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

- Network Attacks
- Increased Attack Surface Area
- Unsecured Environments and Networks
- Unauthorized Access
- Phishing
- Unauthorized Data Movement
- Data Loss
- Attacks on Video and Collaboration Tools
- Malware/APTs
Solutions for Securing the Teleworker

BYOD

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

Enterprise Data Center
- VDI Cloud
- Private Cloud

Cloud Services

Enterprise Rich Client
- Secure Boot
- Full Disk Encryption
- Data Protection

IT

Patching

Local Firewall

MFA

EAC

End Point Policy Enforcement

ERM/DRM
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)

**INTEL® SOFTWARE GUARD EXTENSIONS (SGX)**
Protected execution environment embedded in a process
- With its own code and data
- Provides Confidentiality & Integrity
- Controlled entry points
- Multi-thread support
- Full access to app memory and processor performance

**INTEL® THREAT DETECTION TECHNOLOGY**
- Intel TDT Advanced platform detection: leverages a world-class Intel® Advanced Vector Extensions 2x (Intel® AVX-2x) to provide faster detection and response to advanced threats, such as malware.
- Intel TDT Accelerated Memory Scanning (AMS): leverages a dedicated memory scanning engine to detect and report on memory content, providing real-time protection against memory exploits and malware.

**PROTECTED DATA WITHOUT COMPROMISING PRODUCTIVITY**
Intel’s Hardware Accelerated Encryption
- AES-2X: Provides high-speed, hardware-accelerated encryption for maximum performance.
- VPMADDQS: A 52-bit wide vector multiply and add instruction that is useful for public key cryptographic operations.

**EMBRACING DIGITAL TRANSFORMATION**
Intel Datacenter Technologies for Securing the Teleworker

**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® Select Solution for Hardened Security**
- Dedicated Cores and VM Isolation
- Protected Memory and Isolated Cache and Cores
- Memory Encryption, Max VM Isolation

**Protected Data Without Compromising Productivity**
- 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 is microarchitectural improvements that doubles 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 operations
- Time to write 100 GB of data on Intel® Xeon® processor E5-2697 v3
- Less Than 1% performance overhead to encrypt 100 GB of data with Intel® AES-NI

**Cyber Intelligence Platform Architecture**
- Focus on identifying and responding to sophisticated adversaries
- Applications
- Services
- Data Platform
- Enterprise Security Message Bus
- Security Data Sources
- High-Performance Compute & Storage

**EMBRACING DIGITAL TRANSFORMATION**
References

- NIST Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security (SP-800-46)
  

- NIST’s User's Guide to Telework and Bring Your Own Device (BYOD) Security (SP-800—114)
  

- NIST Advice: Preventing Eavesdropping and Protecting Privacy on Virtual Meetings
  
  
  - NIST Infographic : Conference Call Security
    

- NIST Telework Security Basics
  

- ITL BULLETIN MARCH 2020 Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions
  

- 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/
  
References con’t

• CISA INSIGHTS - Risk Management for Novel Coronavirus (COVID-19)

• 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
  • OMB Memo on Implementing the Telework Enhancement Act of 2010: IT Purchasing

• 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
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?

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Shared Databases</th>
<th>Private/Consortia Blockchains</th>
<th>Public Blockchains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read Access</td>
<td>Users with permissions</td>
<td>Users with permissions</td>
<td>Unrestricted</td>
</tr>
<tr>
<td>Write Access</td>
<td>Users with permissions</td>
<td>Users with permissions</td>
<td>Any transaction which meets blockchain consensus rules</td>
</tr>
<tr>
<td>Examples</td>
<td>Google Sheets, SharePoint</td>
<td>Hyperledger, Corda</td>
<td>Bitcoin, Ethereum</td>
</tr>
</tbody>
</table>
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 offer, for example payment of an insurance premium or deposit of an asset

**Execution**: smart contract monitors 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?
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

- 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
Are We Good?

- 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
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

Any Questions
References

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

<table>
<thead>
<tr>
<th>Service</th>
<th>Provider</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Amazon web services (AWS) cloud computing</strong></td>
<td>Amazon</td>
<td>AWS cloud computing provides on-demand platforms and API’s for reliable, scalable and inexpensive cloud computing services</td>
</tr>
<tr>
<td><strong>Microsoft Azure (Azure) cloud computing</strong></td>
<td>Microsoft</td>
<td>Azure is a cloud computing service for building, testing, deploying and managing applications and services</td>
</tr>
<tr>
<td><strong>Oracle cloud infrastructure (OCI)</strong></td>
<td>Oracle</td>
<td>OCI is a set of complementary cloud services to build and run a wide range of applications and services in highly available host environments</td>
</tr>
</tbody>
</table>
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
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.
• 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.

Sample Plan for current VMs (2091)

- Current Build: $7,000,000
- Optimized Build: $3,000,000

43% Less
## Workload placement decisions across clouds

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

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

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

*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

• 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
Upcoming events
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
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*
THANK YOU FOR ATTENDING