CSO Conference *& Awards*

Produced by CSO | IDC

Ransomware Resiliency with Application Segmentation

In memory of Zachary Campbell

CSO Conference & Awards

Penn Medicine

Produced by CSO | IDC

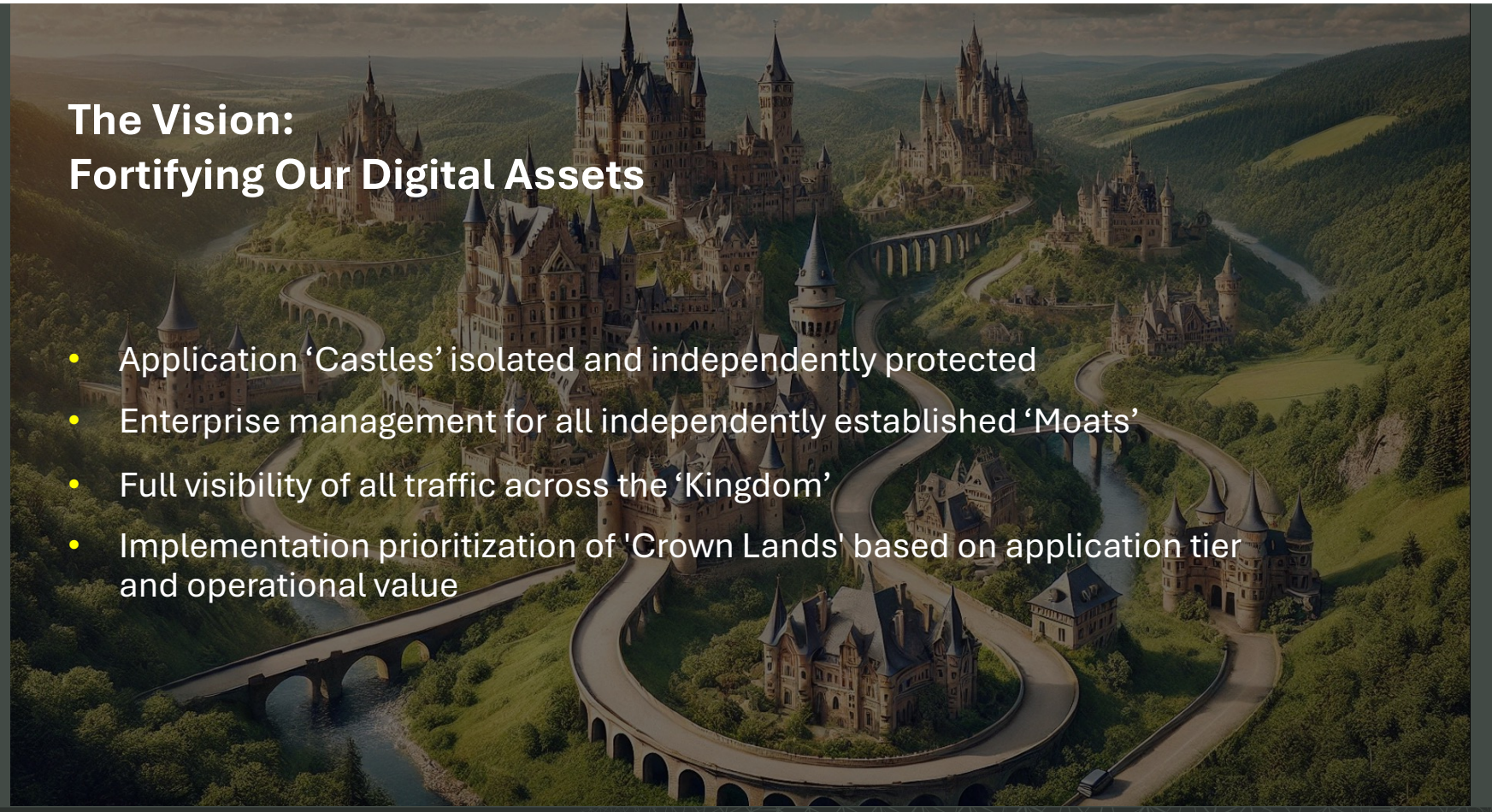
The Modern Threat Landscape

Top four ransomware spreading threats:

- Lateral movement (Pass the Hash, WMI)
- Misconfigured services (Open Shares, Webservices)
- Remote Desktop exposure
- Vulnerability exploitation

CSO Conference & Awards | Penn Medicine

Produced by CSO | IDC


The Vision:
Fortifying Our Digital Assets
• Application ‘Castles’ isolated and independently protected
• Enterprise management for all independently established ‘Moats’
• Full visibility of all traffic across the ‘Kingdom’
• Implementation prioritization of 'Crown Lands' based on application tier and operational value

Challenges and Opportunities: Preparing for Success

- Apprehension of new agent/technology
- Lack of application data flow knowledge, ownership and accountability
- Product maturity challenges for critical use cases
- Competing enterprise initiatives

Strategic Planning: Focusing on Resiliency

- Project management is critical to 'herding cats'
- Establish small wins to build on for bigger wins
- Measure twice/cut once
- Focus on the highest value assets/applications to bring immediate benefit

Building the Foundation: Application & Server Inventory

- ‘What is in it for me’ application inventory
- Developed a user-friendly ‘everyone’ portal for asset verification
- Full IS push to track verification, and validate asset ownership
- Maturing server request/build process

The Technology:
Micro-segmentation Implementation

- At scale Microsoft Windows Firewall management tool
- Step Up Security – Idle, Visibility, Full Segmentation
- Graphical view of data flow with historical traffic monitoring
- Data driven Ransomware Resiliency metrics & scoring

Overcoming Obstacles

- Application administrators are not system administrators
- Communication is a double edge sword
- Garbage In – Garbage Out
- Very long, slow process

Partnership & Collaboration:
Security Solutions are Enterprise Solutions
• Building a user-friendly asset management portal promotes teamwork
• Promoting a culture of asset management benefits everyone
• Helping IS Operations in turn helps Cybersecurity
• Application Segmentation is an Enterprise Project not a Cybersecurity Project
CSO Conference & Awards
Penn Medicine
Produced by CSO | IDC

Results & Impact: Disciplines, Dollars and Defense

MATURED SERVER BUILD AND APPLICATION INVENTORY PROCESS

DECOMMISSION SAVINGS OF 600K

INSECURE CONFIGURATIONS BLOCKED BY DEFAULT (OPEN SHARES)

ABILITY TO INTRODUCE TARGETED CONTROLS (RDP TO DCS)

Looking Ahead:
A Road to Resiliency
• We've only just begun - a small stretch of road is behind us
• Not a quick one-time trip - it's a long journey
• Paving the way for cultural changes across the enterprise
• Multiple stops along the way, spanning multiple years