Myths of Cloud Security Debunked

Michael Sutton
CISO

Agenda

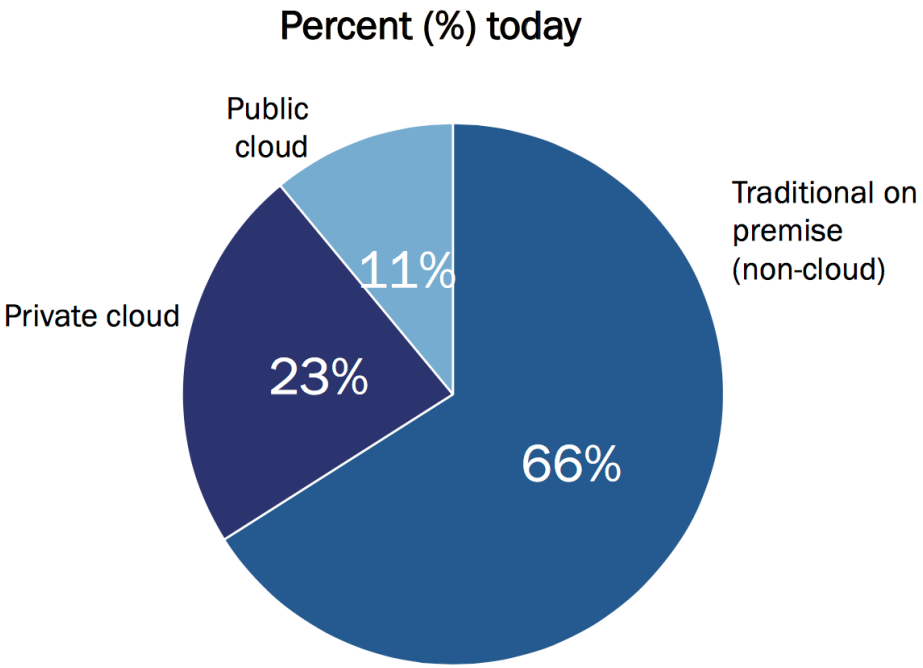
- Myths – Debunking the top 10 cloud security myths
- Zscaler – Security-as-a-Serivice

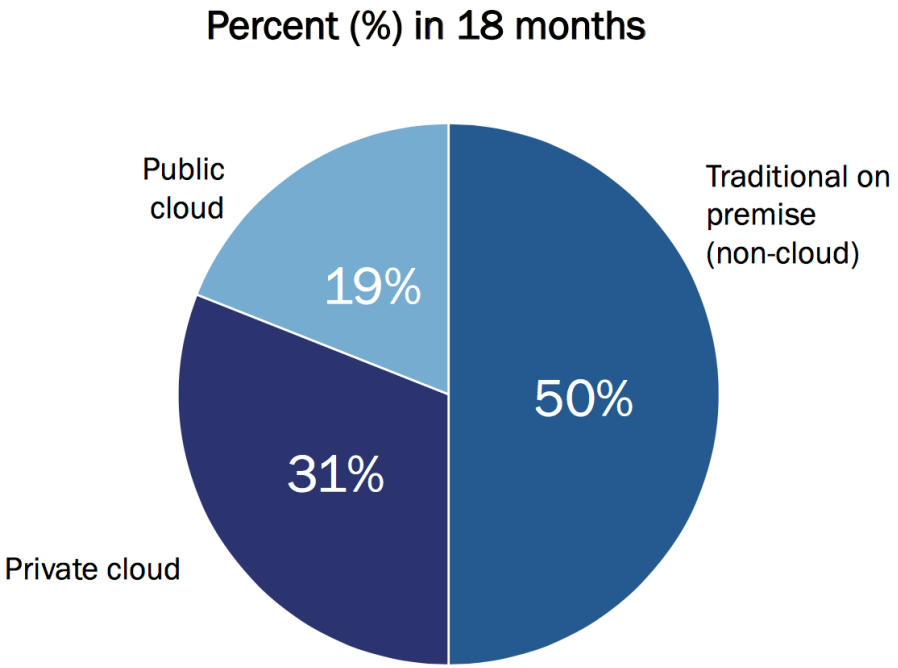
"Cloud computing, by its very nature, is uniquely vulnerable to the risks of myths. It is all about capabilities delivered as a service, with a clear boundary between the provider of the service and the consumer. From a consumer perspective, 'in the cloud' means where the magic happens, where the implementation details are supposed to be hidden. So it should be no surprise that such an environment is rife with myths and misunderstandings."

- David Mitchell Smith, VP and Gartner Fellow

Should I Trust the Cloud?

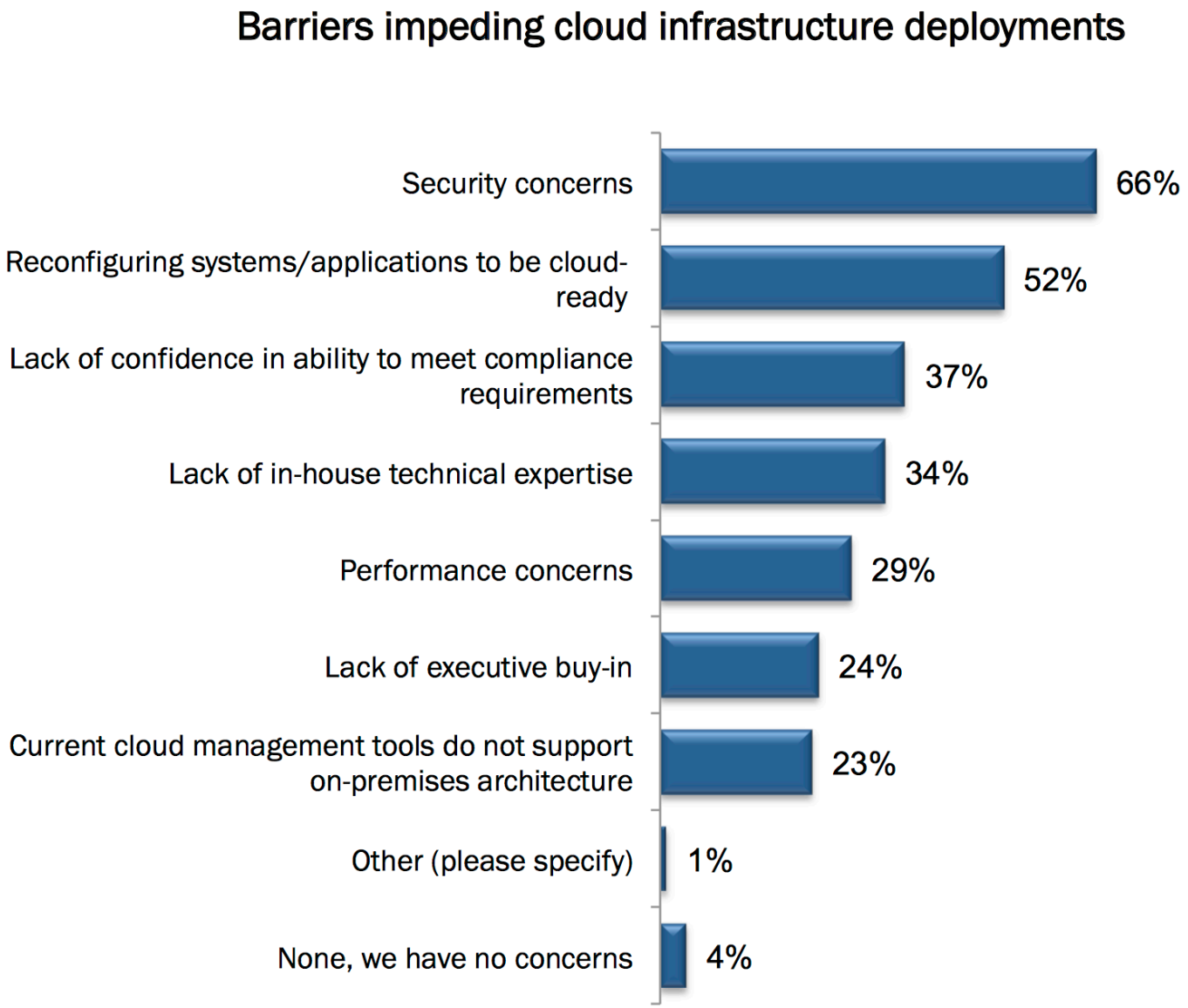
Percentage of your organization's customer data currently that resides on premise versus in the cloud





https://www.cloudpassage.com/assets/img/resources/cso-cloud-security-concerns-and-the-perceived-effectiveness-of-traditional-security-solutions-in-a-cloud-environment.pdf

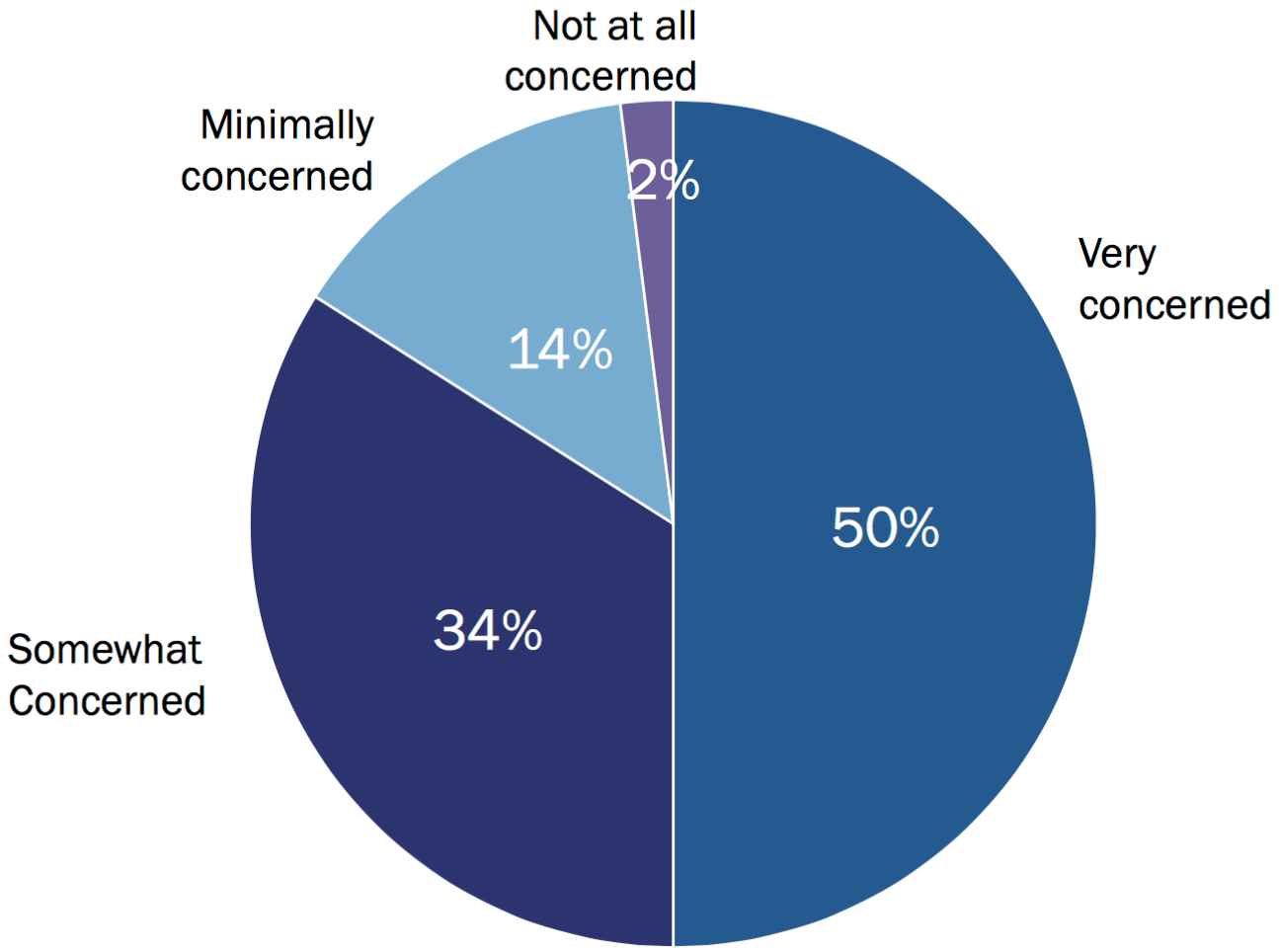
Should I Trust the Cloud?



https://www.cloudpassage.com/assets/img/resources/cso-cloud-security-concerns-and-the-perceived-effectiveness-of-traditional-security-solutions-in-a-cloud-environment.pdf

Should I Trust the Cloud?

Concern with security of customer data residing in the public cloud



https://www.cloudpassage.com/assets/img/resources/cso-cloud-security-concerns-and-the-perceived-effectiveness-of-traditional-security-solutions-in-a-cloud-environment.pdf

Myth 1: We don’t really use the cloud

- Shadow IT is an unstoppable force for most enterprises
- Visibility is a challenge, much less control
- Consumerization of IT has pushed personal cloud apps to the enterprise
- Traditional enterprise apps are moving to the cloud (Office365)
- Saying ‘no’ is no longer viable. IT must shift from ‘Block or Allow’ to ‘‘Manage and Monitor’.
- Learn from your network data to better understand employee behavior and work to implement solutions that maintain productivity by permitting the use of desired resources in a manner that doesn't expose the company to unnecessary risk

Myth 2: I lose control of my data when it goes to the cloud

- Control should not be tied to platform or location
- Data residency and retention can and should be under enterprise control when necessary
- Data portability should be a requirement, as data should remain under corporate ownership and remain accessible
- Data storage practices must conform to regulatory compliance measures
- Determine the level of control over data that is required, regardless of solution and identify cloud vendors that can meet your needs

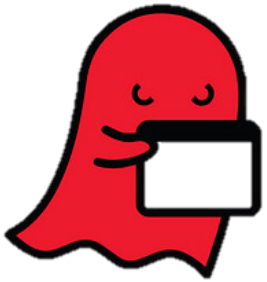
Myth 3: Cloud is less secure than on-premise solutions

- Vast majority of recent data breaches involve data stored on local systems
- Location has little to do with security – people, process and technology will determine security regardless of location
- Cloud providers benefit from economies of scale when securing data
- "Cloud computing is perceived as less secure. This is more of a trust issue than based on any reasonable analysis of actual security capabilities. To date, there have been very few security breaches in the public cloud — most breaches continue to involve on-premises data center environments"

Myth 4: I'm at the mercy of cloud vendors for patching

Heartbleed

POODLE



Ghost

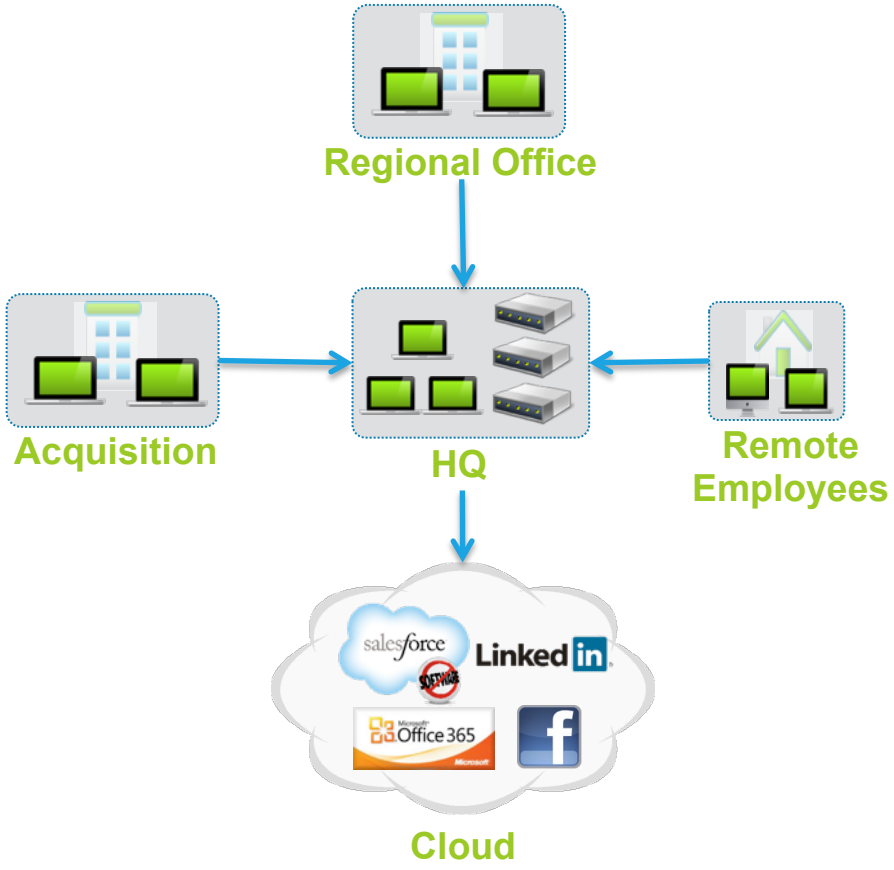
VENOM

FREAK

Shellshock

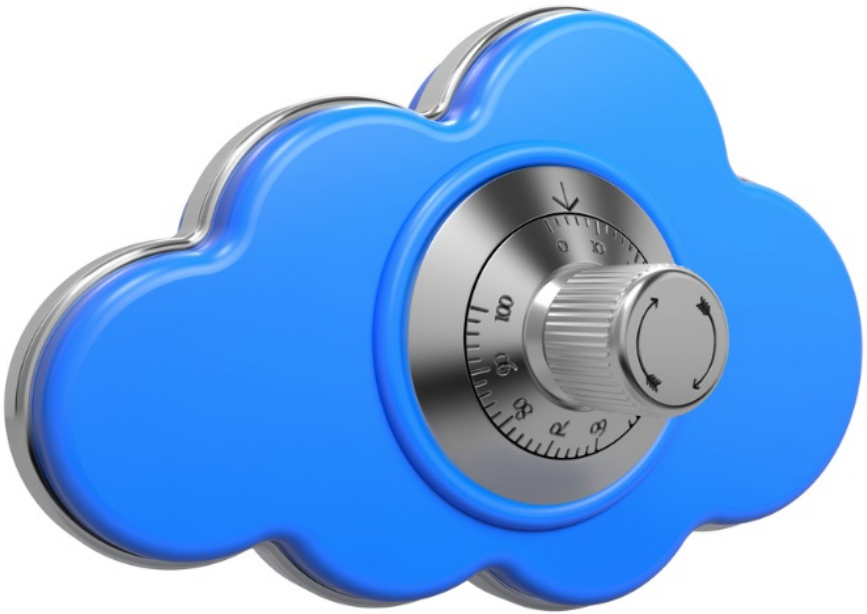
- Software/hardware vendors must also provide patches…but it's your responsibility to apply them
- Open source libraries commonly used in security appliances
- Patching can be costly and time consuming
- Functionality upgrades also force patching
- Cloud vendors have incentive to expedite patching efforts

Myth 5: Appliances provide greater control over scalability/performance



- Appliances require planning for anticipated demand, while the cloud permits paying for actual consumption
- Cloud elasticity places the burden of resource planning with the vendor
- Sudden growth (acquisitions, mergers, etc.) does not necessitate major architectural changes
- Appliance scalability will be impacted by features utilized
- Appliances can only protect what they can see
- Scaling appliances can add complexity to the overall architecture (i.e. load balancers, reporting engines, log aggregators, etc.)

Myth 6: Cloud security is more difficult to manage



- Policies and reporting for numerous locations and remote employees can be managed via a single, web based console
- The heavy lifting required for data consolidation is handled by the vendor
- Data portability ensures that the cloud isn't a silo and interacts with alternate security workflows
- Patching and upgrades are handled by the cloud vendor
- Adding new capabilities is a matter of enabling features as opposed to rearchitecting
- Customers can focus on leveraging as opposed to maintaining solutions

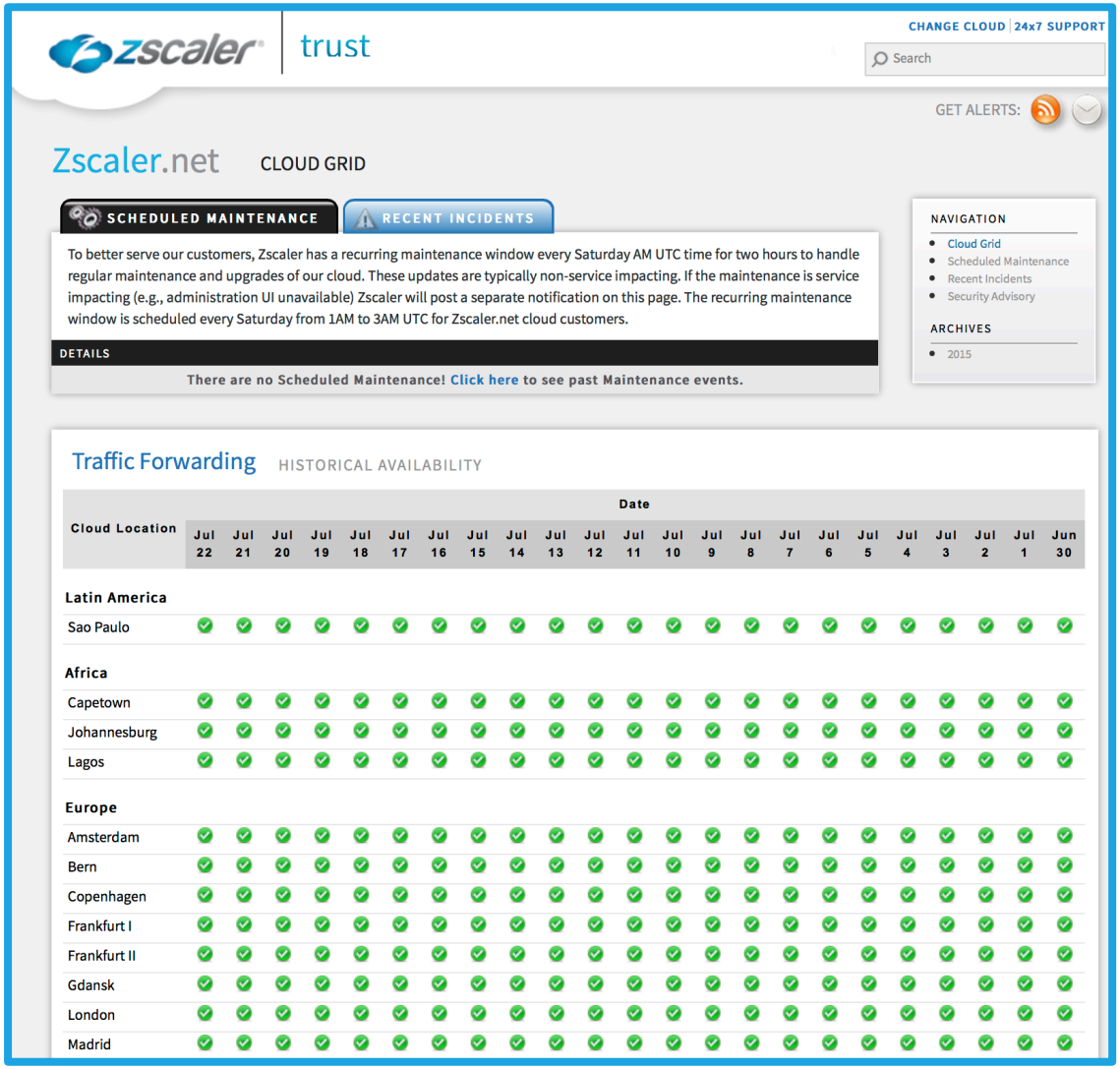
Myth 7: Cloud resources are more exposed to attack

- This myth ignores insider threats
- Even custom enterprise applications are typically Internet facing to accommodate remote users
- Local solutions are less likely to implement strong data security and monitoring
- Enterprises often implement split tunnel VPNs to permit access to internal applications, exposing additional threats
- Cloud infrastructure is typically far more resilient in the face of a DDoS attack
- Economies of scale allow cloud vendors to invest in security people/processes/ technologies

Myth 8: Multi-Tenant Clouds Expose Privacy Concerns

- Hypervisor vulnerabilities are rare and successful attacks are even more so
- Management interface should be isolated from customer resources
- Customer data should be properly encrypted/encoded to further limit privacy threats – this is far less likely in a proprietary, on premise app

Myth 9: Cloud vendors lack transparency



- Consumers of cloud security must demand transparency through online resources (e.g. trust.salesforce.com), SLAs, open policies/procedures and third party attestation
- It is the responsibility of the consumer to ensure that the cloud vendor provides an overall security posture that meets/exceeds the on-premise security posture
- Compliance does not equal security – it forms a baseline, but is not an endgame – customers must ask the right questions
- Not all clouds are equal

Myth 10: Appliances are more reliable than the cloud

- Most enterprises are not in the business of enterprise security or developing/ maintaining IT solutions, which remain cost centers
- Cloud security vendors benefit from *economies of scale* and can afford to invest in world class security, development and operations teams and resources
- Cloud vendors live and die by their reputation
- How many appliances offer reliability/ uptime SLAs?
- Cloud solutions reduce complexity, which works in opposition to security

Zscaler

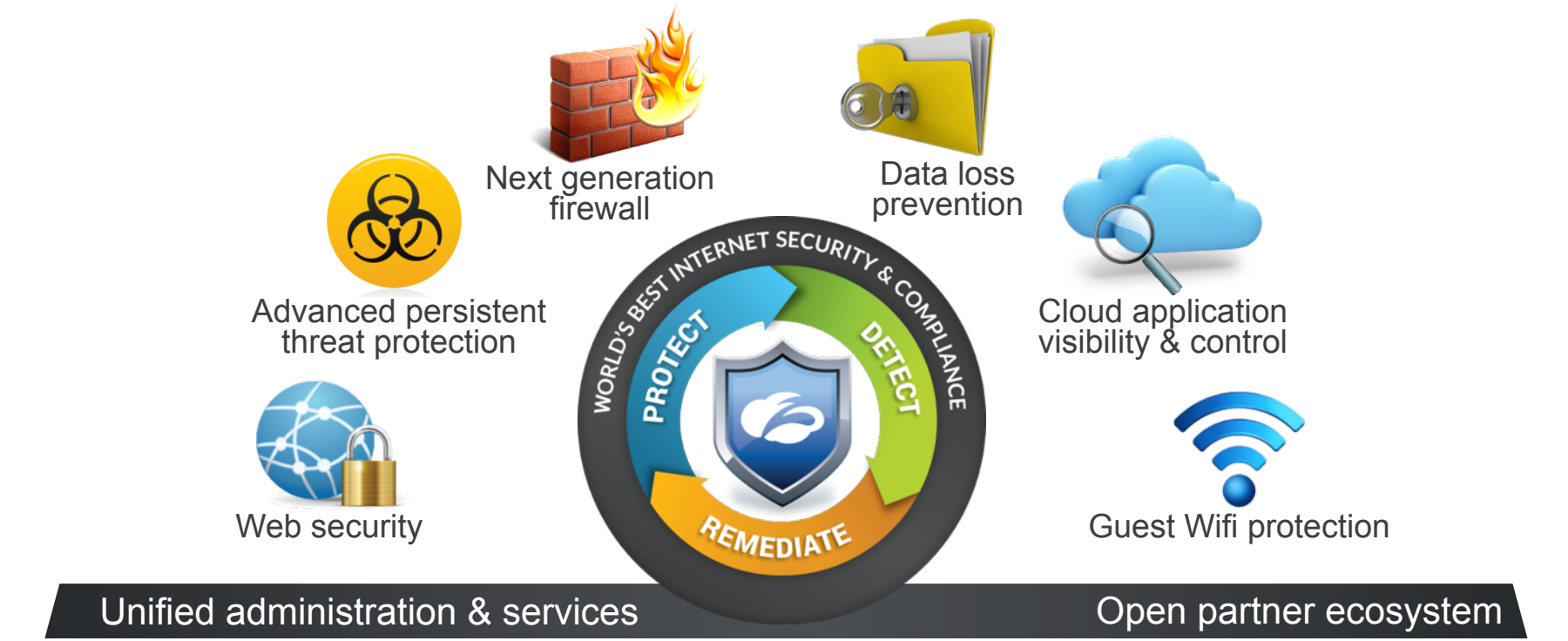
The industry's leading Security-as-a-Service platform

Enter Zscaler: Internet Security and Compliance *everywhere* – delivered via cloud computing

Zscaler Data Centers: The World's Largest Security Cloud

100% reliability, complete redundancy, massive bandwidth
Automatic connection to closest node, policy follows the user
24x7x365 follow the sun operations

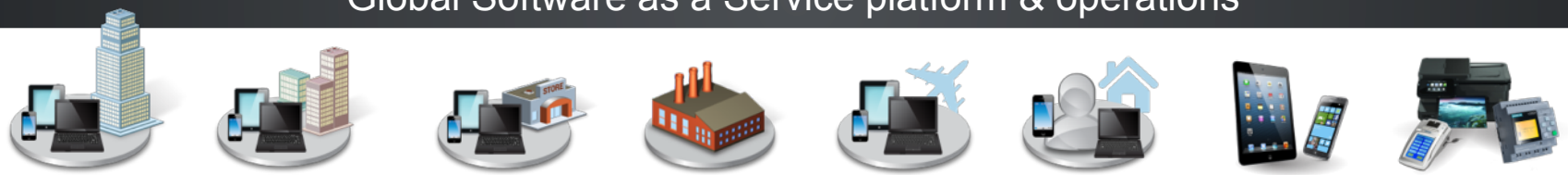
Zscaler is a comprehensive, unified *Internet Security and Compliance* platform



Unified administration & services | Open partner ecosystem

Policy management | SSL inspection | Bandwidth control | Reporting & analytics

Global Software as a Service platform & operations



Better security, everywhere, with much lower cost of ownership

Consider Three Users…

	Office	Coffee Shop	Airport
Device	PC	Laptop	Tablet/ smartphone
Protection	IDS, IPS, FW, SWG, DLP, etc.	Host based AV and firewall	Nothing
Visibility	Location based reporting	Nothing	Nothing

- *We must seek security solutions that ensure consistent policy, protection and visibility, regardless of device or location.*
- Cloud provides the opportunity to level the playing field.

Thank you

Michael Sutton
CISO
@michaelawsutton