13TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

cybersecuritysummit.org

RESILIENCE UNLOCKED

TITLE SPONSOR

Island

#cybersecuritysummit #css13

Kernel Level Security vs. Traditional Methods

Unveiling Unprecedented Cyber Defense

Tony Chiappetta

President, CHIPS

Distributor of AppGuard for North and South America

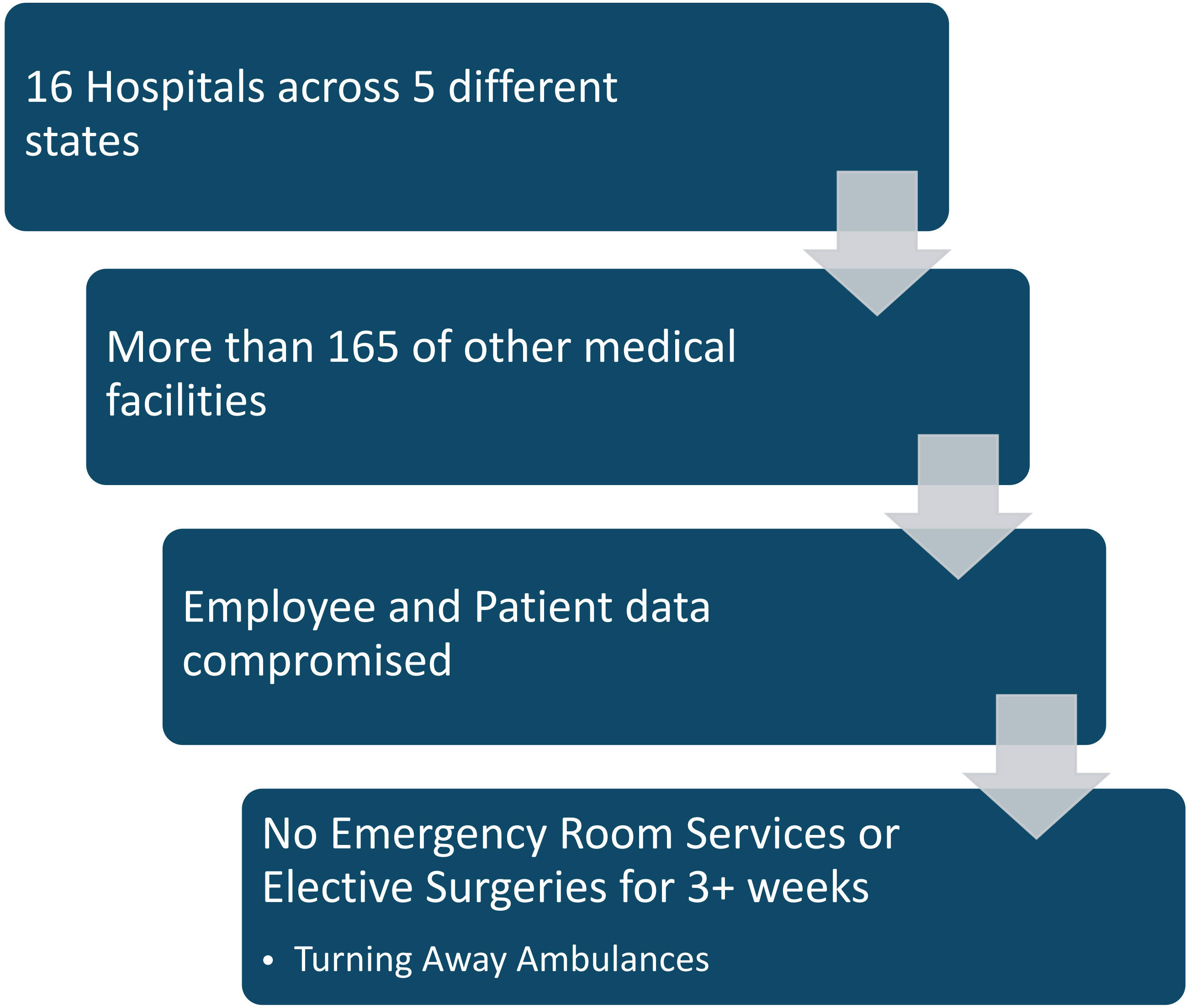
https://prevent-ransomware.com

Business Impact of a Successful Ransomware Attack

- Weeks or Months to recover.
- Ransom Demand of
  $1-2 Million.
- Recover Costs averaging $4.45 Million +.
- Customer Loss and Reputational Damage.

Prospect Medical Ransomware Breach August 4th, 2023

PROSPECT MEDICAL HOLDINGS, INC.



16 Hospitals across 5 different states

More than 165 of other medical facilities

Employee and Patient data compromised

No Emergency Room Services or Elective Surgeries for 3+ weeks

- Turning Away Ambulances

How did this happen?

New Ransomware Group – *Rhysida.*

Well crafted phishing email – Internal ticketing system.

Compromised a user with administrative rights.

Cobalt Strike and PowerShell used to deliver payloads.

- Data Encryption

-Further Avoid Detection

The Hospital Technical Landscape

- Servers
- Desktops
- Laptops
- Tablets
- Internet of Things
- Medical IoT
- Vendor Devices
- Patient Devices, Visitors, Employees, etc.

Traditional NIST Framework

Identify	Identify vulnerabilities to better understand the risks to systems, assets, data and features.
Protect	Implement security measures for protection of critical infrastructure services.
Detect	Implement security measures that would detect attacks
Respond	Implement security measures to attempt to respond to a deployed attack
Recover	Formulate and maintain a plan to prevent future attacks & implement measures needed to restore functions and services

New patterns of malware that do not match known behavior, or analysis with past big data **may slip through.**

It takes time to detect a malware that attacks with new behaviors and unknown vulnerabilities.

As the attack has already been implemented, **a complete response can be very difficult or costly**.

Risk remains for zero-day attacks

Traditional NIST Framework

Identify Identify vulnerabilities to better understand the risks to systems, assets, data and fe

Protect I o

Detect I d

Respond I r

Recover Formulate and maintain a plan to prevent future attacks & implement measures needed to restore functions and services

atterns of malware that do not known behavior, or analysis with g data **may slip through.**

s time to detect a malware that with new behaviors and vn vulnerabilities.

attack has already been nented, **a complete response very difficult or costly.**

Risk remains for zero-day attacks

Detect and Respond Solutions

Mainstream Detection Methodologies

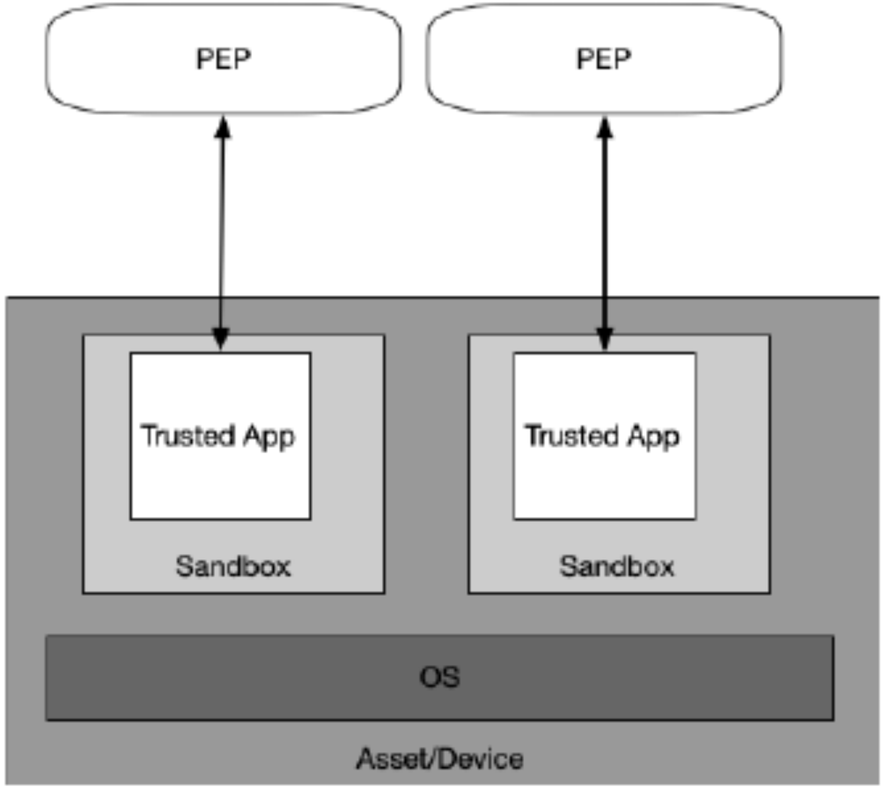
- Signatures
- Behaviors
- Machine Learning
- Artificial Intelligence
- Cloud
- False Positives
- Fails to Detect > Fails Open

Zero Trust

- NIST SP 800-207

An operative definition of zero trust and zero trust architecture is as follows:

Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.



What if an Endpoint Only Processed Trust Actions?

- Simplified Security Posture
- Added Efficiency
- No Patching Fire Drills
- Less Reactive Support Needs
- No missed detections
- No false positives
- No reliance on threat detection

How? – Kernel Level Protection

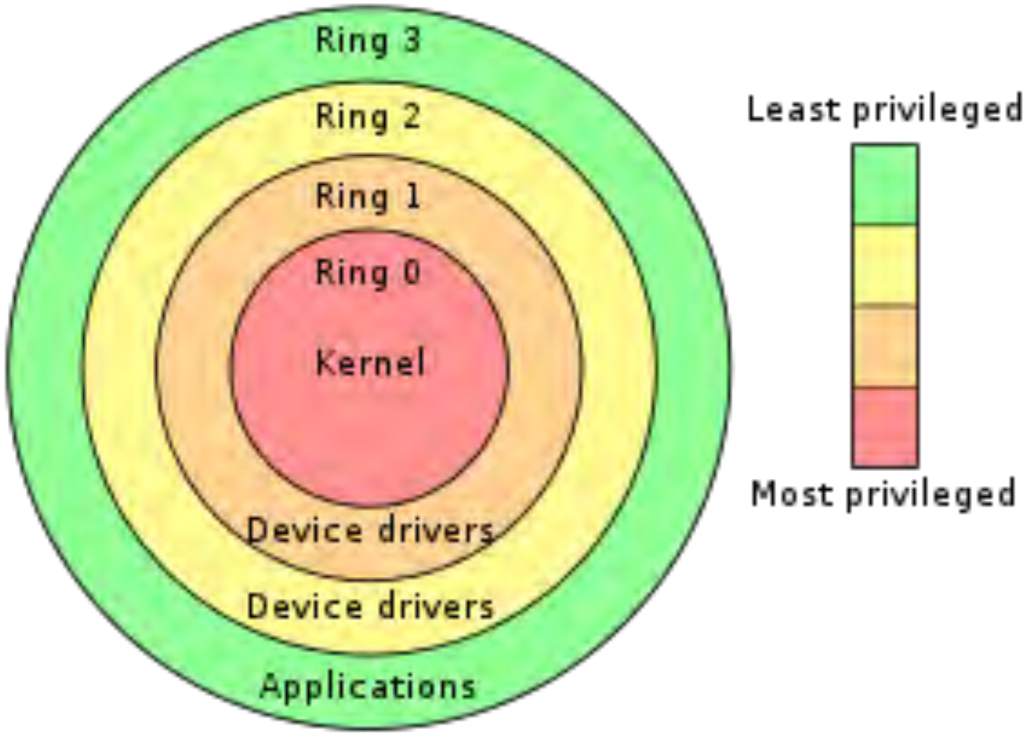
- Protection moves from the Application Layer to the Kernel Level

- Kernel-level Driver that strictly enforces a Policy

- No means No – end of conversation

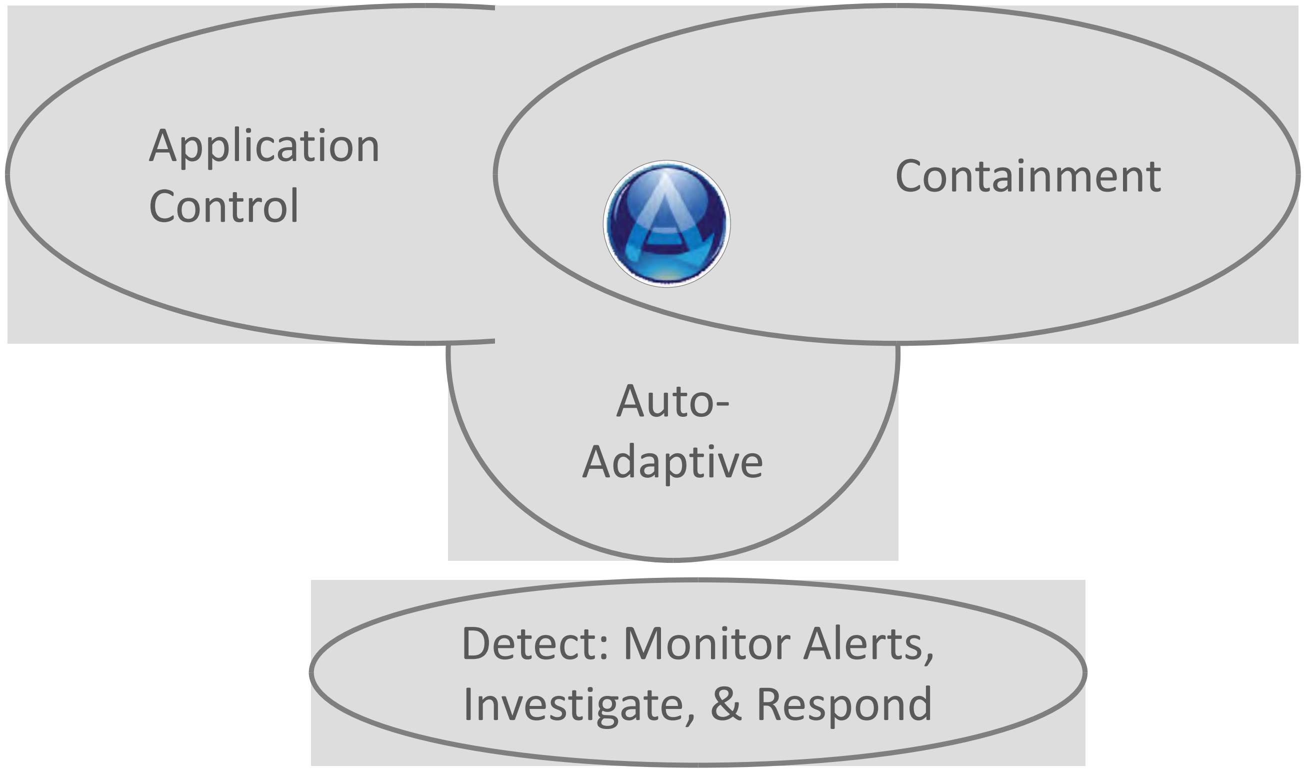
- Sounds like Whitelisting?

  Starts with Application Launch Control, but so much more



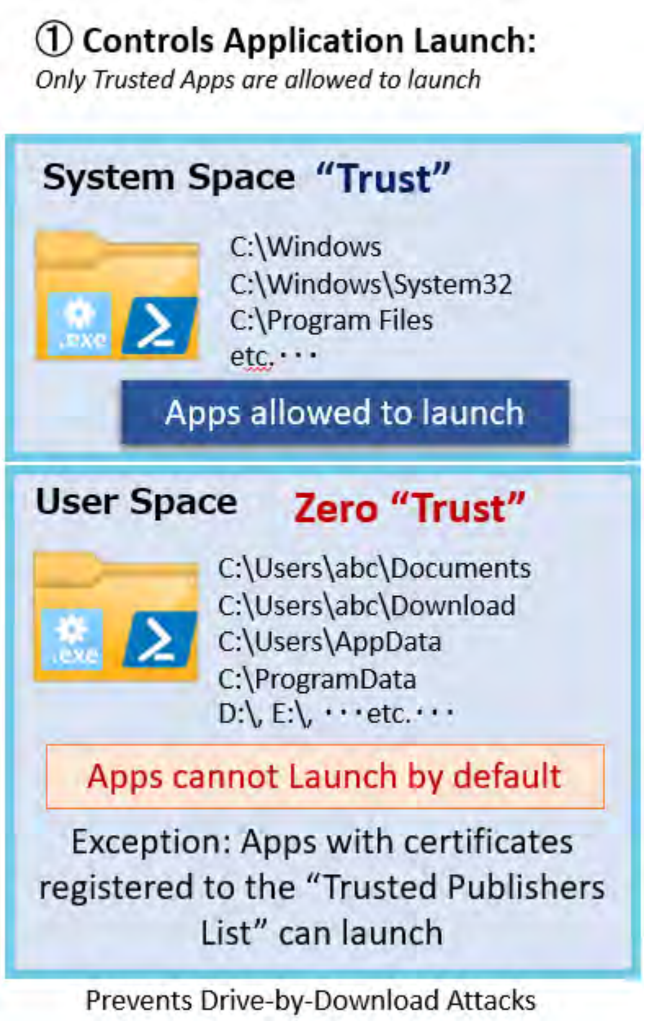
Benefits

- Precedes Windows Permissions and Windows Administrators cannot bypass protection
- Reduces unauthorized applications
- A program can't leave its "Bubble"
- Can't pierce other "Bubbles"
  - NotPetya 2017
  - LSAS protection



Strict Enforcement of System Space vs. User Space

- Hard separation of User Space and System Space
- Existing Applications can update themselves as normal
- Dynamic Protection – no constant enumeration



① **Controls Application Launch:**
Only Trusted Apps are allowed to launch

System Space “Trust”

C:\Windows
C:\Windows\System32
C:\Program Files
etc.・・・

Apps allowed to launch

User Space Zero “Trust”

C:\Users\abc\Documents
C:\Users\abc\Download
C:\Users\AppData
C:\ProgramData
D:\, E:\, ・・・etc.・・・

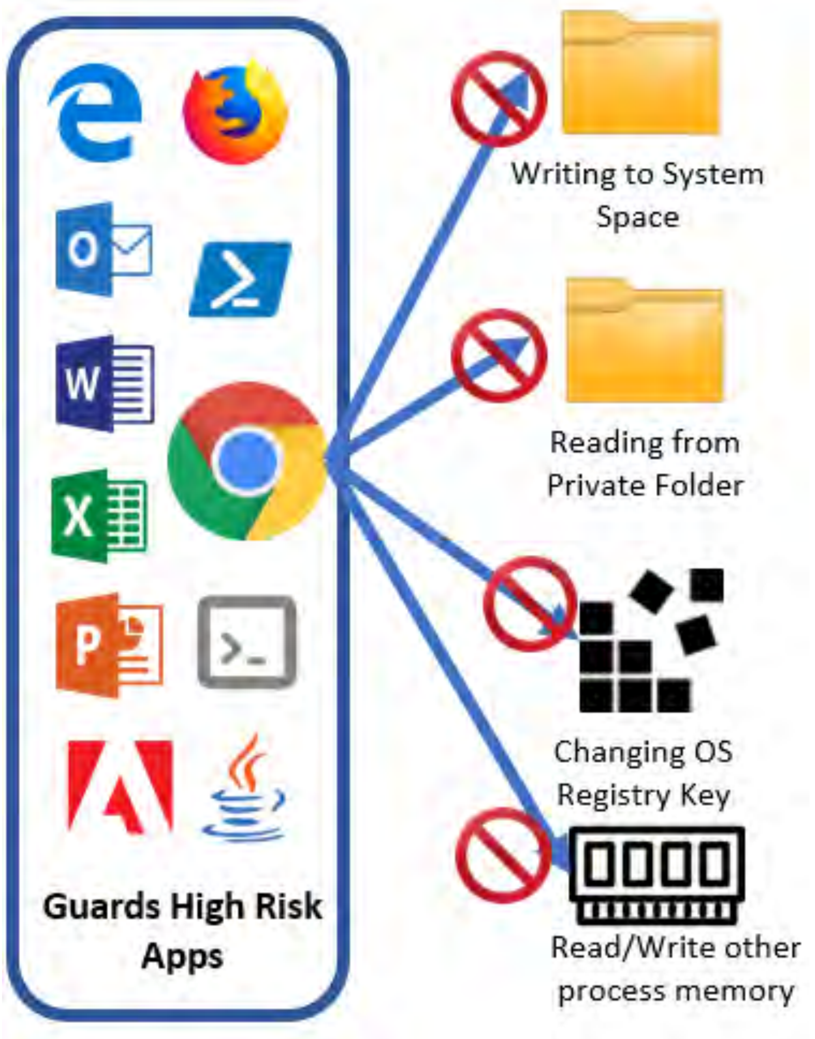
Apps cannot Launch by default

Exception: Apps with certificates registered to the “Trusted Publishers List” can launch

Prevents Drive-by-Download Attacks

How does this play out?

- Post-launch, Guard and MemoryGuard protections monitor Application processes and block prohibited actions
- With Isolation Technology, Prevents any harmful process from executing

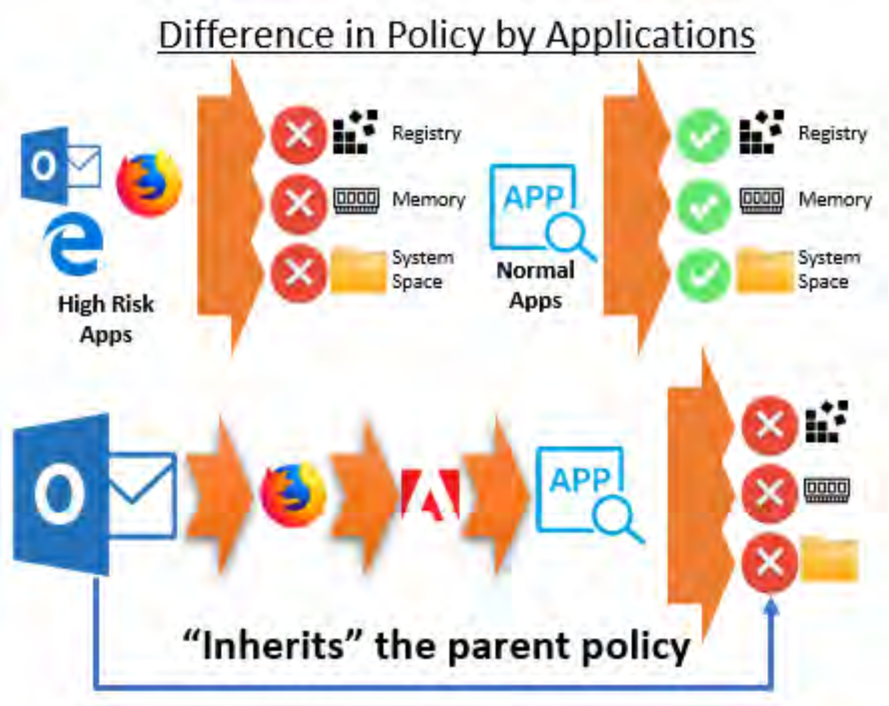


How does this play out?

- The original “parent” policy is inherited to the child and grandchild processes

(Example: Not 3rd Party App but Outlook policy is inherited)

- Dynamically protects systems from UNKNOWN & Advanced threats



Isolation and Containment

- Not a new concept
- Used by the US Federal Government for Decades
  - Network Segmentation
  - Data Pool Segmentation
  - Least privileged access
- Now applied to the Windows Operating Systems
  - Since 2014

Use in Businesses

- No unwanted applications
- No exploitable holes in the Operating System or Applications
- Emerging & Undetectable threats are no longer a risk
- No cyber end of life
- Lower reactive support needs

Not the “End All” Solution

- Networks are more than just Windows devices
  - What percentage of your network is Windows?

0% Detection

100% Prevention

Seeing is **Believing!**

- Visit our booth # 619
- Get a FREE AppGuard Shirt
- Get your questions answered
- Use the QR Code to register for our Technical Deep Dive

  on November 2nd, 2 PM CT