Virginia Information Technologies Agency

Welcome and Opening Remarks

Mike Watson

May 6, 2020

May ISOAG Agenda

Mike Watson, Opening and Welcome Remarks

Steve Orrin, Intel

Blake Carpenter, Grant Thornton, LLP

Shana Sumpter, University of Richmond

Demetrias Rogers, VITA

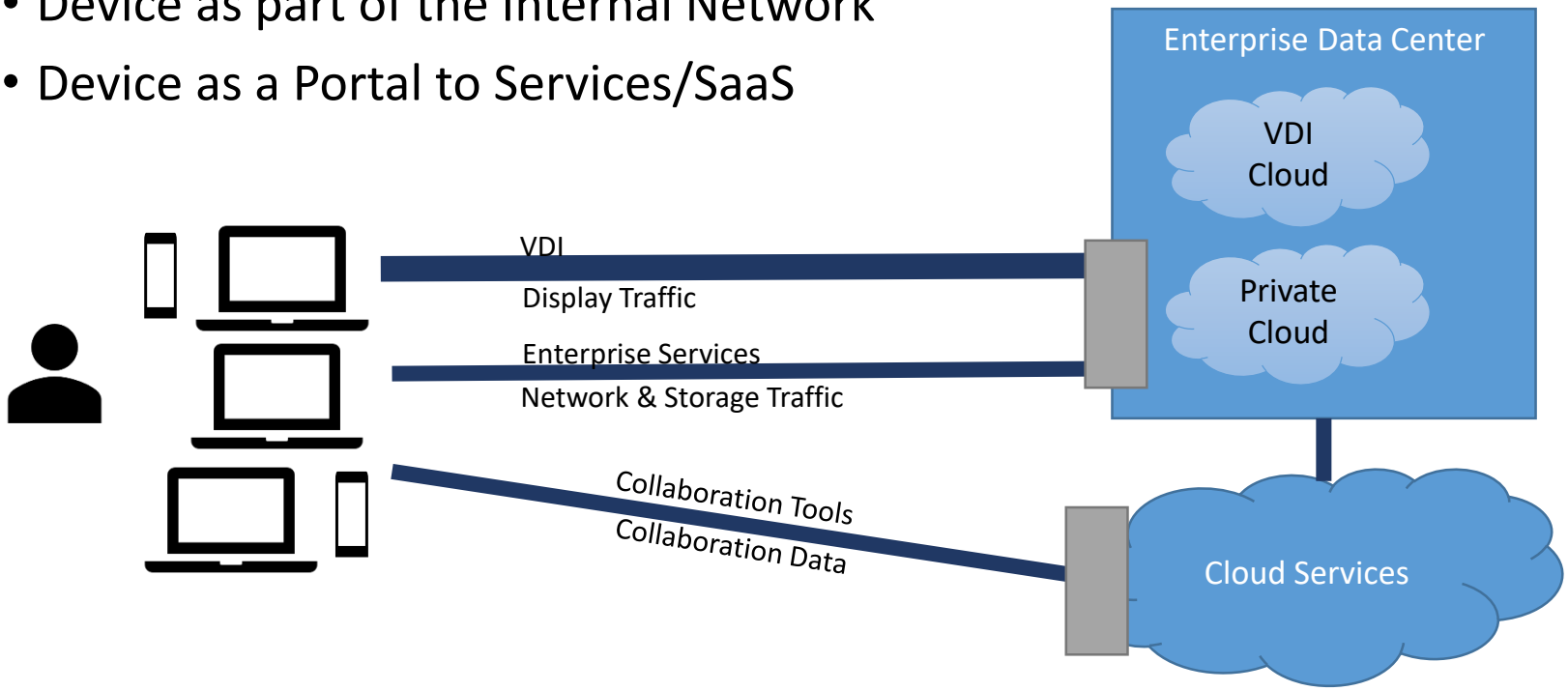
Securing Telework

EMBRACING DIGITAL TRANSFORMATION

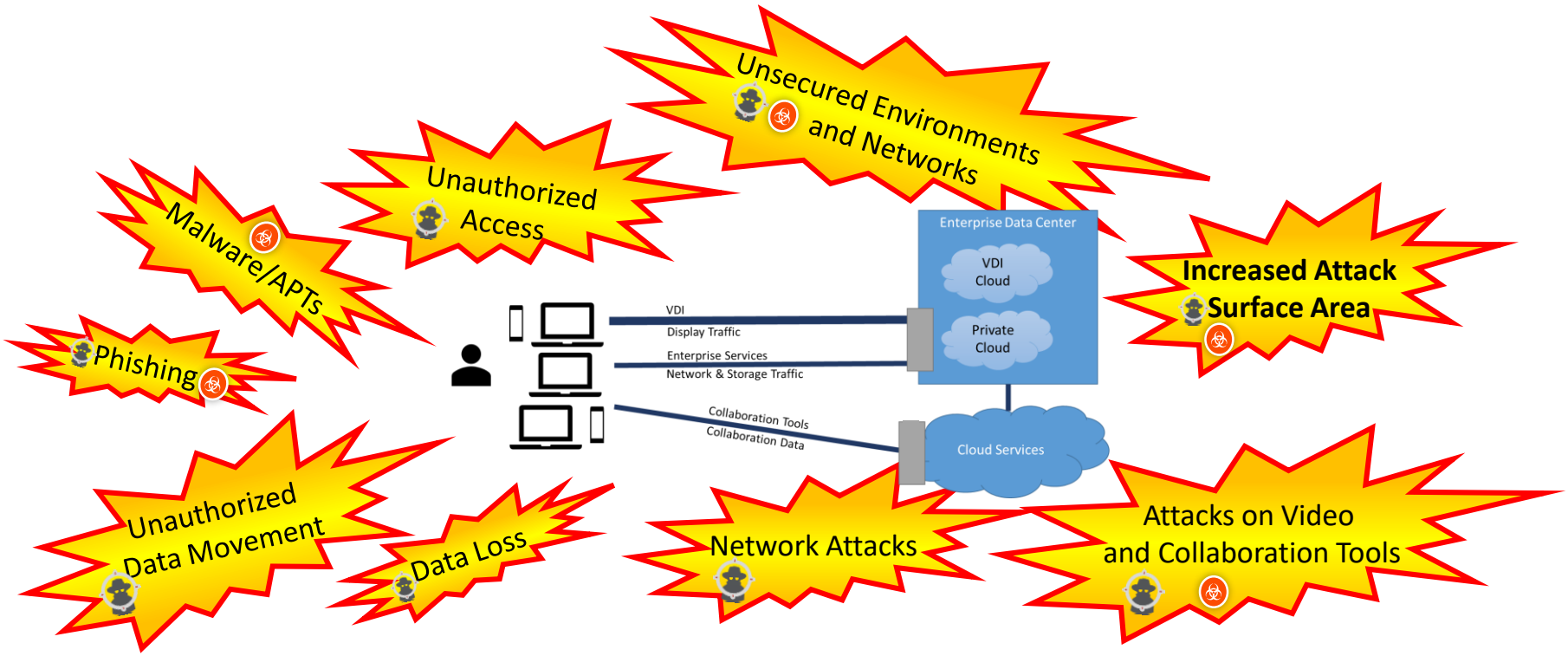
Steve Orrin
Federal CTO, Intel Corp

Teleworker Modes of Operation

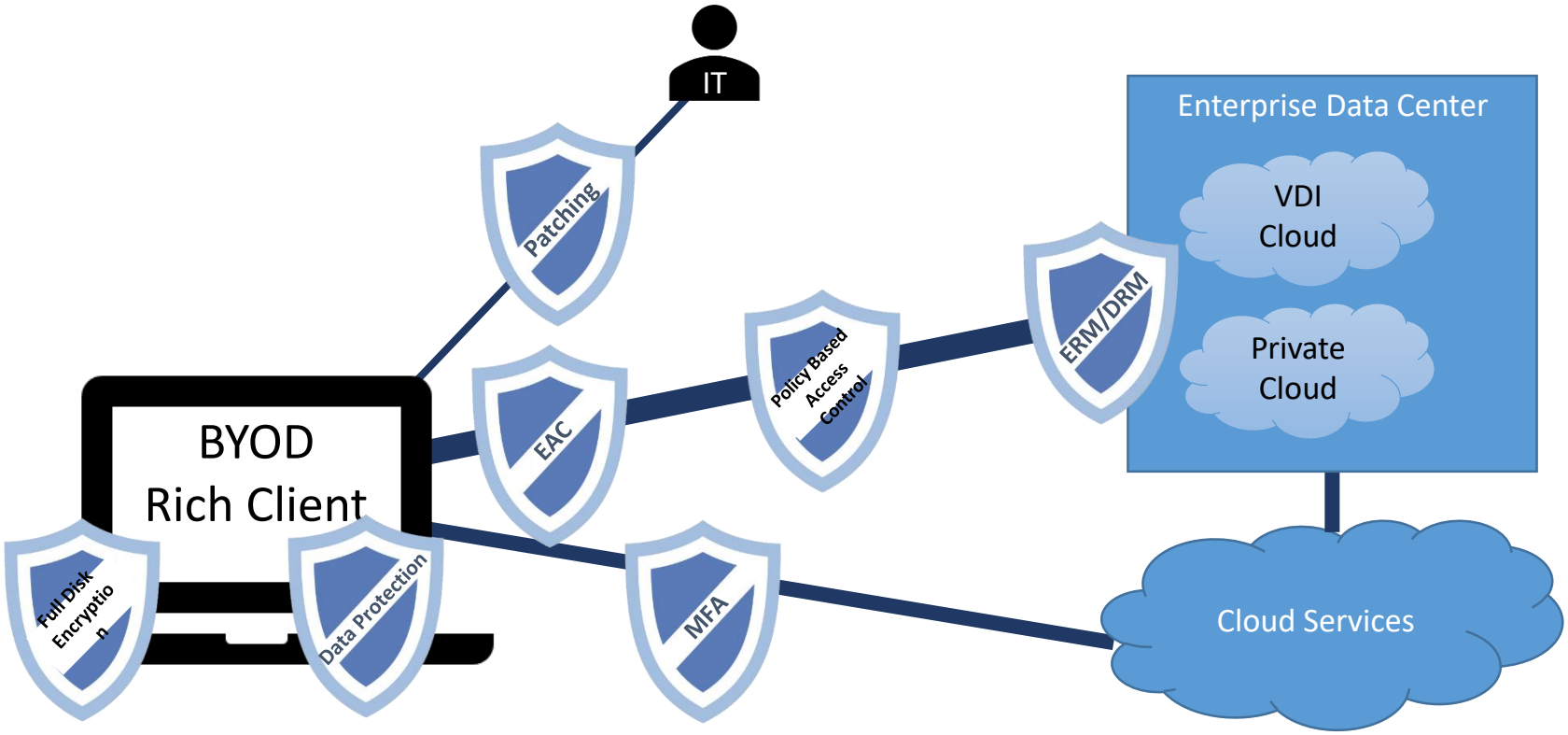
- Device as a Terminal (VDI)
- Device as part of the Internal Network
- Device as a Portal to Services/SaaS



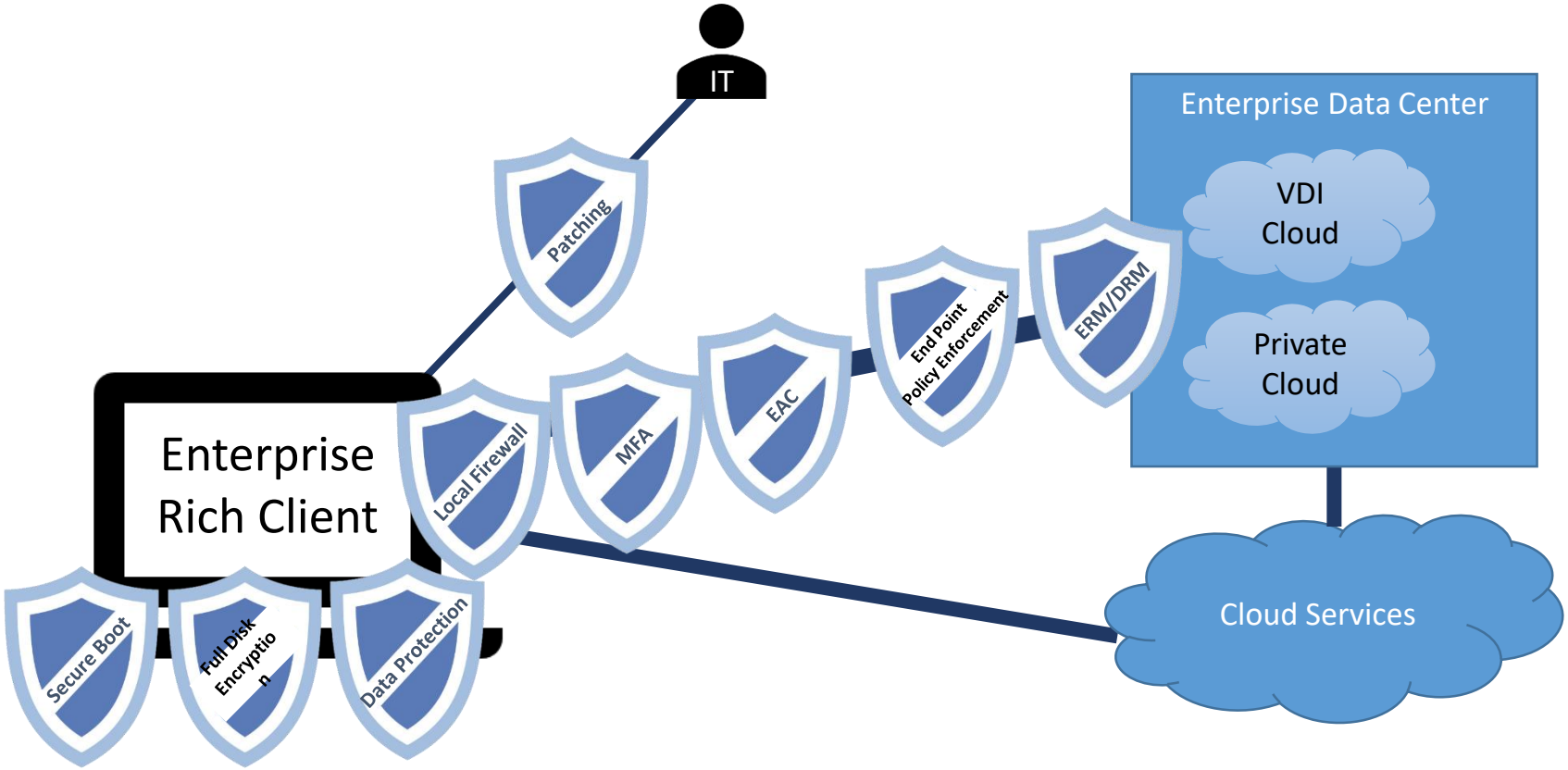
Threats to Teleworking



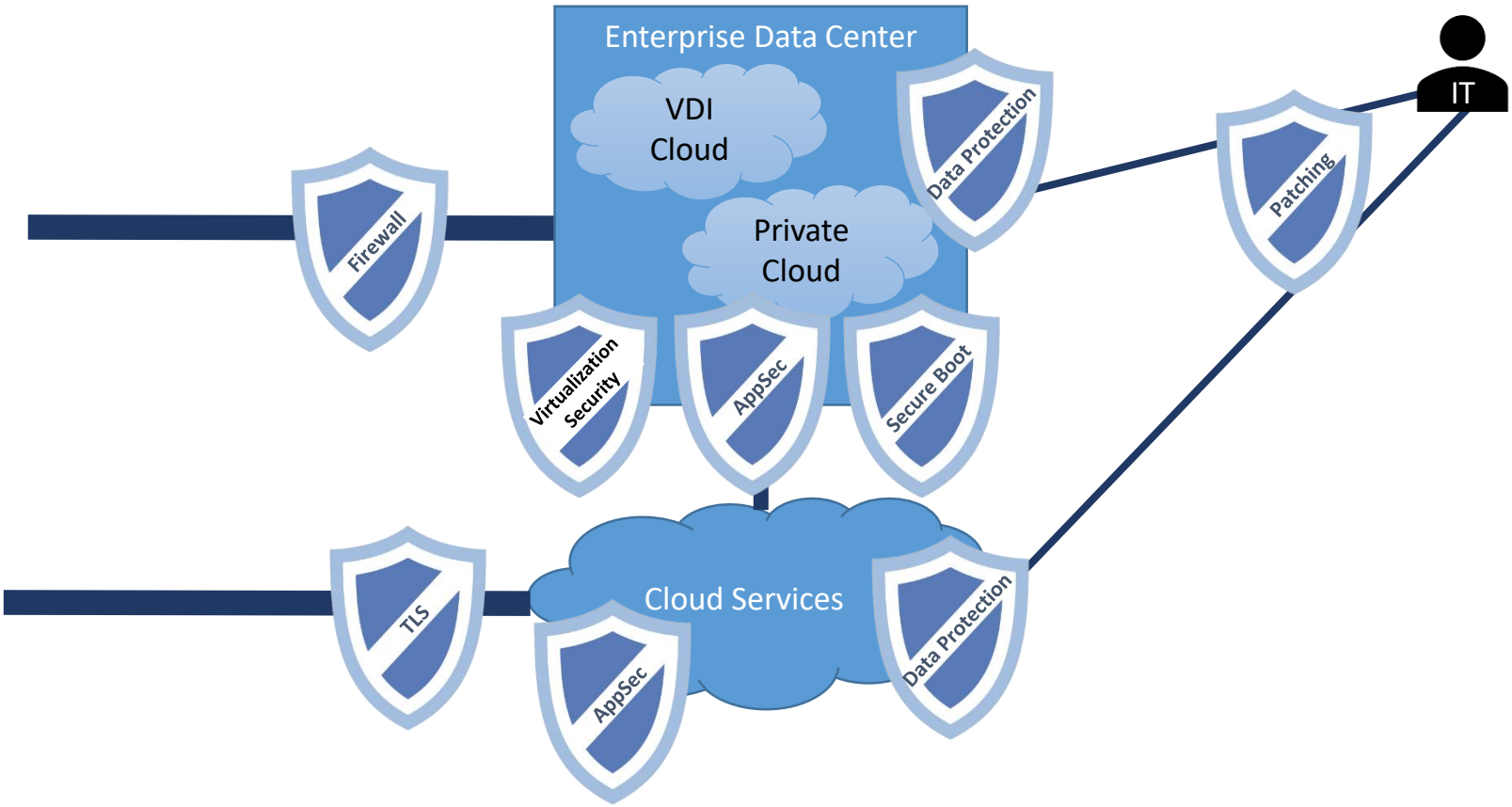
Solutions for Securing the Teleworker
BYOD



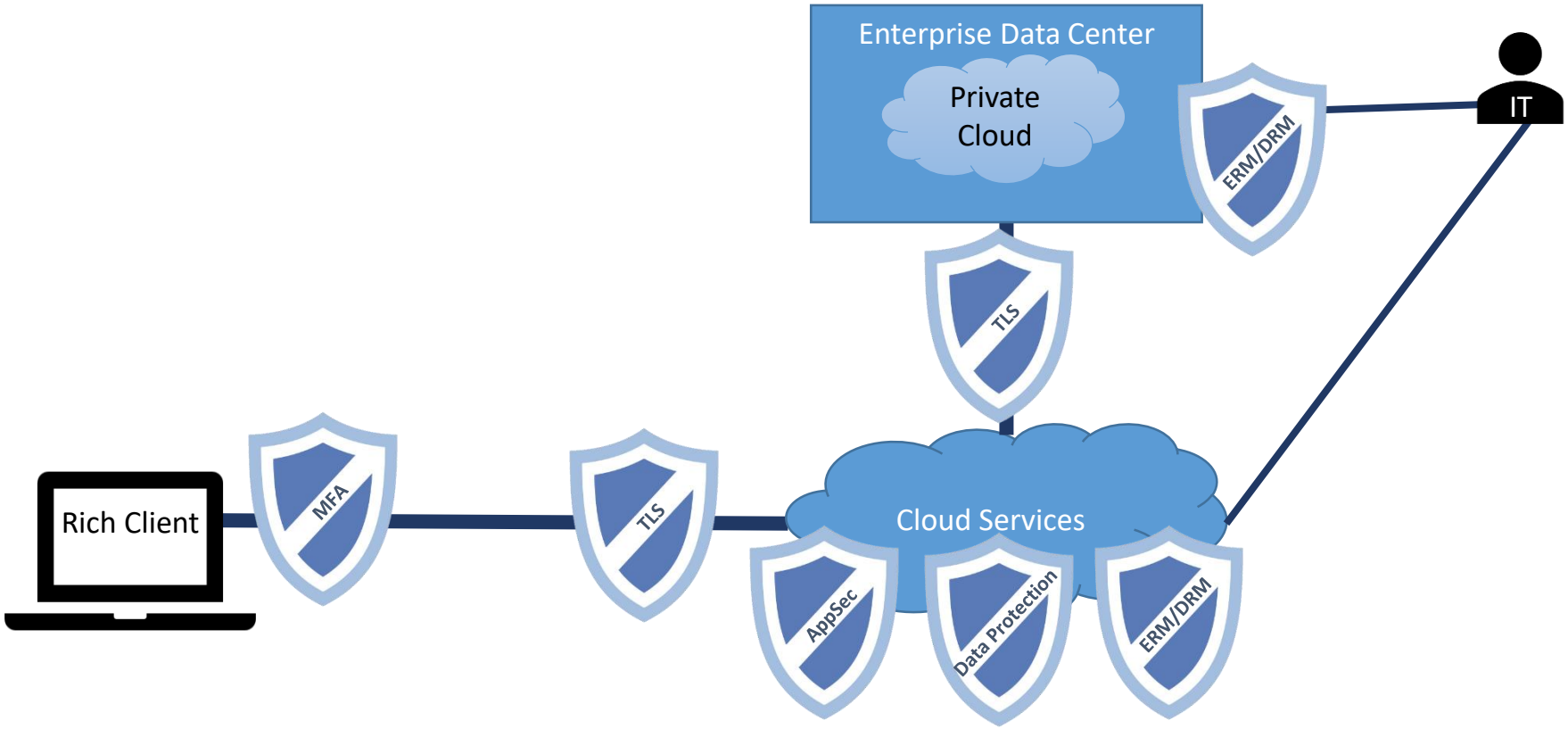
Solutions for Securing the Teleworker
End Points in unsecured environments and networks



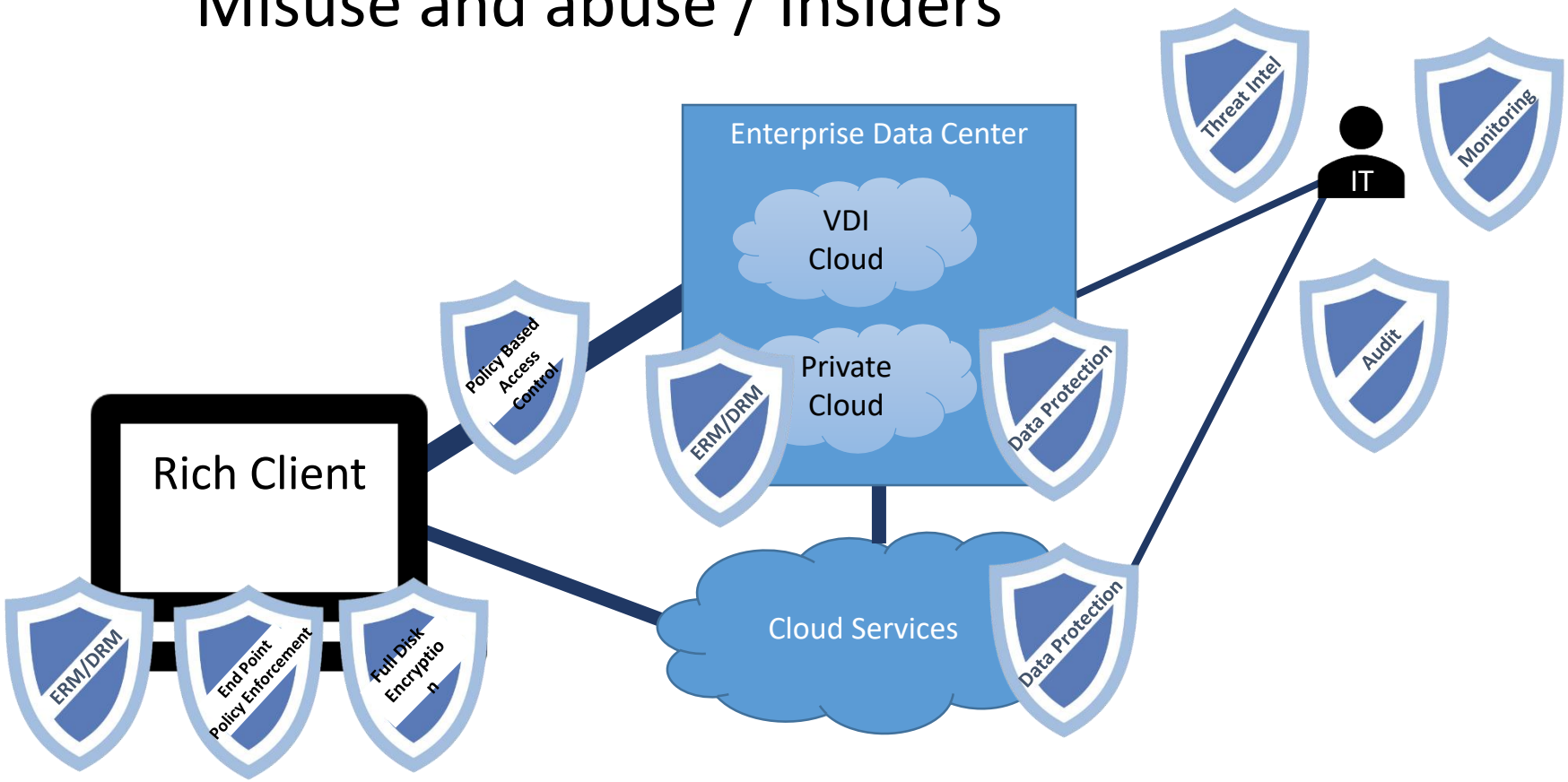
Solutions for Securing the Teleworker VDI Systems and Cloud Services



Solutions for Securing the Teleworker As-a-Service clients



Solutions for Securing the Teleworker
Misuse and abuse / Insiders



What can I do Today/ Tomorrow

- Short-term
  - Educate employees
    - Home Security Guidance
    - Security Training for Telework
  - Push Patches and Require Users to Patch their devices
  - If you have it, turn on EAC, ERM/DRM and DLP
  - Turn on and enforce TLS for your web connections
  - Implement Personal Device based 2FA for accessing your resources and content (Enterprise and Cloud)
  - Make sure End Point Security Agents are enabled and up to date
  - Manage and enforce security policies for the different types of User Devices
  - Enable Full disk encryption
- Long-term
  - Establish zero trust best practices
  - Implement MFA with physical devices and other factors
  - Use ERM and Policy Based Data Access methodologies
  - Implement Deep Stack security Solutions
    - Secure Boot With Attestation
    - Virtualization and Container Security
    - Firmware Security and Monitoring
  - Extend Audit, Threat Intelligence and Monitoring to Teleworker environments
  - Extend enterprise security to the teleworker locations
    - Managed Devices, Managed Networks

Recommendations for Securing the Home Office

- System Security Tips
  - Update your systems (Windows Update, Mac Update, Phone updates, etc.)
  - Update your End Point Security Software and Run regular scans
  - Turn on and use Local FW and Enable the router and modem firewall
    - Set QoS Settings to allow high bandwidth apps like Video Conferencing priority
  - Reduce Runtime Surface area of attack
    - Close apps that are not in use
    - Close browser before going to new/ different sites
    - Logout of/close secure sessions before checking email or browsing

- Modem/Router/WiFi Security Tips
  - Change the default administrative password of all routers and modems to something unique
  - Use a unique password to access your ISP's web portal
  - Enable two-factor authentication wherever possible.
  - Change the WiFi network name (i.e., SSID) password to something unique and Ensure the WiFi network (i.e., SSID) name does not provide any identifying information
  - Carefully guard who has knowledge of the WiFi network password
  - Enable automatic updates for all routers and modems
  - Turn on WPA2 or WPA3
  - Disable WPS if possible
  - Enable network address translation (NAT)
  - Enable DNS filtering on the router and/or modem
  - Disable UPnP

STOP. THINK. CONNECT.
https://www.stopthinkconnect.org/


Backup

Intel Client Technologies for Securing the Teleworker

INTEL® HARDWARE SHIELD SECURITY CAPABILITIES

BIOS — *Helps prevent malicious software injection by locking down the memory in the BIOS*

Boot Flow — *Helps dynamically ensure OS and virtual environment are running directly on Intel® hardware*

OS Visibility — *Unique OS visibility of how BIOS is using hardware (proves BIOS is behaving correctly)*

PROTECTED DATA WITHOUT COMPROMISING PRODUCTIVITY

INTEL'S HARDWARE-ACCELERATED ENCRYPTION/DECRYPTION

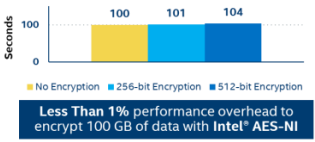
Intel® SHA Extensions — New instructions to accelerate the cryptographic Secure Hash Algorithm (SHA) variants SHA-1 and SHA-256

AES-2X — Similar to AES-NI, the SHA-NI is a family of instructions designed to improve performance and efficiency of SHA on x86

VPMADD52 — AES-2X is microarchitectural improvements that doubles the throughput of the AES engine and AES-NI

VPMADD52 is a 52-bit wide vector multiply and add instruction that is useful for public key cryptographic operation

...coming on Whitley



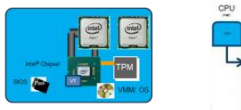
Less Than 1% performance overhead to encrypt 100 GB of data with **Intel® AES-NI**

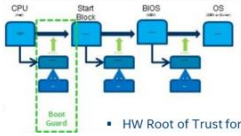
...built into the processor, or massively scale up with Intel® Quick Assist Technolo...

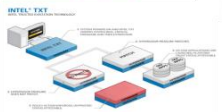
SECURE BOOT

Intel® Trusted Execution Technology (TXT) and Intel® BootGuard (BtG)

Trusted Execution Technology BootGuard





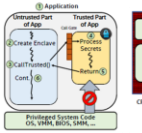


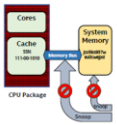
- HW Root of Trust for Secure Boot
- Verified boot or Verified & Measured Boot options
- Ability to use TPM
- Ability to extend chain of trust all the way to Hypervisor and VMs

INTEL® SOFTWARE GUARD EXTENSIONS (SGX)

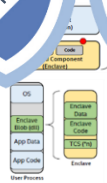
Protected execution environment embedded in a process

- With its own code and data
- Providing Confidentiality & Integrity
- Controlled entry points
- Multi-thread support
- Full access to app memory and processor performance





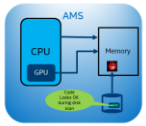
- Security perimeter is the CPU package boundary
- Data and code unencrypted inside CPU package
- Data and code outside CPU package is encrypted and integrity checked
- External memory reads and bus snoops see only encrypted data



INTEL® THREAT DETECTION TECHNOLOGY

Architecture – Exploit Detection

- **Intel TDT: Advanced platform telem...**
  - Use platform telemetry to detect ... exploits in re... CPUs
  - Applicable to Client and Server platforms.
  - Can also be use distinct indicators from platform telemetry to orchestrate the detection of an ongoing attack



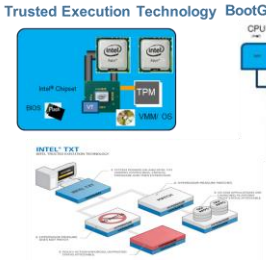
- **Intel TDT: Accelerated Memory Scanning (AMS)**
  - Malware Detection via Memory scanning
  - AMS enables offload of memory scanning to the integrated GPU
  - Detects advanced memory & 0-day attacks + leverages GPU to provide a much higher scanning capacity leading to higher efficacy

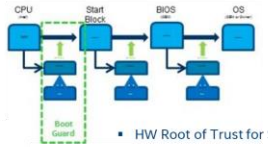
Hardware-assisted anti-malware solution focused on attacks which are hard to detect with software-only solution such as 0-day and advanced memory attacks

Intel Datacenter Technologies for Securing the Teleworker

SECURE BOOT

Intel® Trusted Execution Technology (TXT) and Intel® BootGuard (BtG)





- HW Root of Trust for Secure Boot
- Verified boot or Verified & Measured Boot options
- Ability to use TPM
- Ability to extend chain of trust all the way to Hypervisor and VMs

Virtualization Security

Secure Boot

PROTECTED DATA WITHOUT COMPROMISING PRODUCTIVITY

INTEL'S HARDWARE-ACCELERATED ENCRYPTION/DECRYPTION

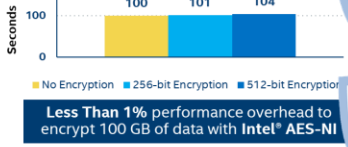
Intel® SHA Extensions — New instructions to accelerate the cryptographic Secure Hash Algorithm (SHA) variants SHA-1 and SHA-256

Similar to AES-NI, the SHA-NI is a family of instructions designed to improve performance and efficiency of SHA on x86

AES-2X — AES-2X is microarchitectural improvements that doubles the throughput of the AES engine and AES-NI

VPMADD52 — VPMADD52 is a 52-bit wide vector multiply and add instruction that is useful for public key cryptographic operation

...coming on Whitley



Less Than 1% performance overhead to encrypt 100 GB of data with **Intel® AES-NI**

Acceleration built into the processor, or massively scale up with Intel® QuickAssist Technology

ERM/DRM

Data Protection

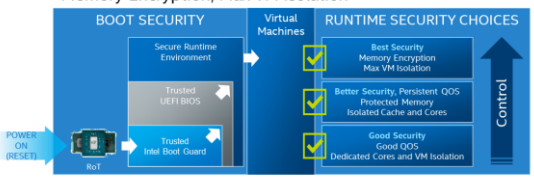
Full Disk Encryption

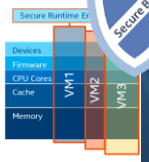
TLS

INTEL® SELECT SOLUTION FOR HARDENED SECURITY

SECURING THE MOST CRITICAL WORKLOADS

- Dedicated Cores and VM Isolation
- Protected Memory and Isolated Cache and Cores
- Memory Encryption, Max VM Isolation





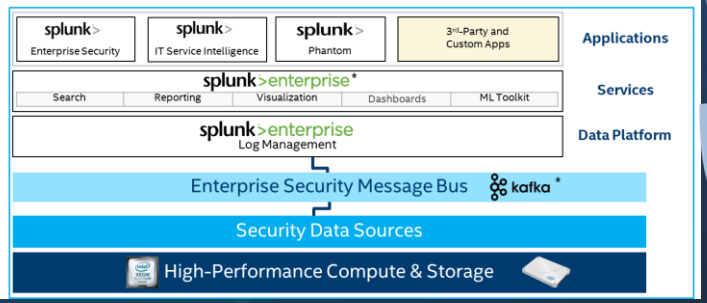
Data Protection

Virtualization Security

Secure Boot

Cyber Intelligence Platform Architecture

Focus on identifying and responding to sophisticated adversaries



Monitoring

Threat Intel

References

- NIST Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security (SP-800-46)
  - https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final
- NIST's User's Guide to Telework and Bring Your Own Device (BYOD) Security (SP-800—114)
  - https://csrc.nist.gov/publications/detail/sp/800-114/rev-1/final
- NIST Advice: Preventing Eavesdropping and Protecting Privacy on Virtual Meetings
  - https://www.nist.gov/blogs/cybersecurity-insights/preventing-eavesdropping-and-protecting-privacy-virtual-meetings
  - NIST Infographic : Conference Call Security
    - https://www.nist.gov/system/files/documents/2020/03/17/Conference%20Call%20Security%20Graphic.pdf
- NIST Telework Security Basics
  - https://www.nist.gov/blogs/cybersecurity-insights/telework-security-basics
- ITL BULLETIN MARCH 2020 Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions
  - https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-03.pdf
- DHS/CISA Enterprise VPN Security Alert (AA20-073A)
  - https://www.us-cert.gov/ncas/alerts/aa20-073a
- DHS/CISA Security Tip (ST04-006) Understanding Patches and Software Updates
  - https://www.us-cert.gov/ncas/tips/ST04-006
- Center for Internet Security (CIS) Telework and Small Office Network Security Guide
  - https://www.cisecurity.org/blog/small-offices-big-security-new-guide-for-securing-telework-environments/
  - https://cdn2.hubspot.net/hubfs/2101505/CIS Controls Telework Security Guide.pdf

References con't

- CISA INSIGHTS - Risk Management for Novel Coronavirus (COVID-19)
  - https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus_0.pdf
- OPM's Telework Guidance - Security and IT
  - https://www.telework.gov/guidance-legislation/telework-guidance/security-it/
- OMB/Whitehouse memos on Teleworking:
  - OMB Memo on Implementing the Telework Enhancement Act of 2010: Security Guidelines
  - https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-27.pdf
  - OMB Memo on Implementing the Telework Enhancement Act of 2010: IT Purchasing https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-20.pdf
- GSA: 72 FR 9532 - Information Technology and Telecommunications Guidelines for Federal Telework and Other Alternative Workplace Arrangement Programs
  - https://www.govinfo.gov/content/pkg/FR-2007-03-02/pdf/07-951.pdf
- GSA Guidelines for Alternative Workplace Arrangements
  - https://www.gsa.gov/cdnstatic/FMRBulletin_2006-B3.pdf

Blockchain and Government

An updated presentation to Virginia Information Technologies

Information Security Officers' Advisory Group

May 6, 2020

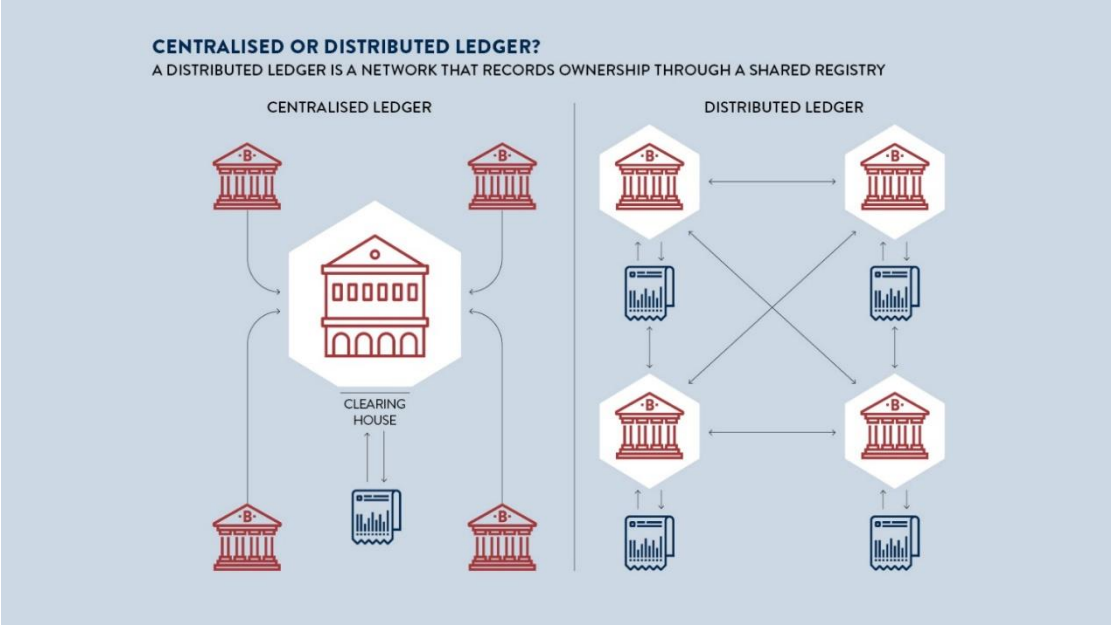
Agenda

- How do blockchains work?
- Regulation and law enforcement
- Governmental use cases

How do blockchains work?

What is blockchain technology?

- Distributed ledger of transactions
- Enables peer-to-peer trust and exchange of value

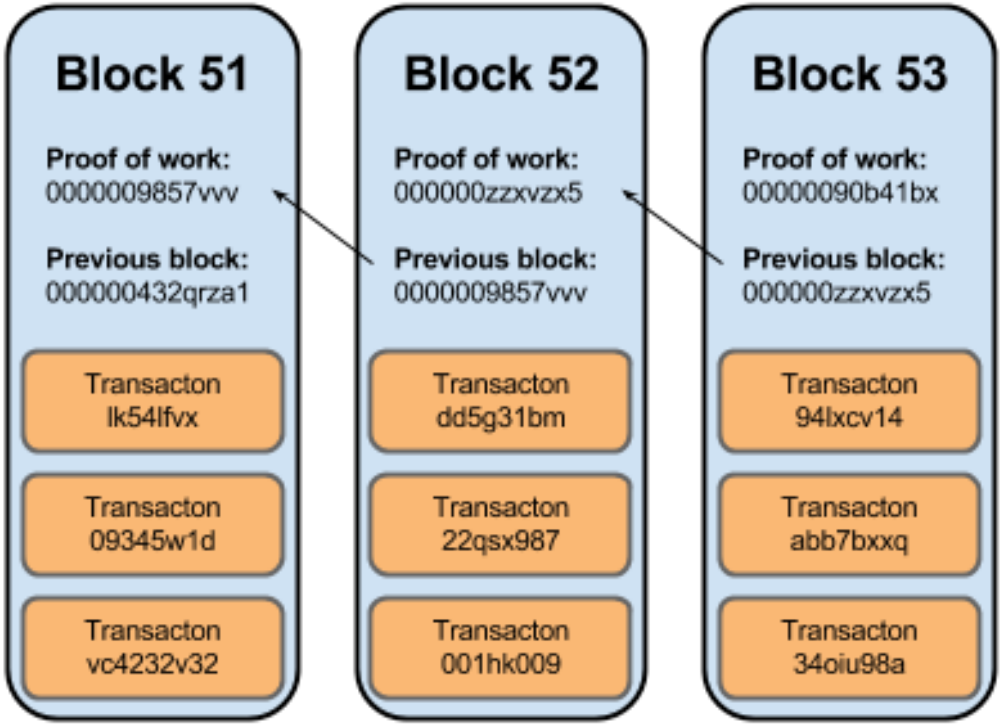


Who has read/write privileges?

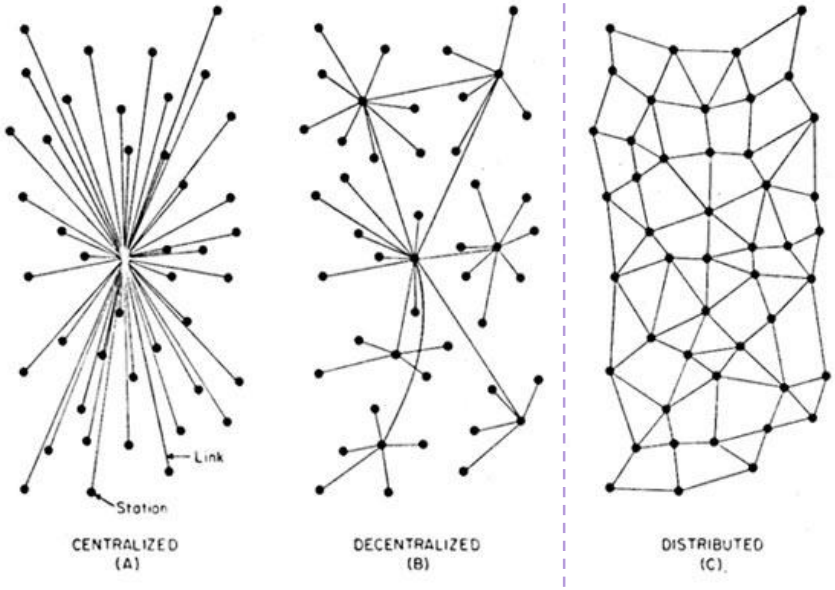
Attributes	Shared Databases	Private/Consortia Blockchains	Public Blockchains
Read Access	Users with permissions	Users with permissions	Unrestricted
Write Access	Users with permissions	Users with permissions	Any transaction which meets blockchain consensus rules
Examples	Google Sheets, SharePoint	Hyperledger, Corda	Bitcoin, Ethereum

How do blockchains validate transactions?

- Consensus:
  - Proof of stake
  - Delegation
  - Proof of work
- Incentives discourage cheating
- Immutable: expensive/ impractical to alter past transactions



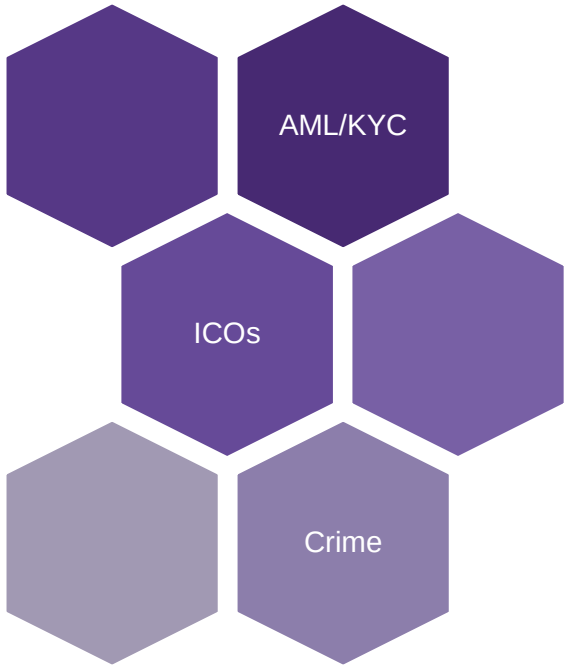
Properties of distributed networks



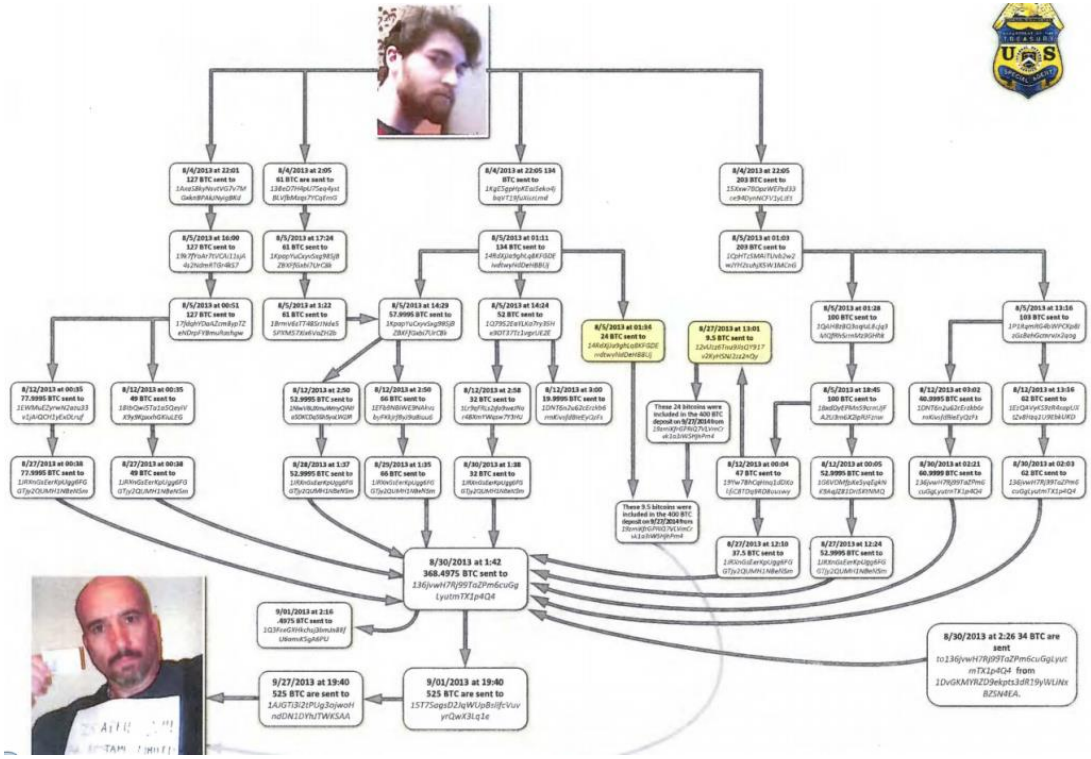
- Note the pattern of connections does not revolve around a single or handful of nodes
- Full nodes maintain a complete copy of the ledger (going back to the "genesis" block)
- Taking down one (or even many) nodes may slow the network temporarily, but not stop it
- For public blockchains, anyone with the appropriate hardware can run a node
- Many distributed chains can continue to run even if there is only *one* computer running it

Regulation and law enforcement

Regulatory issues



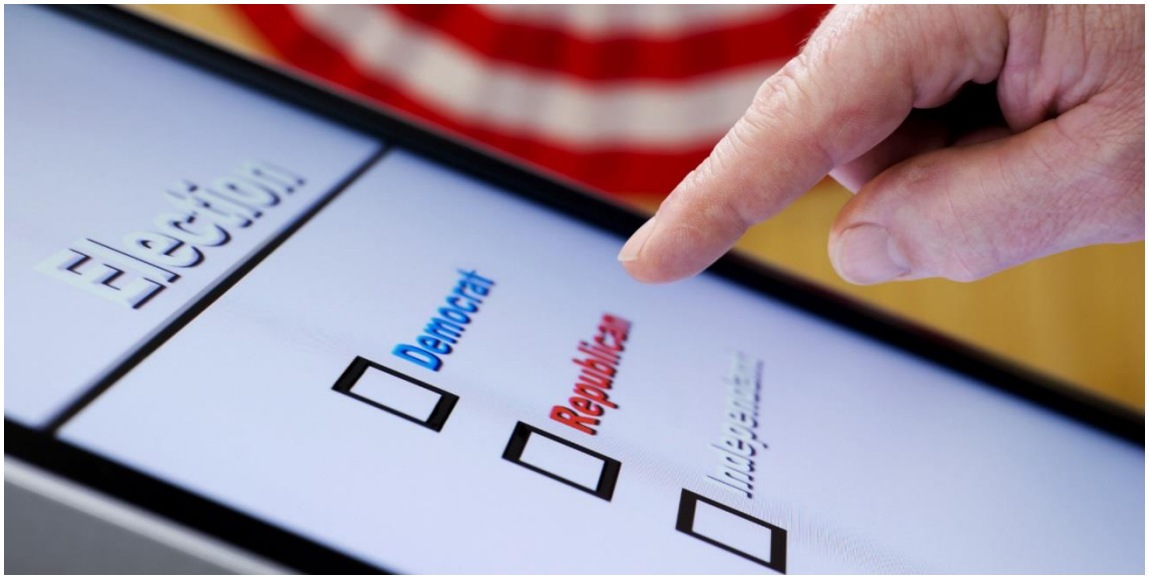
Law enforcement



Governmental use cases

Recordkeeping

- Transparent, secure authentication of records
- HHS audit trail/EHR
- Treasury's equipment
- Land deed registry
- E-voting/survey data



Smart contracts – what are they?

Vending Machine

- **Initial setup:** the machine must be built, programmed, and stocked before it can be used
- **Transparent terms**: the price of each product is clearly displayed
- **Self-executing:** no clerk needed, simply pay and select product

Smart Contract

- **Initial setup:** the contract code must be programmed and tested for bugs before deployment
- **Transparent terms:** computer code underlying smart contracts is readable by potential users
- **Self-executing:** no person needed, blockchain records payment and contract delivers

Smart contracts – how do they work?

Offer: computer code is programmed

- defines the terms of the agreement
- deployed to a blockchain, e.g. Ethereum

Acceptance: of nsurance premium or deposit of an asset

Execution: smart contract monitor
for an acceptance. Once satisfied, code executes:

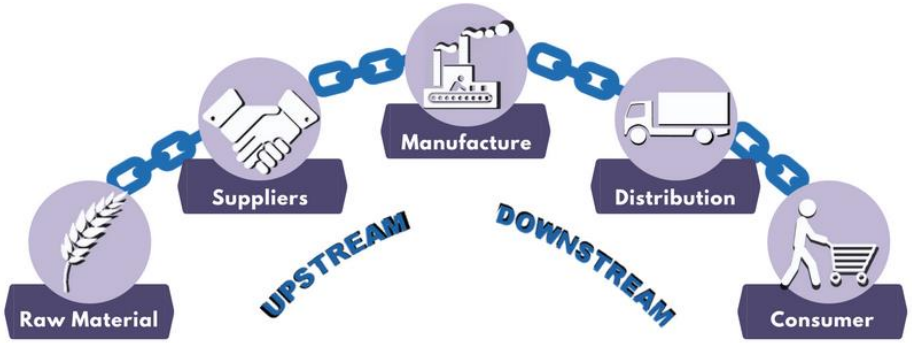
- **Payment alone**: when funds are received, the contract delivers the goods/services
- **Time-based**: e.g. a smart bond makes interest payments on pre-defined schedule
- **Oracle data**: third-party or program (IoT) which supplies external info, e.g.
  - Prime interest rate on Jan. 1
  - Did it rain in Richmond on Tuesday?

Grant Thornton

Supply chain and digital identity

Supply chain provenance

- USPS package delivery
- Naval aviation parts
- IBM, Walmart Food Trust



Digital identity

- Unforgeable, digital credentials
- CDC crisis response
- Illinois Blockchain Initiative
- Army secure communications
- Enables other use cases such as e-voting or electronic health records

Payments and accounting

Digital payments

- Grants and entitlements
- Central Bank Digital Currencies
- Stablecoins

Accounting and audit

- Creation of audit evidence
- Automated internal controls
- Reducing reconciliations
- Impact on audits

Questions?

Contact Information

Blake Carpenter, CPA
Audit Manager
Grant Thornton, LLP

Blake.Carpenter@us.gt.com

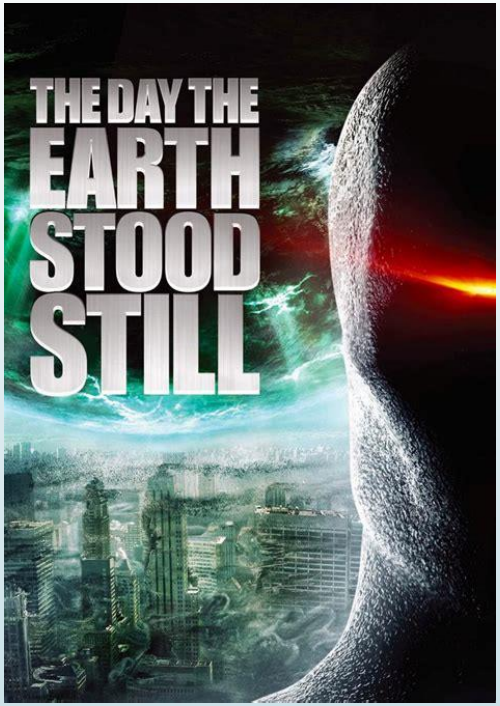
Twitter.com/@blakechain
LinkedIn.com/in/blakemcarpenter

Post-COVID Security

Adapting to the "New" Normal

Shana Sumpter, MSIA, CISSP®, CISA®, CRISC®

Coronavirus in Virginia



Twentieth Century Fox, 2008

- Cases of COVID-19 in Virginia
- Governor issues stay at home order for the Commonwealth
- Social distancing now the norm
- Businesses and schools across Virginia close or go remote
  - Flatten the curve

Remote Operations Overnight

- Business continuity
  - Got a plan, right?
- Telework in 0 to 60
- BYOD with or without a policy
- Scale up on software and services

Microsoft, 2004

Are We Good?

ABC, 1992

- Buy it! Do it! Make it happen!
- Securing the remote workspace
- Relax security controls…not so fast
  - Paper processes
  - System access
- Zoombombing? Is that a thing?

"You Like Me! You Really Like Me!"

- The network now includes home networks
- Security awareness is critical
  - Cybersecurity really is everyone's responsibility now
- Don't add insult to injury
  - Regulations have not relaxed, neither should controls

AP, 1985

Here they come…

- Back to "normal"
  - In-office, remote, or both
  - Scale down
  - About that free software
- Return to the office
  - Out of date workstations
  - Business processes
  - Inventory control

AMC, 2016

Still Defending the Enterprise

Thank you

References

- American Broadcasting Company. 1992. "Urkel Much Face." Retrieved from https://tenor.com/view/urkel-reactions-faces-emotive-steveurkel-gif-4491512.
- AMC Networks. 2016. "The Walking Dead: Pushing Walkers Off The Road." https://youtu.be/kdphXtLDz_I.
- Microsoft. 2004. "Halo 2." Retrieved from https://youtu.be/82NUo0PNsrI.
- The Cut. 2014. "The Science of 'You Like Me! You Really Like Me!'" Retrieved from https://www.thecut.com/2014/10/explaining-you-like-me-you-really-like-me.html.
- Twentieth Century Fox. 2008. "The Day the Earth Stood Still." Retrieved from https://tvguide1.cbsistatic.com/rovi/showcards/movie/292495/thumbs/16815273_1300x1733.jpg.

Virginia Information Technologies Agency

Cloud Services, Pricing and Strategy

Demetrias Rodgers,
Director of Platform Operations and Enterprise Services
Kevin Washington,
Cloud Services Lead

May 6, 2020

Agenda

- Overview of cloud service providers
- What are the planned cloud deployment services?
- Cloud optimization
- Future state
- Public cloud pricing

Cloud service providers

Service	Provider	Description
Amazon web services (AWS) cloud computing	Amazon	AWS cloud computing provides on-demand platforms and API's for reliable, scalable and inexpensive cloud computing services
Microsoft Azure (Azure) cloud computing	Microsoft	Azure is a cloud computing service for building, testing, deploying and managing applications and services
Oracle cloud infrastructure (OCI)	Oracle	OCI is a set of complementary cloud services to build and run a wide range of applications and services in highly available host environments

Cloud services

Initial cloud services deployment will include services in the following categories:

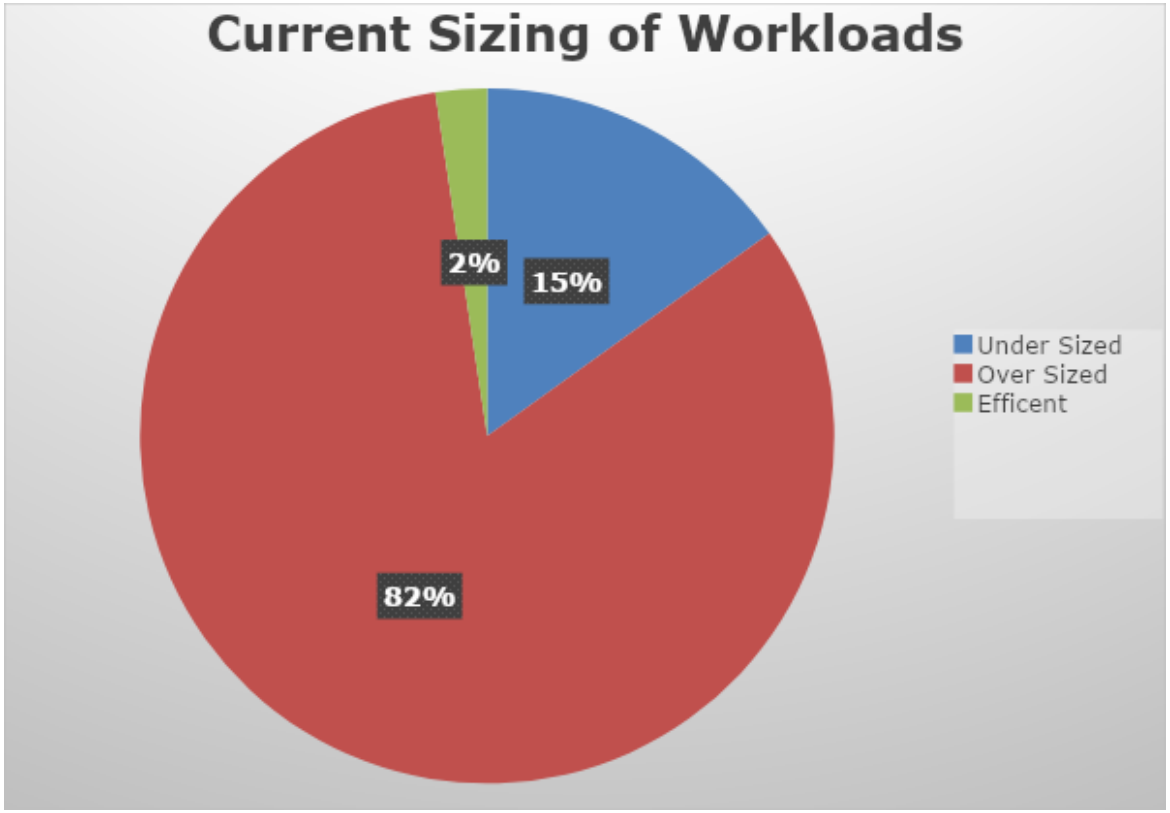
- Compute services
- Storage services
- Networking and data center services (e.g. monitoring and auditing capabilities)
- DevOps services – (AWS and Azure)
- Data analysis services (data lake and catalog services)
- VITA will continuously make new services available as required

Cloud workload optimization

- One of the directives VITA has provided is a no "lift and shift" approach for cloud service migrations
- VITA has a duty to ensure that workloads are optimized for cloud consumption prior to migrating to the cloud; if it is not optimized, then it could result in higher costs to the agency and commonwealth as a whole
- VITA will implement artificial intelligence in our environment to analyze application usage and present appropriate cloud templates to ensure the application is migrated with the correct configuration

Workload utilization

Current workload analysis



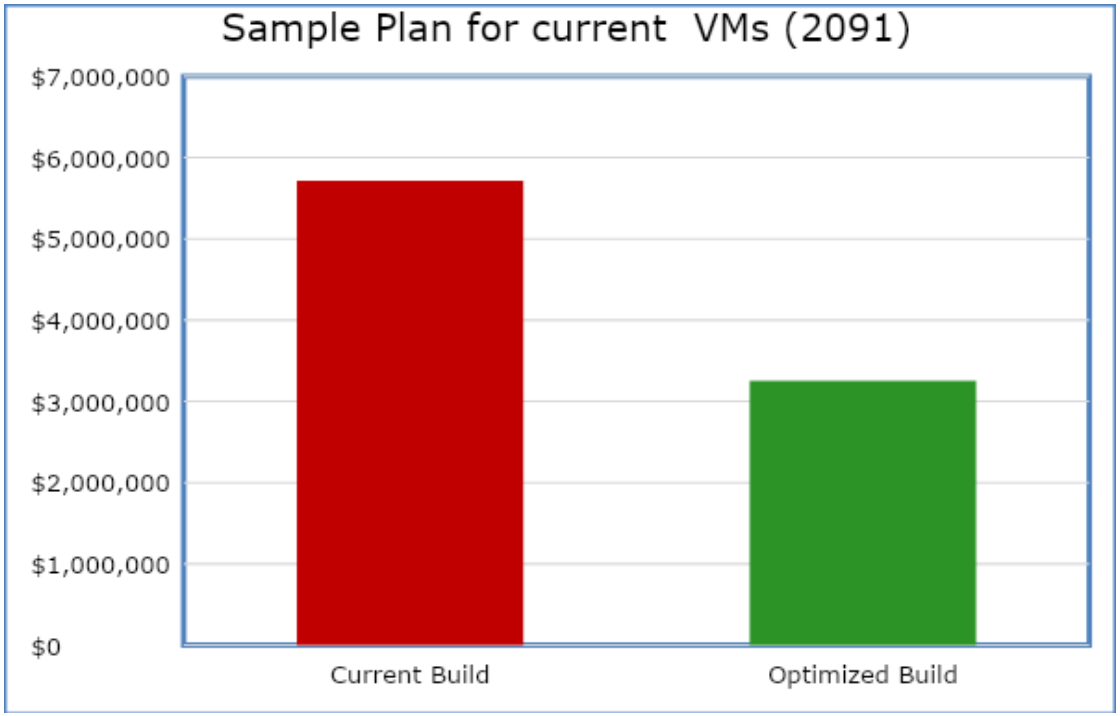
- 50 VMs (2%) are performing well and efficiently sized
- 316 VMs (15%) do not have enough resources allocated to prevent performance issues
- 1725 VMs (83%) have more resources allocated than they need

How are cloud services charged?

- Cloud service providers have a few different ways of charging customers. The methodology varies based on the services an agency leverages:
  - Consumption-based
  - Monthly costs
  - Subscription-based services
- VITA's chargeback strategy must support the various cloud services offered by VITA, maintaining a balance between the desire to take advantage of service and financial flexibility and the need for cost recovery and predictability, necessary for budget optimization and management
  - Propose simplifying the charging mechanism through service bundles to support ordering, chargeback and billing requirements
  - There will also be stand-alone services including platform and DevOps services

Provide data for placement decision BEFORE migration

Data-driven analysis will provide significant cost avoidance by ensuring environments are properly configured and utilizing virtual compute resources best fit for the individual use case. These data points will assist agencies in projecting future costs and highlight gaps in productivity



43% Less

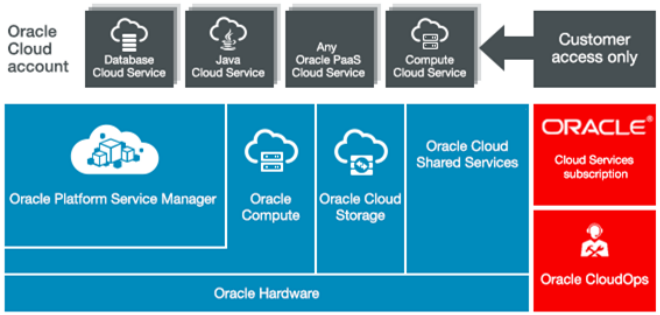
Workload placement decisions across clouds

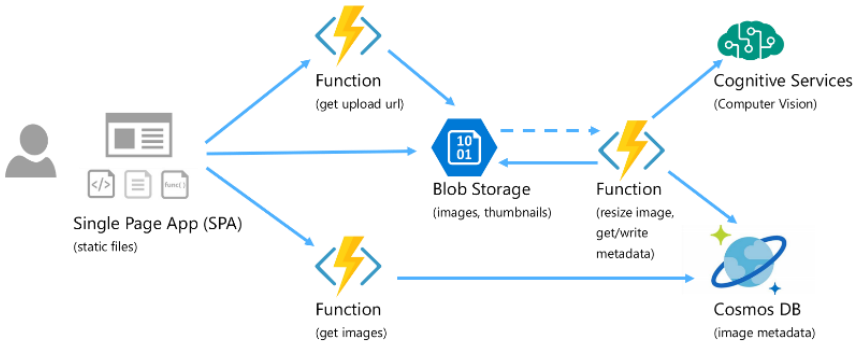
Azure by Dept	On-Demand Allocation	On-Demand Consumption	Storage Allocation	Storage Consumption	Difference
DOC	$ 12,128	$ 5,690	$ 3,764	$ 2,060	-$8,142.00
DMV	$ 22,903	$ 16,536	$ 2,836	$ 1,150	-$8,053.00
DSS	$ 55,941	$ 40,268	$ 14,401	$ 6,847	-$23,227.00
TAX	$ 41,730	$ 31,574	$ 8,842	$ 3,800	-$15,197.00
VDOT	$ 72,402	$ 60,448	$ 19,204	$ 11,519	-$19,639.00
VEC	$ 20,181	$ 17,100	$ 5,071	$ 3,334	-$4,818.00
Totals	$225,285	$171,616	$54,118	$28,710	-$79,076.00

AWS by Department	On-Demand Allocation	On-Demand Consumption	Storage Allocation	Storage Consumption	Difference
DOC	$ 9,626	$ 5,642	$ 2,190	$ 1,480	-$4,704.00
DMV	$ 15,988	$ 14,642	$ 1,346	$ 1,183	-$1,509.00
DSS	$ 45,392	$ 37,049	$ 6,944	$ 4,636	-$10,651.00
TAX	$ 32,021	$ 27,457	$ 4,127	$ 3,066	-$5,625.00
VDOT	$ 57,544	$ 52,483	$ 9,768	$ 8,095	-$6,734.00
VEC	$ 18,183	$ 14,623	$ 2,565	$ 2,358	-$1,202.00
Totals	$178,754	$151,896	$26,940	$20,818	-$30,425.00

Future state

VITA is looking to operate at the speed of business, providing infrastructure, application optimization, and development services that will enable agencies to meet a CI/CD and RAD model.





***CI/CD** – Continuous Integration and Continuous Delivery
***RAD** – Rapid Application Development

Public cloud pricing

Updated

Monthly rate	AWS	Azure	Oracle
Windows instance (Tier 1)	$643.90	$643.90	$728.53
Windows instance (Tier 2)	$571.86	$571.86	$640.22
Linux instance (Tier 1)	$564.23	$564.23	$666.27
Linux instance (Tier 2)	$470.88	$470.88	$552.54
Consumption-based cloud charges (storage)	~$0.75/GB on average		
Consumption-based cloud charges (non-storage)	Supplier cost with VITA overhead mark-up		

*These rates are in addition to existing private cloud rates which are already in use. Traditional storage rates do not apply to public cloud pricing.
**Additional infrastructure services may be needed to support the public cloud service, such as increased network bandwidth.

One-time costs

Updated

- Agency account set-up:
  - $564.50 per agency/only charged once per agency
  - Setup required to add a new Agency into the Virtual Data Center landing zone
- Managed service account set-up:
  - $1,129.00 per project
  - Charged per project
- Stealth license set-up:
  - $195.88 per instance
  - Set-up cost for stealth license service
- Migration and consulting:
  - Labor rates
  - No mark-up is applied to material costs if required

Rate model

- Developed outside of the normal budget cycle
- Fixed public cloud rates:
  - Based on public cloud rates in Unisys contract
  - Indirect expenses layered into fixed rates
    - Examples include: Cloud workload optimization service, virtual firewalls, security, 10GB sandbox, full packet capture, enterprise allocations
- AWS, Azure, and Oracle consumable rates:
  - Multiple rates that vary in cost each month
  - Not possible to develop fixed rates due to the variable nature of cloud pricing
  - Marked-up using a percentage to recover indirect expenses

Minimum commitment period

- Public cloud services have a minimum service commitment period of one billing cycle
- A customer will be invoiced the chargeback resource unit rate for one billing cycle even if the service ordered is installed and decommissioned within the same billing cycle
- The chargeback resource unit rate is not prorated for a portion of the billing cycle.

Invoicing of cloud services

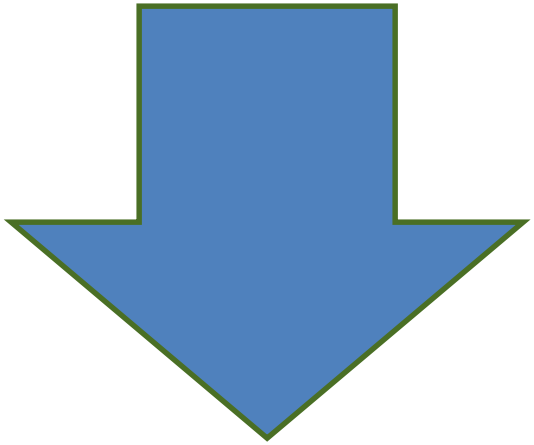
- Invoicing of cloud services will follow the normal process
- Expenses will appear within your comprehensive bill
- Fixed rates will be billed on a monthly basis
- Consumable expenses will be billed based on charges incurred by VITA + mark-up %
  - Applies to AWS, Azure and Oracle expenses
  - Different methodology than normal rated services
  - Similar to legacy telco approach

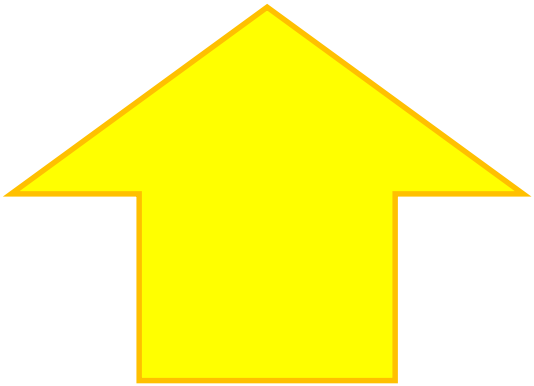
FY22+ impact to rates

- The current public cloud rate will change in FY22

Downward rate pressure

- Higher consumption
- Lower fixed expenses
- Over-recovery of expenses in FY20/21





Upward rate pressure

- Lower projected consumption
- Higher fixed expenses
- Under-recovery of expenses in FY20/21

Questions?

Virginia Information Technologies Agency

Upcoming events

Virginia Information Technologies Agency

The next IS orientation will be held on June 30, 2020

1 – 3 p.m. in room 1211 (CESC)
Presenter: Marlon Cole (CSRM)

Registration link:
http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10

Virginia Information Technologies Agency

Future ISOAG

June 3, 2020

Speakers: Kevin Heaslip,VT

Eric Culbertson, ATOS

Alan Gernhardt, VA Freedom of Information Advisory Council

ISOAG meets the first Wednesday of each month in 2020

ADJOURN

THANK YOU FOR ATTENDING

Picture courtesy of www.v3.co.uk