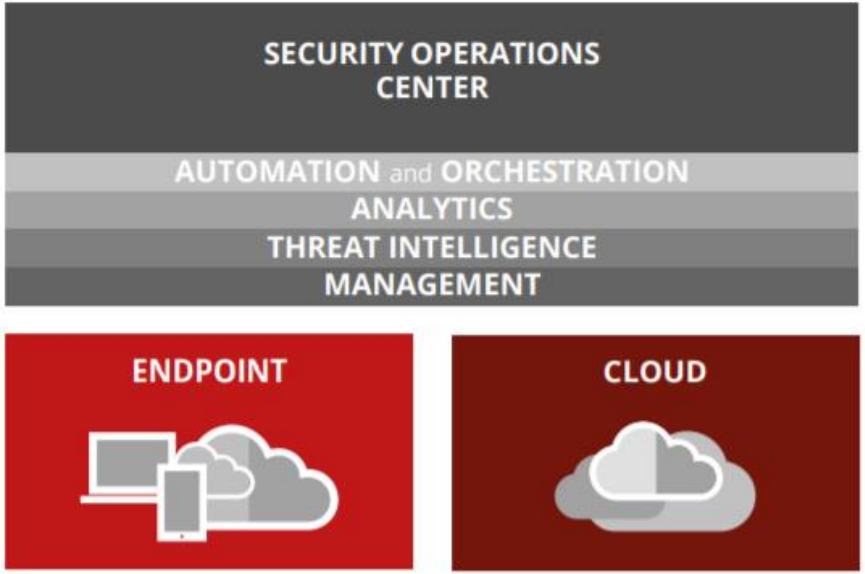


Data is to this century what oil was to the last one: a driver of growth and change.

McAfee Corporate Portfolio Strategy

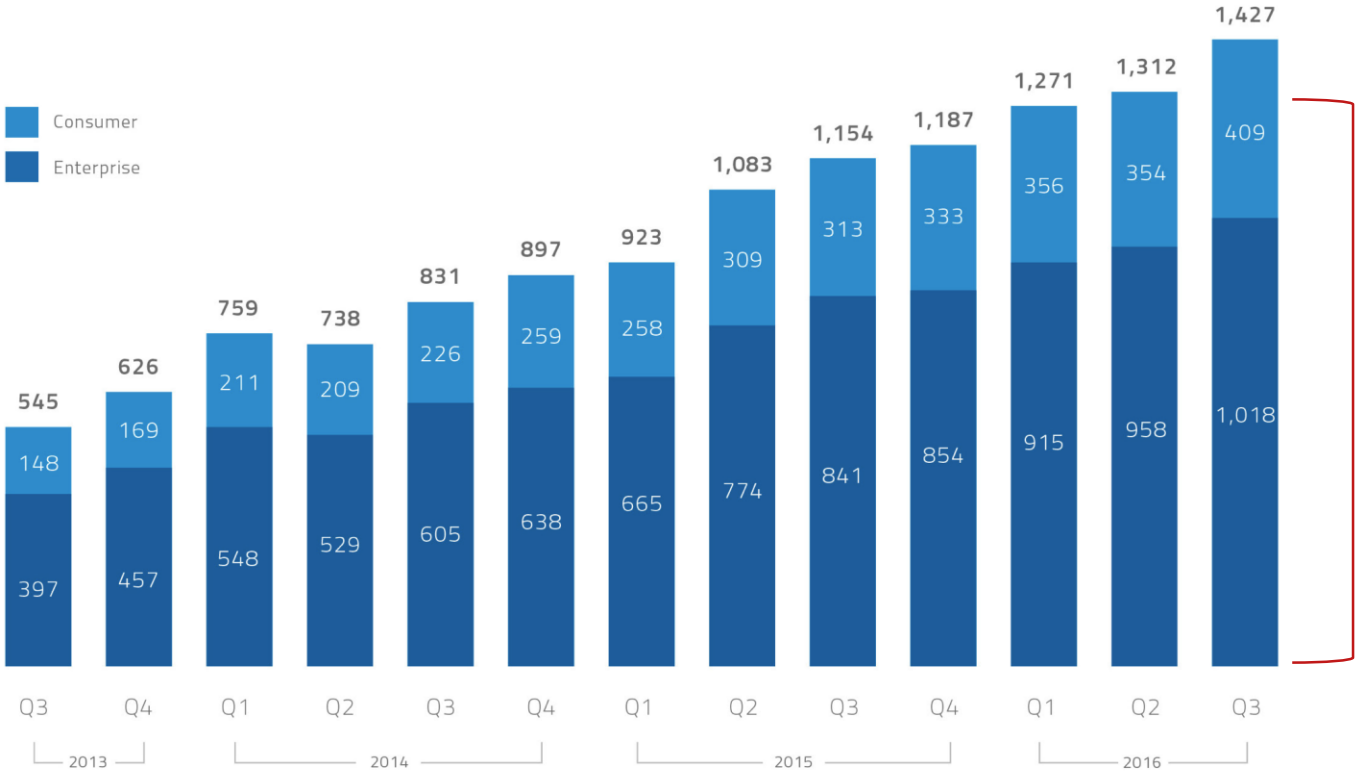
Delivering an integrated and open security system focused on endpoint and cloud security control points, unified in security operations through management, threat intelligence, analytics and orchestration





Cloud Is Taking Over

The Average Enterprise Uses 1,427 Cloud Services



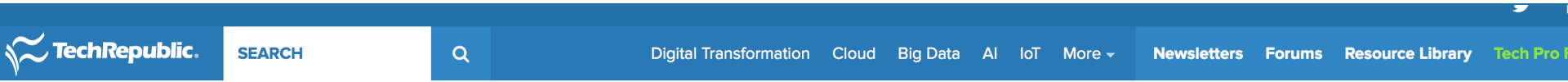
Network security fails to protect all data in the cloud & mobile era

Data created natively in cloud is invisible to network security

50% of cloud traffic is cloud-to-cloud and invisible to network security

Data uploaded to cloud from mobile is invisible to network security

How Secure Is The Cloud?

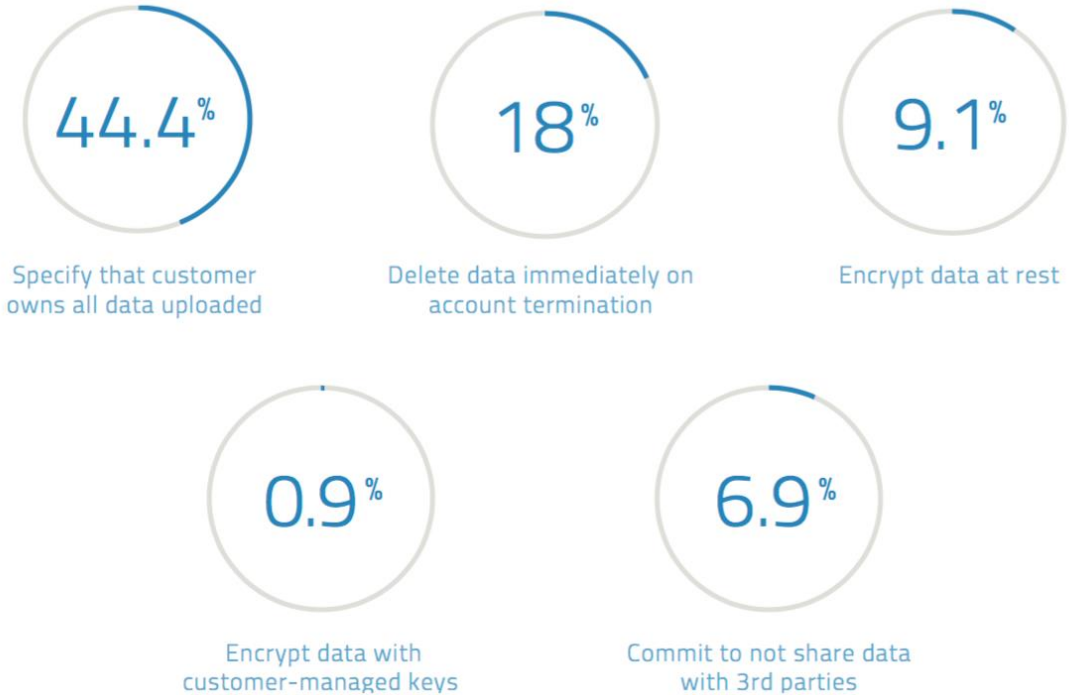


SECURITY

Tesla public cloud environment hacked, attackers accessed

"The message from this research is loud and clear—the unmistakable potential of cloud environments is seriously compromised by sophisticated hackers identifying easy-to-exploit vulnerabilities," Gaurav Kumar, CTO of RedLock, said in a press release. "In our analysis, cloud service providers such as Amazon, Microsoft and Google are trying to do their part, and none of the major breaches in 2017 was caused by their negligence. However, security is a shared responsibility: Organizations of every stripe are fundamentally obliged to monitor their infrastructures for risky configurations, anomalous user activities, suspicious network traffic, and host vulnerabilities. Without that, anything the providers do will never be enough."

Security Controls Vary by Provider



Security Controls Vary by Provider

Do not allow anonymous access

Of services provide user activity logging

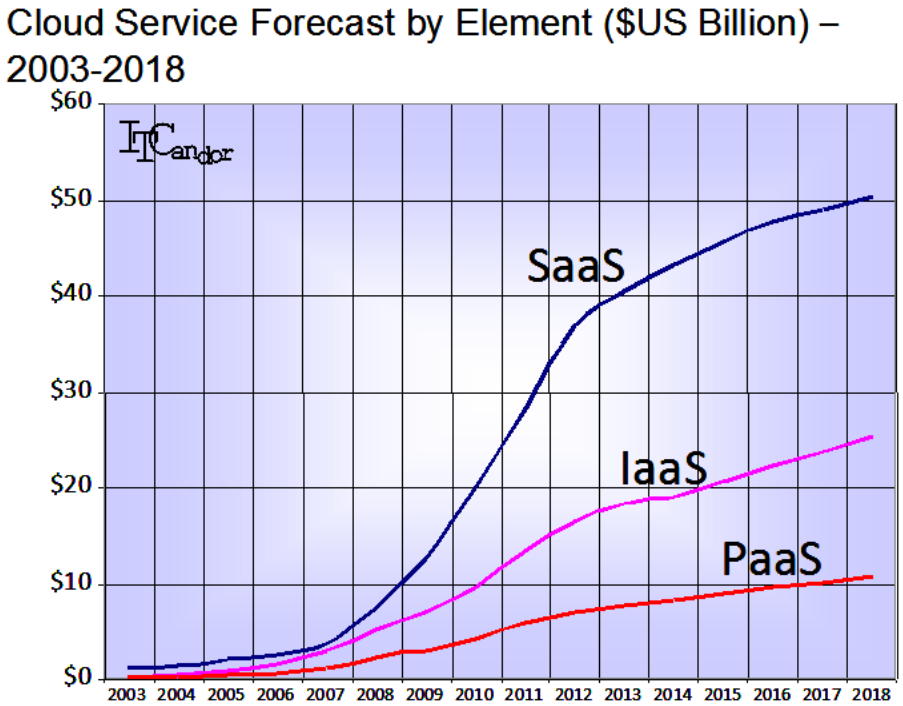
Offer data access logging

Provide integration with enterprise identity

Support multi-factor authentication

Provide identity federation using SAML, OAUTH or similar services

IaaS and PaaS Growing Fastest

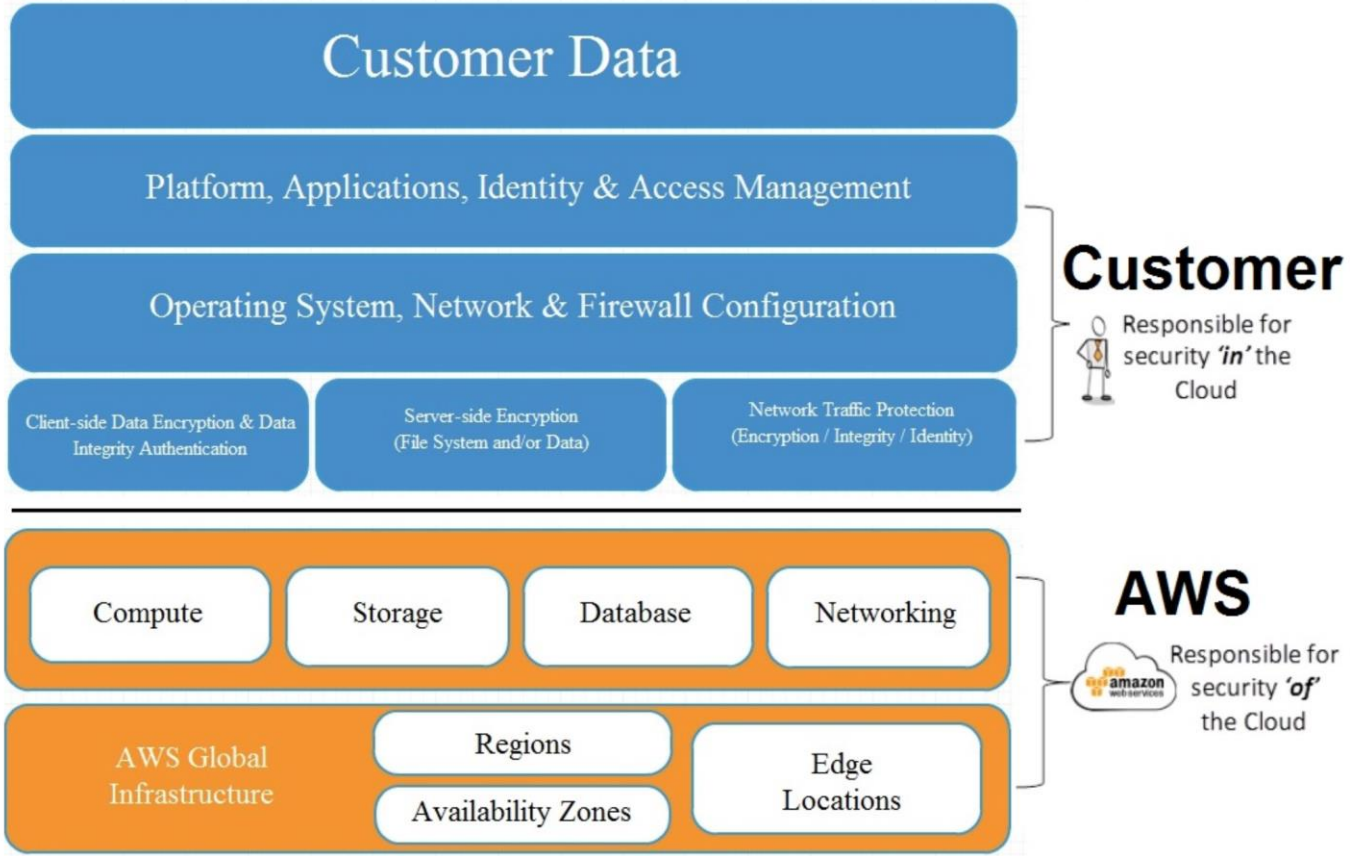


What are customers most concerned about?

- Security/regulatory requirements
- Collaborative nature of cloud
- Lack of Visibility, multiple clouds
- Increasing external/internal threats targeting cloud
- Well intentioned employee error
- Cloud providers' access to sensitive data

Who's Responsibility Is Cloud Security?

Cloud Shared Security Responsibility Model



Cloud Customer Needs

Identify

- Identify sensitive data in SaaS and IaaS services
- Understand access to and sharing of sensitive data
- Examine IaaS security configurations to eliminate vulnerabilities
- Discover and govern shadow SaaS/IaaS usage
- Detects threats – compromised accounts, insider threats, malware

Control

- Build sharing and collaboration guardrails
- Define and enforce access policies based on device, geo, role
- Delete high-risk files violating DLP policies
- Quarantine mid-risk files violating DLP policies
- Autonomously remediate low-risk files violating DLP policies

Protect

- Encrypt structured data with your own keys
- Implement IRM to protect data outside of the cloud

Introducing Cloud Access Security Brokers

Gartner

"Cloud access security brokers have become an essential element of any cloud security strategy, helping organizations govern the use of cloud and protect sensitive data in the cloud. Security and risk management leaders should align CASB vendors to address specific use-case requirements"

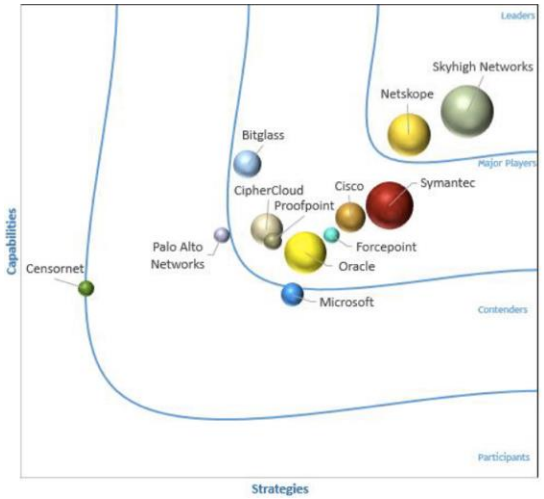
"Security leaders should deploy CASB for the centralized control of multiple services that would otherwise require individual management."

The Skyhigh Security Cloud enables organizations to accelerate their business by giving them total control over their data in the cloud

Analyst Reports: Skyhigh: Once, Twice, Three Times a Leader

Gartner®

IDC



FORRESTER®

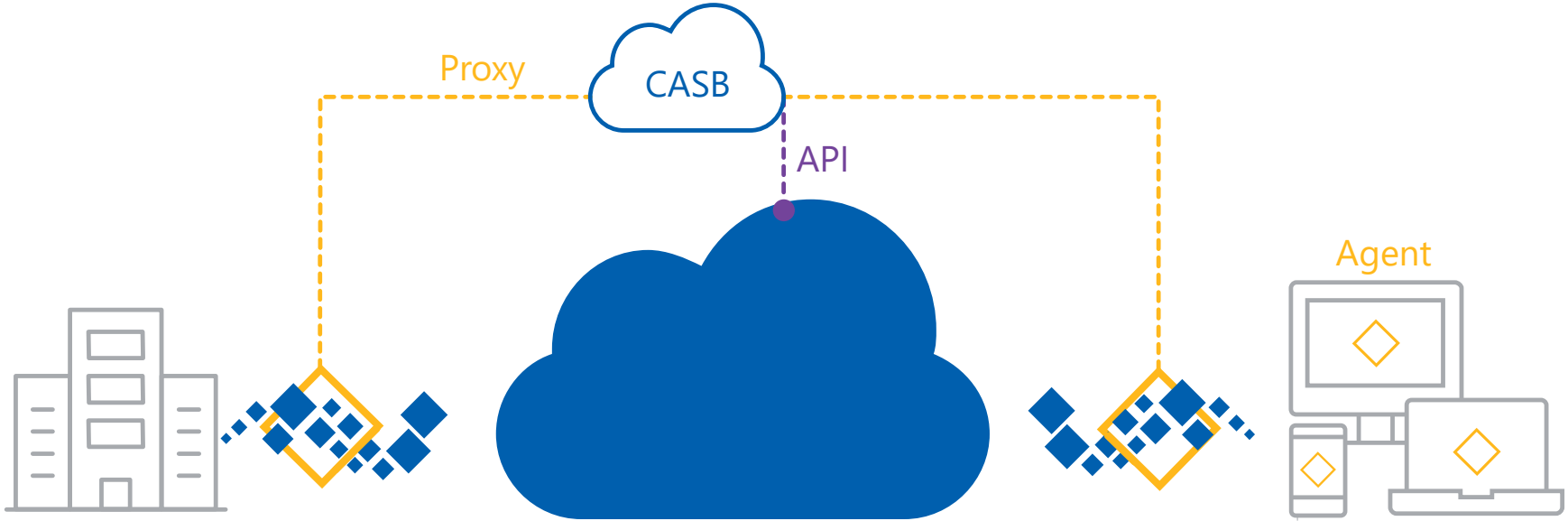
Network security fails to protect all data in the cloud & mobile era

Data created natively in cloud is invisible to network security

50% of cloud traffic is cloud-to-cloud and invisible to network security

Data uploaded to cloud from mobile is invisible to network security

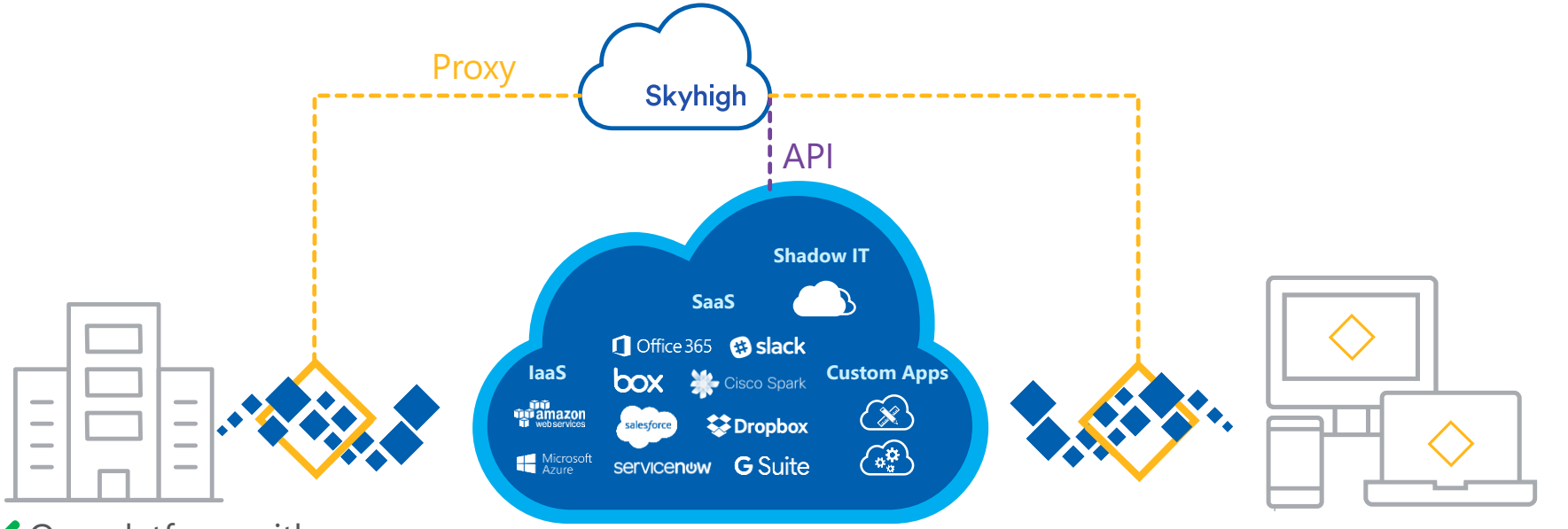
Different approaches to protecting data in the cloud & mobile era



✓ Real time
✗ Complete coverage
- ✗ Data at rest
- ✓ Data uploaded
- ✗ Data created in cloud
- ✓ Standard apps
- ✗ Certificate pinned apps
- 3rd Party Access

✗ Real time
✓ Complete coverage
- ✓ Data at rest
- ✓ Data uploaded
- ✓ Data created in cloud
- ✓ Standard apps
- ✓ Certificate pinned apps

Skyhigh – Proxy, API & McAfee Integration

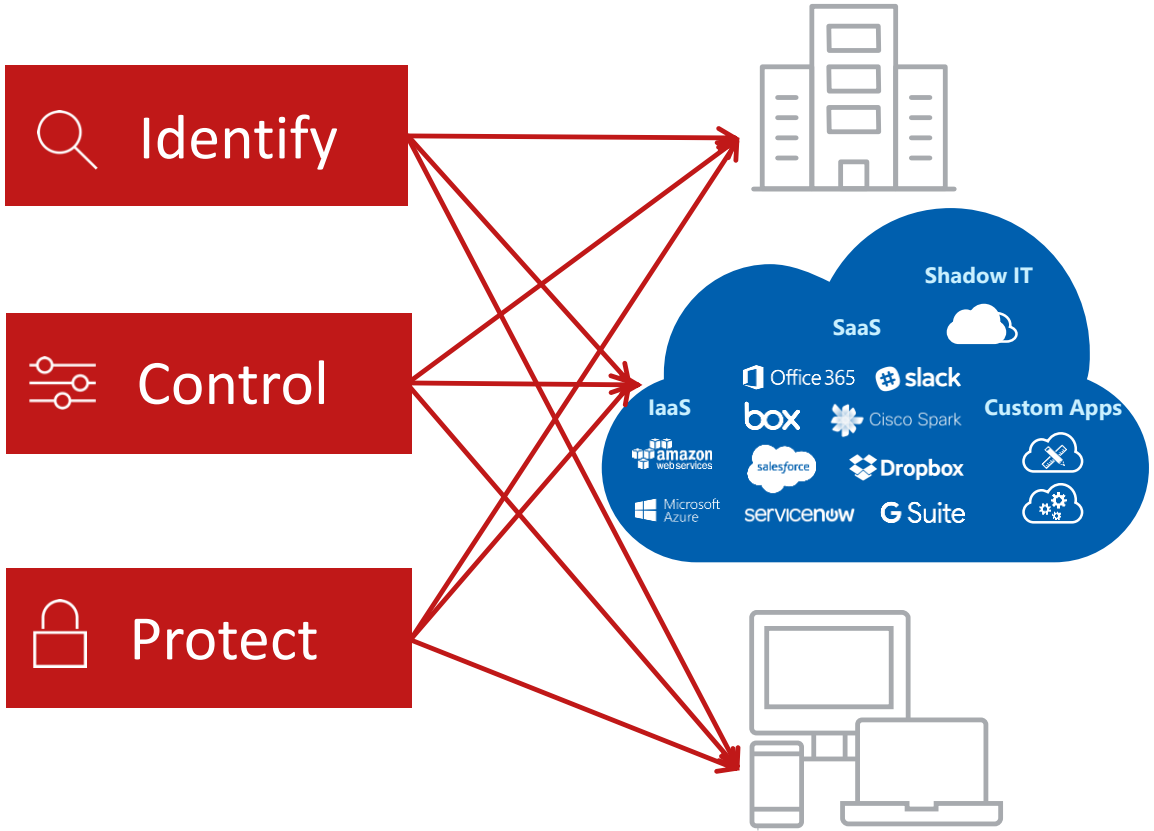


- One platform with unified polices across cloud services

- Real time
- Complete coverage
  - Data at rest
  - Data uploaded
  - Data created in cloud
  - Standard apps
  - Certificate pinned apps

- No new agents
- No friction

Skyhigh cloud-native data security framework

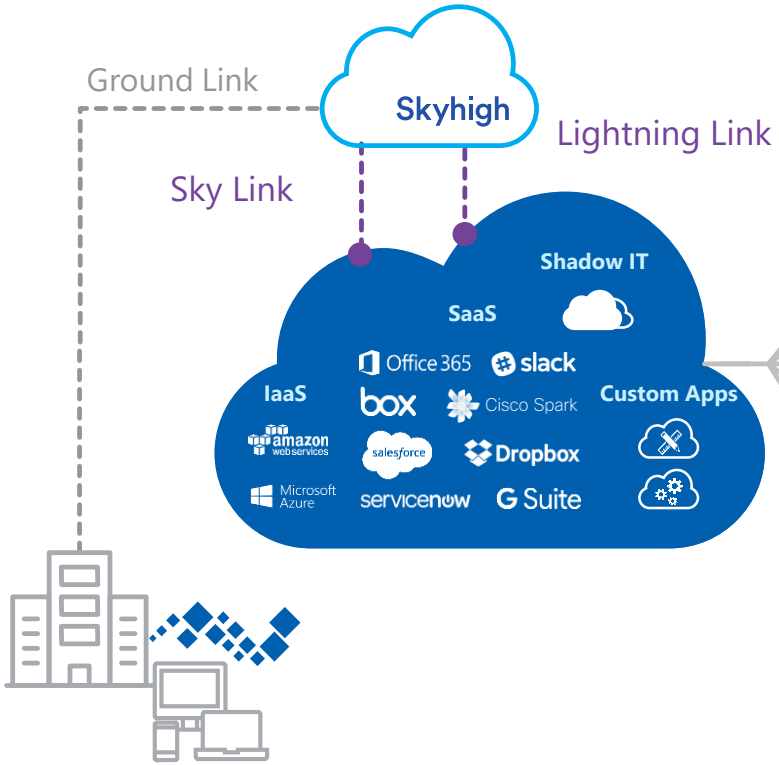


Understand information content and context

Take real-time action deep in cloud services

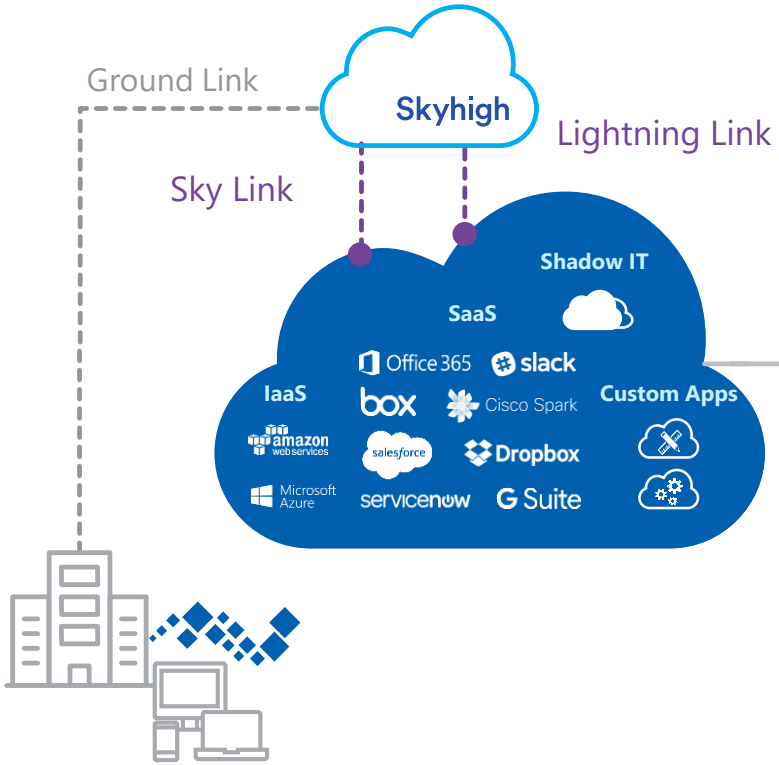
Apply persistent protection to data

Identify



- Identify sensitive data in SaaS and IaaS services
- Understand access to and sharing of sensitive data
- Examine IaaS security configurations to eliminate vulnerabilities
- Discover and govern shadow SaaS/IaaS usage
- Detects threats - compromised accounts, insider threats, malware

Control



Build sharing and collaboration guardrails

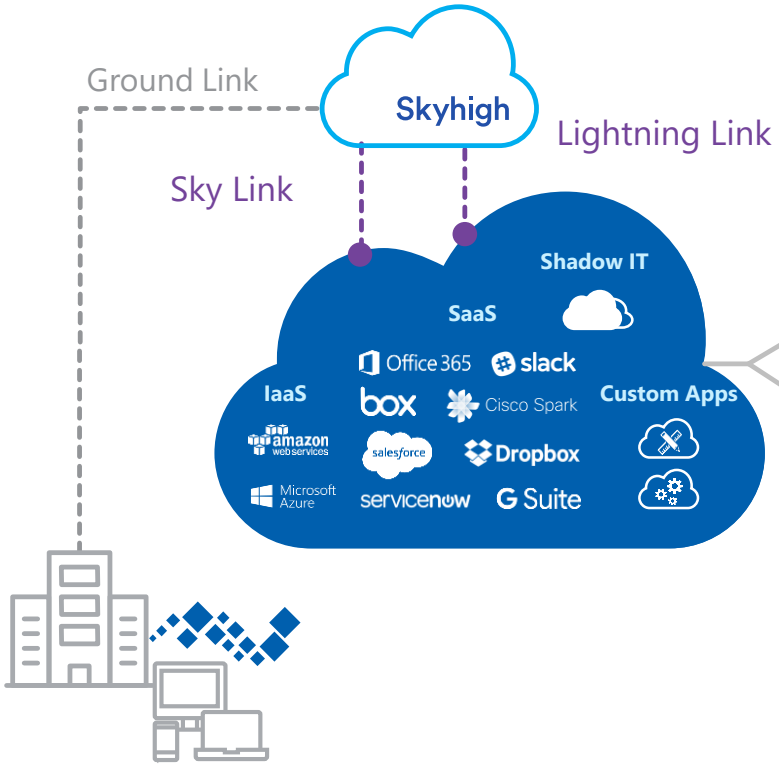
Define and enforce access policies based on device & geo

Delete high-risk files violating DLP policies

Quarantine mid-risk files violating DLP policies

Autonomously remediate low-risk files violating DLP policies

Protect



Encrypt structured data with your own keys

Implement IRM to protect data outside of the cloud

Customer Demands

Innovation – IaaS Review, custom apps, UEBA, automation to simplify management

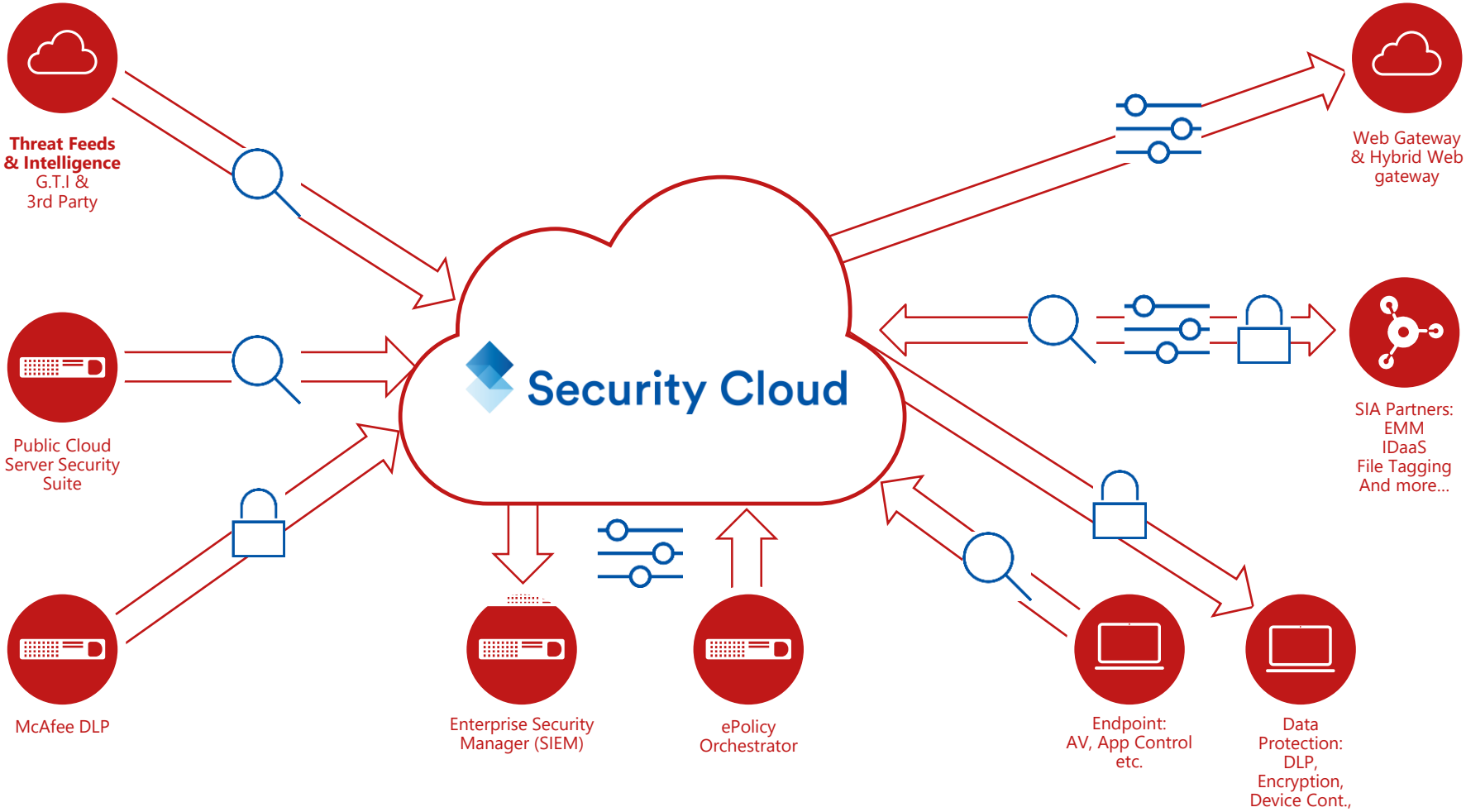
Frictionless Approach – no agents and no app breakage, one unified platform

Cloud Scale – processing billions events/day/customer requires cloud scalability

Flexible Deployment Options – Integration with existing technology, Email Gateway

Control All Traffic – Business partners, collaboration control, cloud-to-cloud traffic

Integration with McAfee Portfolio


Threat Feeds
& Intelligence
G.T.I &
3rd Party
Public Cloud
Server Security
Suite
McAfee DLP
Security Cloud
Enterprise Security
Manager (SIEM)
ePolicy
Orchestrator
Web Gateway
& Hybrid Web
gateway
SIA Partners:
EMM
IDaaS
File Tagging
And more...
Endpoint:
AV, App Control
etc.
Data
Protection:
DLP,
Encryption,
Device Cont.,

Customer Examples

Hard Data from the Cloud Adoption and Risk Report

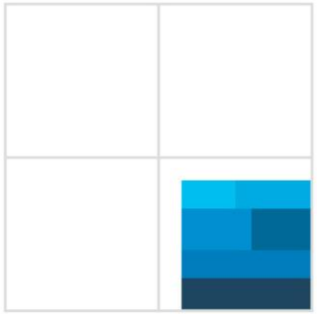
Anonymized usage data from 600+ companies

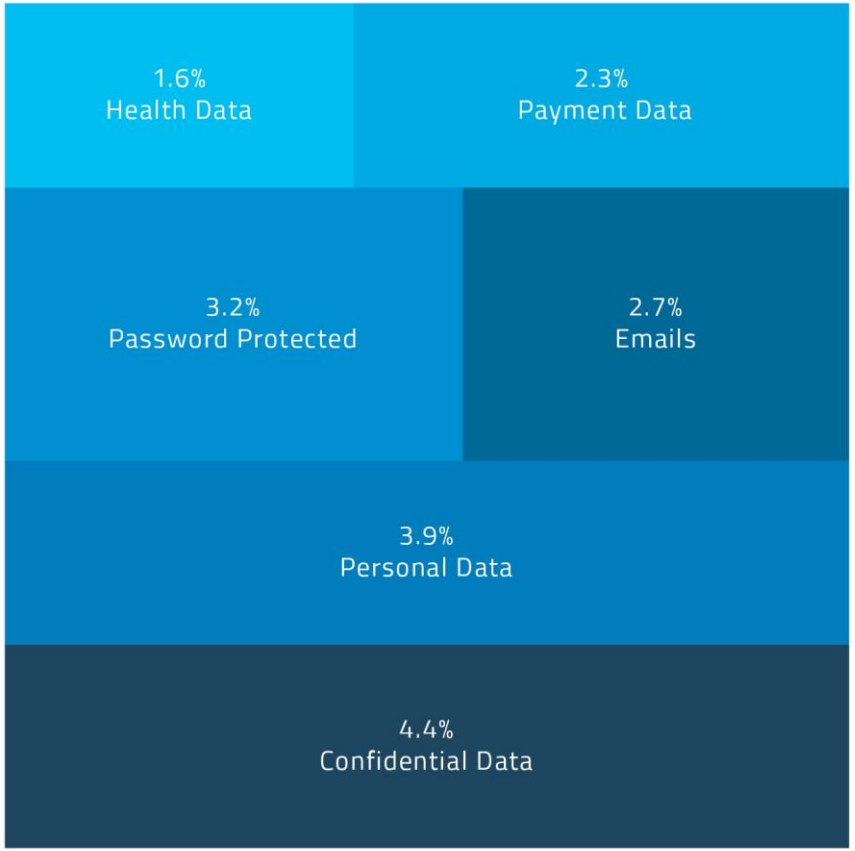
30+ million users

78 countries worldwide

20,000+ cloud services analyzed

18.1% of files in the Cloud contain Sensitive Data





Perform DLP for Data Uploaded to or Created in the Cloud

aetna℠

Ensure compliance with healthcare regulatory requirements within O365, Box, and Salesforce

- Uniform policies across cloud services
- Policies based on keywords, data identifiers, IDM, EDM
- Multi-tier remediation based on severity

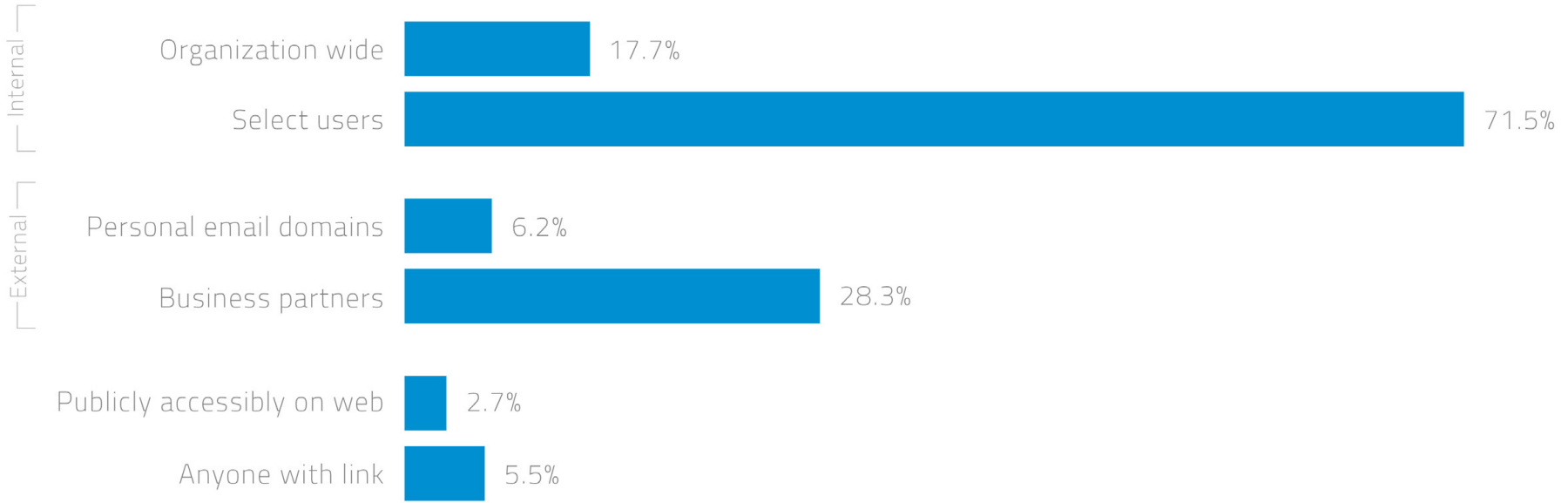
Manage Personal Data to Conform to GDPR & Other Privacy Regulations

European Financial Institution

Ensure compliance with GDPR & 50+ country banking regulations within multiple cloud services

- Uniform policies across cloud services
- Policies based on fingerprinting, user behavioral analysis and modern DLP
- Block link sharing to unapproved domains

34.5% of Documents in Cloud are Shared Externally



Build Guardrails for Cloud Collaboration

AstraZeneca

Enable collaboration while preventing unauthorized sharing in Office 365 & Box

- Eliminate sharing to personal emails or via open links
- Create whitelist of valid business partner email domains
- Layer content into policies via DLP engine

The Average User Connects to Enterprise Cloud Services from 2.8 Devices

2.8 Devices

Prevent Data Loss due to usage of Personal Devices

Enable BYOD while preventing data loss from Salesforce, ServiceNow, O365, Box, and Google via lost or stolen devices

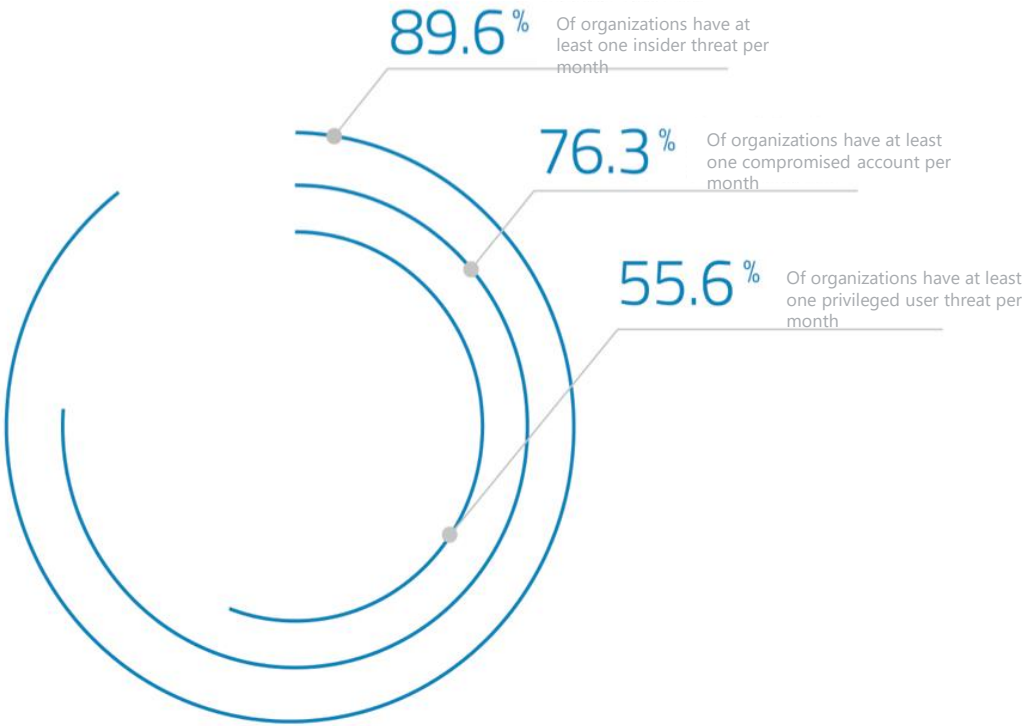
- Check for device certificate, confirm user/device mapping
- Limit access based on device or location
- Block access or limit to view-only

The Average Enterprise Experiences 17 Cloud Threats Per Month

9.3 Insider threat anomalies per month

5.1 Compromised accounts anomalies per month

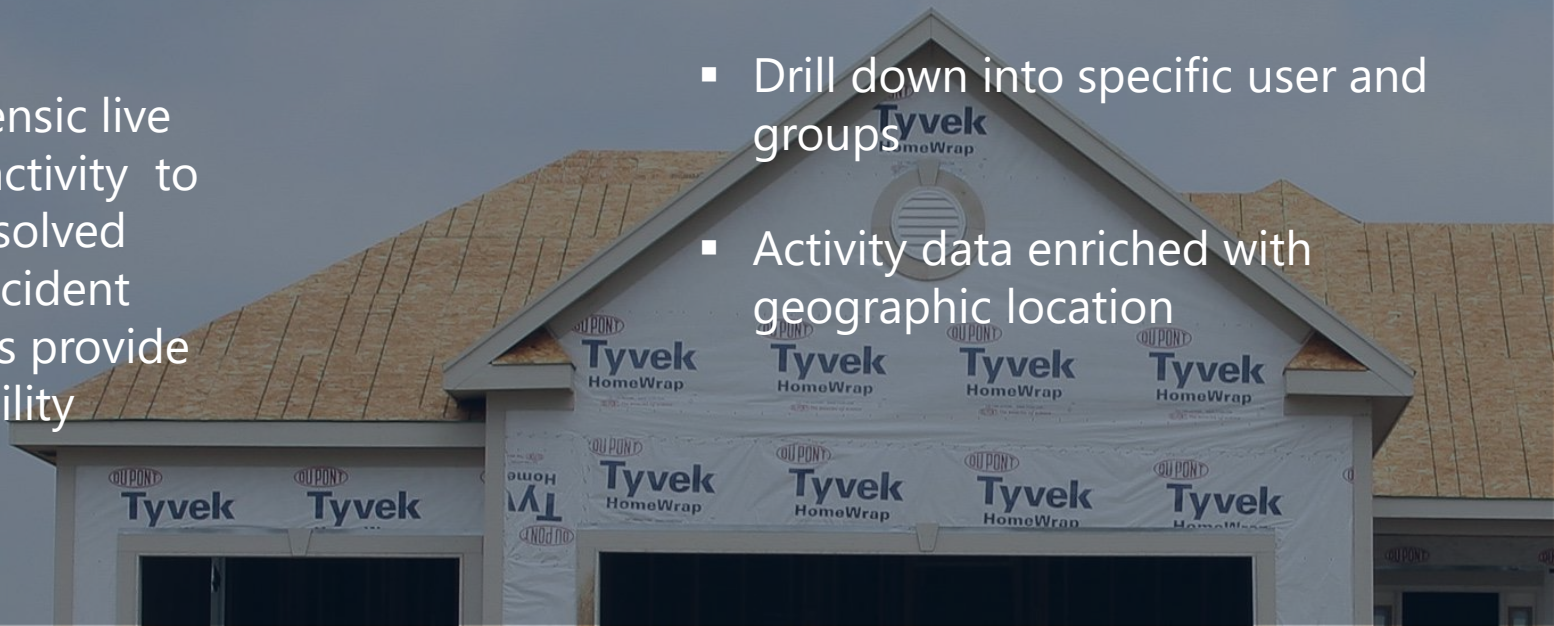
2.8 Privileged user threats anomalies per month



Support Investigations by Tracking all Activity within Sanctioned Cloud Services

Created forensic live log of O365 activity to quickly resolved security incident investigations provide auditability

- Activities organized into 13 categories for easy navigation
- Drill down into specific user and groups
- Activity data enriched with geographic location

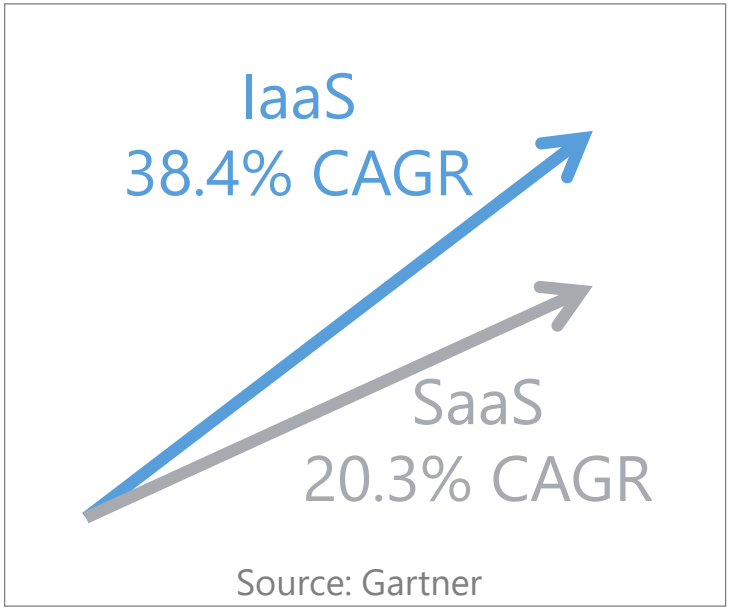


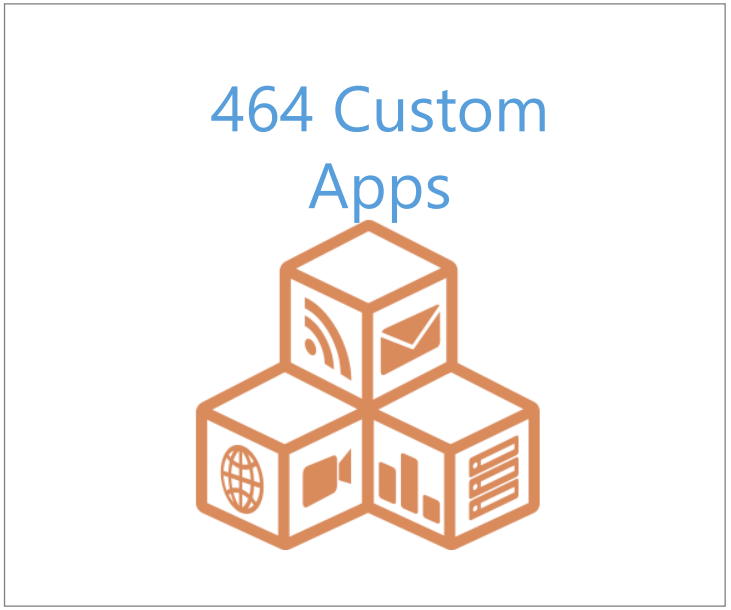
Protect Against Threats to Cloud Data

Prevented data loss from Salesforce, Box, and O365 due to compromised accounts, insider threats and privileged user threats

- Analyze usage across multiple cloud services
- Leverage UEBA to identify threats without pre-defined policies or thresholds
- Adjust sensitivity with real-time preview

IaaS and Custom Apps Fastest Growing Segment of Cloud





Extend Protection from SaaS to Custom Apps and IaaS

BlueCross BlueShield

- Eliminated AWS security vulnerabilities and wrapped custom apps with DLP and activity monitoring

- Leveraged AI to map custom applications
- Extended DLP from SaaS to custom apps
- Audited and remediated AWS security configurations

One SaaS Example – Risk or No Risk?

6.2 Licenses you grant to Prezi for use of Public User Content and Private User Content

back to top

In order to provide the Service to you in accordance with these terms, we need certain licenses from you in order for us to, e.g., host, store and display the content. For example, we need the right to publicly display/perform the work to allow us to display it on the computer monitor of any party who is not the copyright holder. We need the right to reproduce the content so that it can be saved to our servers. We need to create derivative works and modify the content, for example, when transcoding an uploaded image into a format that will work most efficiently with the Service.

With respect to Private User Content, you hereby do and shall grant to Prezi (and its successors, assigns, and third party service providers) a worldwide, non-exclusive, revocable, royalty-free, fully paid, sublicensable, and transferable license to use, host, store, reproduce, modify, create derivative works, communicate, publish, publicly perform, publicly display, distribute and transmit the content SOLELY FOR THE PURPOSE of providing you, and those with whom you have shared your presentations, with the Service. This license ends when you delete your Private User Content or your account is closed (either by you or by us), except (i) to the extent that your Private User Content has been shared with others and they have not deleted it and (ii) that we retain a license to maintain a back-up copy of your Private User Content indefinitely.

With respect to Public User Content, you hereby do and shall grant to Prezi (and its successors, assigns, and third party service providers) a worldwide, non-exclusive, revocable, royalty-free, fully paid, sublicensable, and transferable license to use, host, store, reproduce, modify, create derivative works, communicate, publish, publicly perform, publicly display, distribute and transmit the content (1) for the purpose of providing you, and those with whom you have shared your presentations (including the public), with the Service; and (2) in connection with promotion and marketing of Prezi products and services, including without limitation allowing third parties to search or index the content, in connection with email promotions, product demonstrations, and the like. This license ends when you delete your Public User Content or your account is closed (either by you or by us), except (i) to the extent that your Public User Content has been shared with others and they have not deleted it and (ii) that we retain a license to maintain a back-up copy of your Public User Content indefinitely.

Regardless of whether you designate content public or private, Prezi makes no claim of ownership to your User Content, and obtains no rights to your content other than as provided for herein.

Q & A