IARPA Cloud Computing

Kerry Long | Program Manager

Office of the Director of National Intelligence

IARPA

BE THE FUTURE

The United States Intelligence Community

IARPA Mission

IARPA envisions and leads *high-risk, high-payoff research* that delivers innovative technology *for future overwhelming intelligence advantage*

- Our problems are **complex** and **multidisciplinary**
- We emphasize **technical excellence** & **technical truth**

IARPA Cloud Computing R&D Difference

Question: How to Improve Security of the Cloud ?

Question: How to Improve Security with the Cloud ?

- Today's Global clouds are concentrating talent and resources like never before to conceive, develop and deploy computing innovations at an unprecedented pace
- These innovations are mostly being focused on improving quantities such as availability, flexibility, and efficiency
- Computer security is getting some attention from the cloud, but it is mostly to placate regulators and to provide security controls that resemble those applied to legacy data centers (where's the innovation ?)
- With a little bit of effort (from IARPA) we could refocus the enormous innovation potential of the cloud to improve computer security
- The Global cloud could help us resolve some difficult computer security challenges. IARPA seeks to demonstrate this possibility through carefully chosen examples

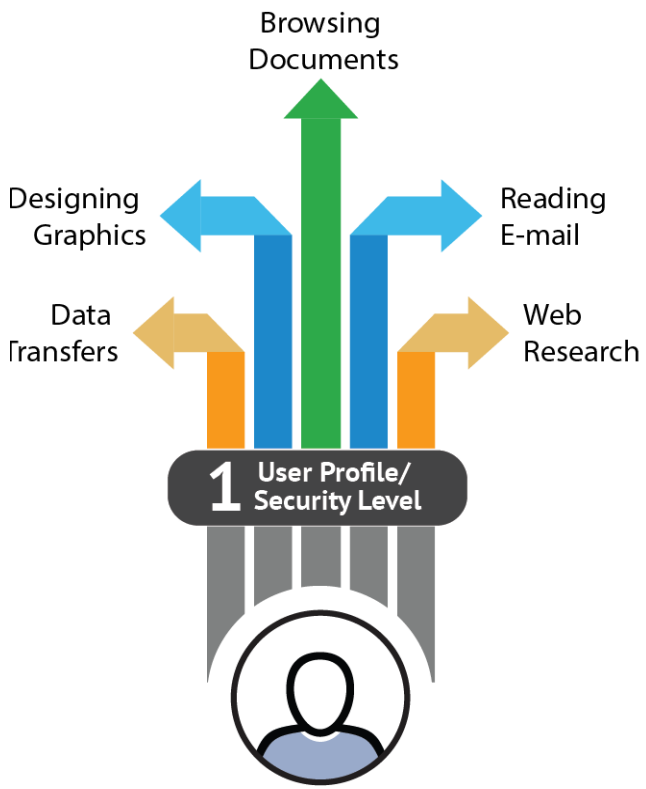
Our First Example – VirtUE Phase 1

Program Goal: Use the technologies of the cloud to create a new user interface that mitigates user-based computer threats in the government's computing environment - " A better VDI"

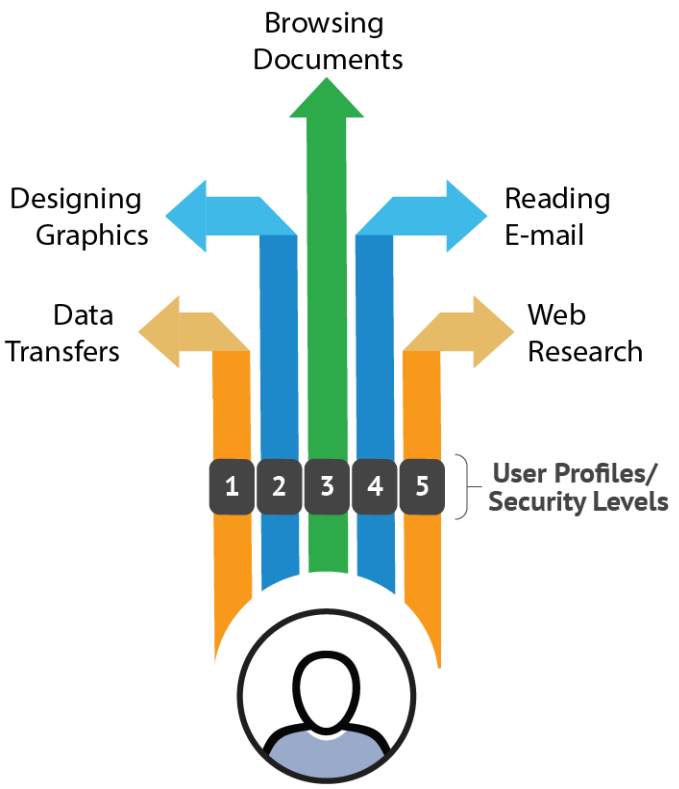
Mitigate this Computer Security Conundrum:

- Computer users are responsible for most of our current security incidents. Spear-Phishing, Malicious Web content, user carelessness or malice
- Users need convenient access to computing resources to maintain productivity and achieve organizational goals

CURRENT MODEL



VIRTUE MODEL



Activity Risk Level

- High Risk
- Medium Risk
- Low Risk

Redesign the Legacy User Environment Leveraging AWS EC2

Current Model

Virtue Model

1 desktop environment per user

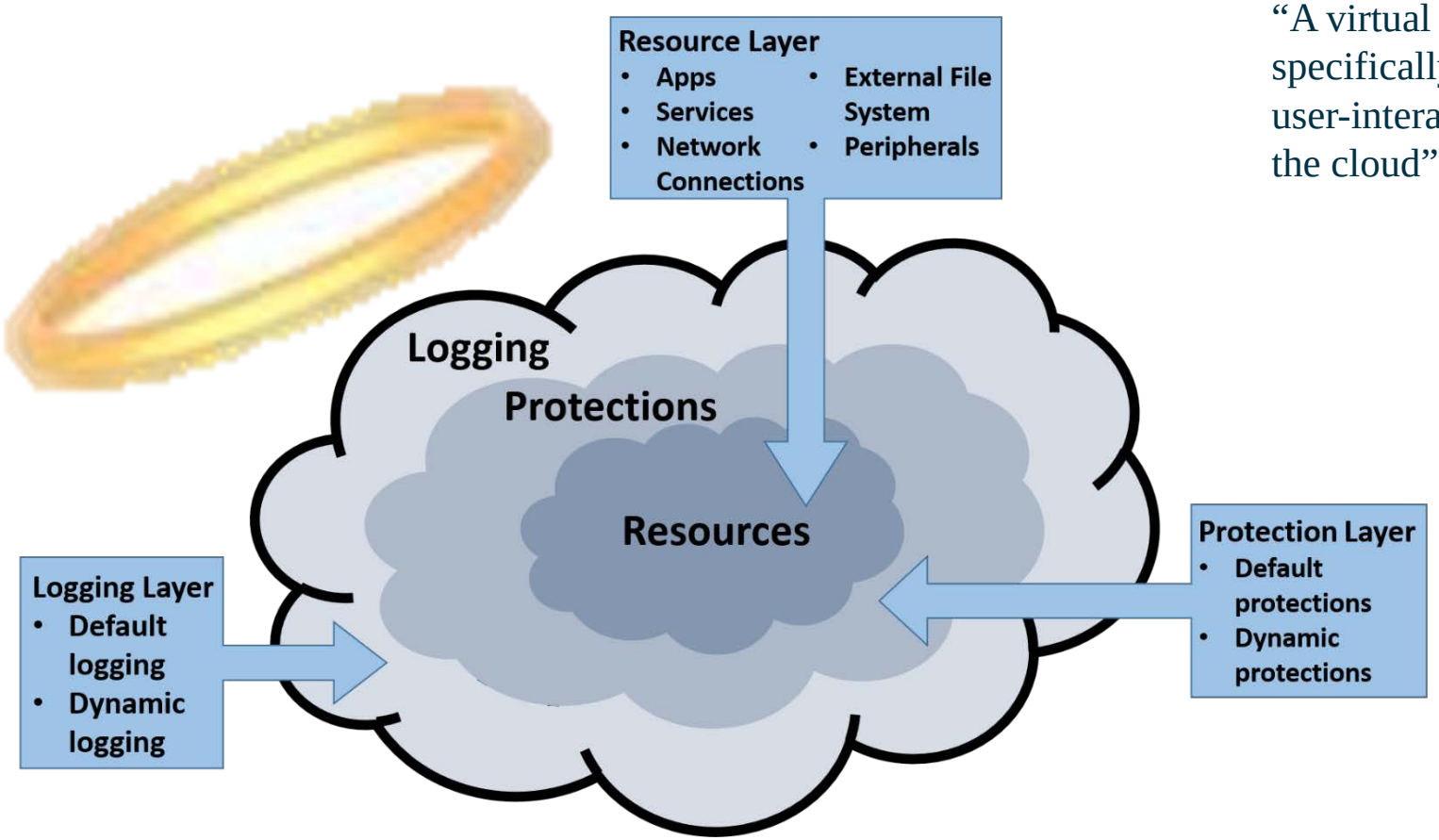
1 desktop environment = multiple user roles, generic logging and protections

5 or more Virtue environments per user

1 Virtue environment = one user role, role-tailored logging & protections

Resource Utilization must be comparable !

Build a Dynamic, Securable User Environment Using the Cloud – A "Virtue"



"A virtual appliance built specifically for the purpose of safe, user-interactive computing tasks in the cloud"

VirtUE Phase 1 Facts

- Awarded Sept 1, 2018
- 18 Months duration
- 4 Performers
- Star Lab
- Siege Technologies
- BBN
- Next Century & Virginia Tech
- All performer results and software released open source (BSD license)
- Johns Hopkin University APL Test & Evaluation Partner

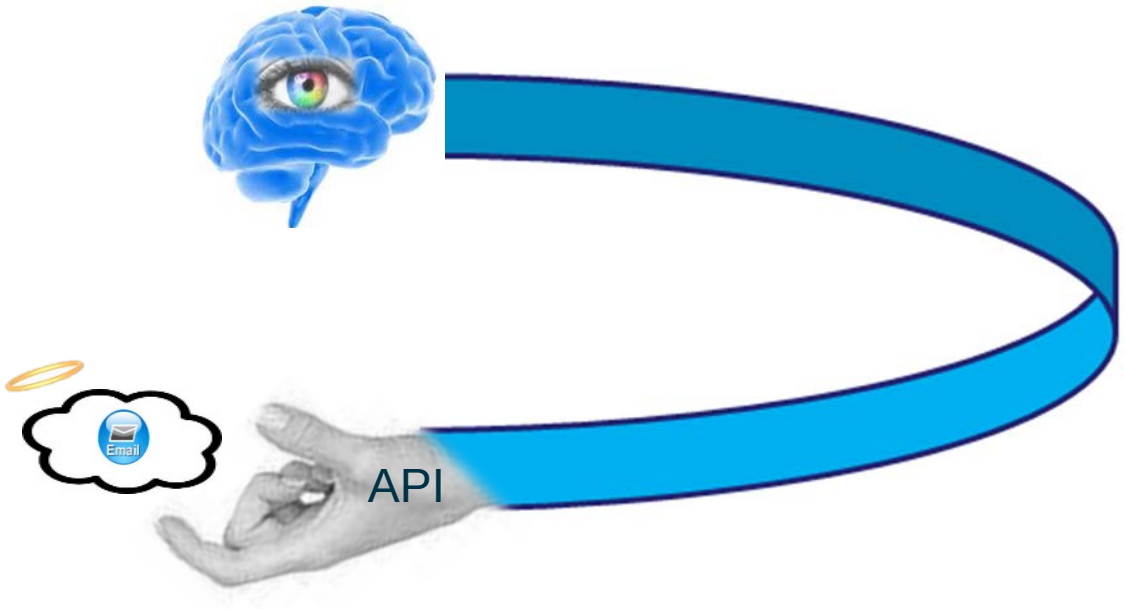
Our Second Example – VirtUE Phase 2

Program Goal: Leverage user environments developed in VirtUE phase 1 to develop new cloud logic that minimizes the expense and increases effectiveness of computer security

Address Shortcomings of host-based Computer Security Analytics

- Current security analytics are extremely costly and often ineffective. Consume vastly more data than they need but often do not collect the data needed
- Security analytics are not effectively tied to security responses. Results in organizations applying unnecessarily expensive security measures on users

Build “Dynamic” Security Logic/Analytics That Leverage Virtues



Dynamic Analytics Improve Protection Possibility

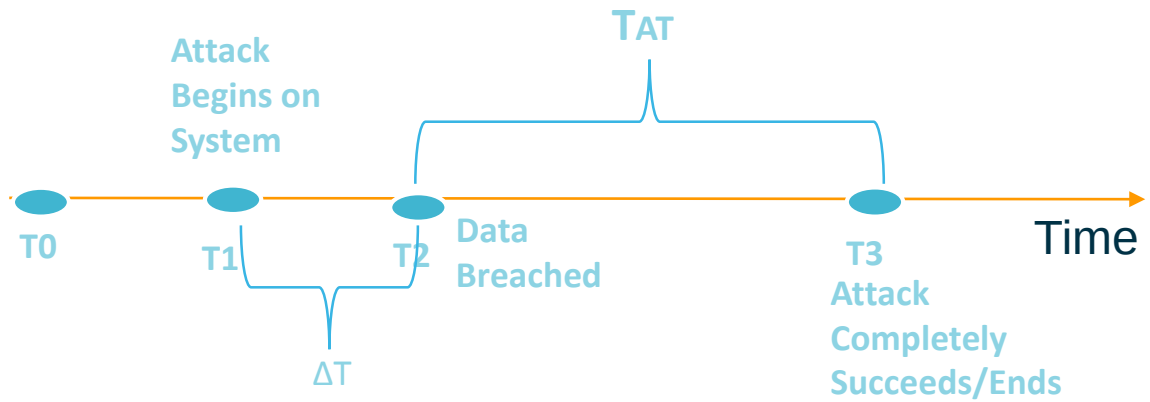
Current: Host-based Anti-Virus (AV) software constantly scans newly opened files on a user's desktop to ensure it does not contain malicious logic

1. **User experiences delays and slow computer access whenever user creates a new index of work files**

2. **Computer takes several minutes each morning to boot up loading large AV modules in memory as well as new AV definition files**

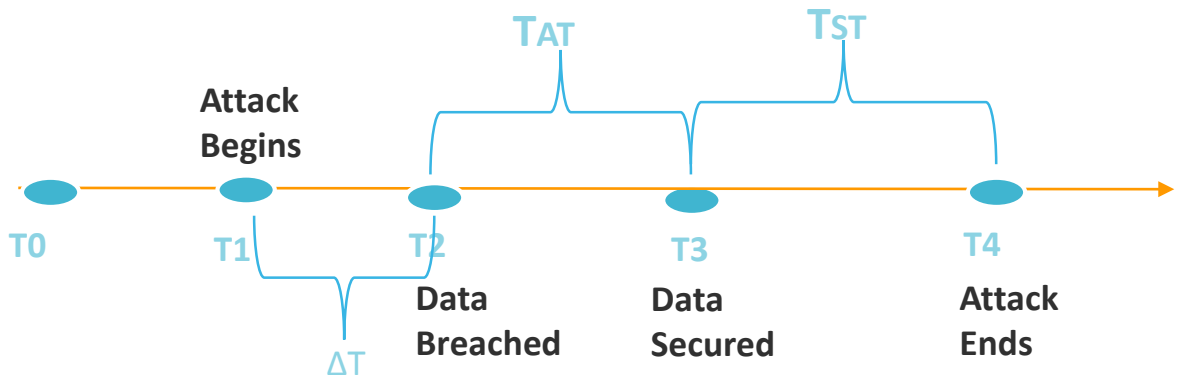
A VirtUE Solution: Dynamic Analytic analyzes user process artifacts and networking logs. Leverages Virtue ability to kill a user process to protect the user or invokes AV when the risk warrants

Defining Protection Benefits/Costs as A function of time



- Security protections for data provide little benefit value between T0 and T1 when there is no attack. (Prophylactic Security is Expensive !)
- Protections provide value during ΔT. The bigger ΔT the better value; So benefit value α ΔT.
- Data at risk and protections fail during T_{AT} → yielding a " negative Benefit Value" α T_{AT}

Defining Protection Benefits/Costs as A function of time



- Security protections for data provide little benefit value between T0 and T1 when there is no attack. (Prophylactic Security is Expensive !)
- Positive protection benefit value resumes during T_{ST}. The Bigger T_{ST} the better value; So benefit value α T_{ST}

Measuring Protection Effectiveness

Example: During a Recovery