Modernization Challenges For The IT Infrastructure At The National Ignition Facility

17th International Conference on Accelerator & Large Experimental Physics Control Systems (ICALEPCS)

Allan Casey
NIF&PS IT Manager

October 5 – 11, 2019

LLNL-PRES-791807
This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract DE-AC52-07NA27344. Lawrence Livermore National Security, LLC

Lawrence Livermore National Laboratory

NIF is successfully taking 400 shots per year! What is the problem?

- 2009 Infrastructure
  - XP VxWorks 5.4
  - Solaris 10
  - Old protocols: NFSv2, rsh, NIS
  - End-of-life hardware

- 2019 Infrastructure
  - OEL7, Java8, Oracle RAC
  - Windows 2016
  - Cisco UCS/Nexus/MDS
  - NetApp AFF storage
  - Docker / Kubernetes
  - Desire for easy user access

- Update Expectation
  - Upgrade every 3-5 years
  - Patch weekly if not daily
  - Migrate to the latest technologies
  - Do all of the above with no downtime!

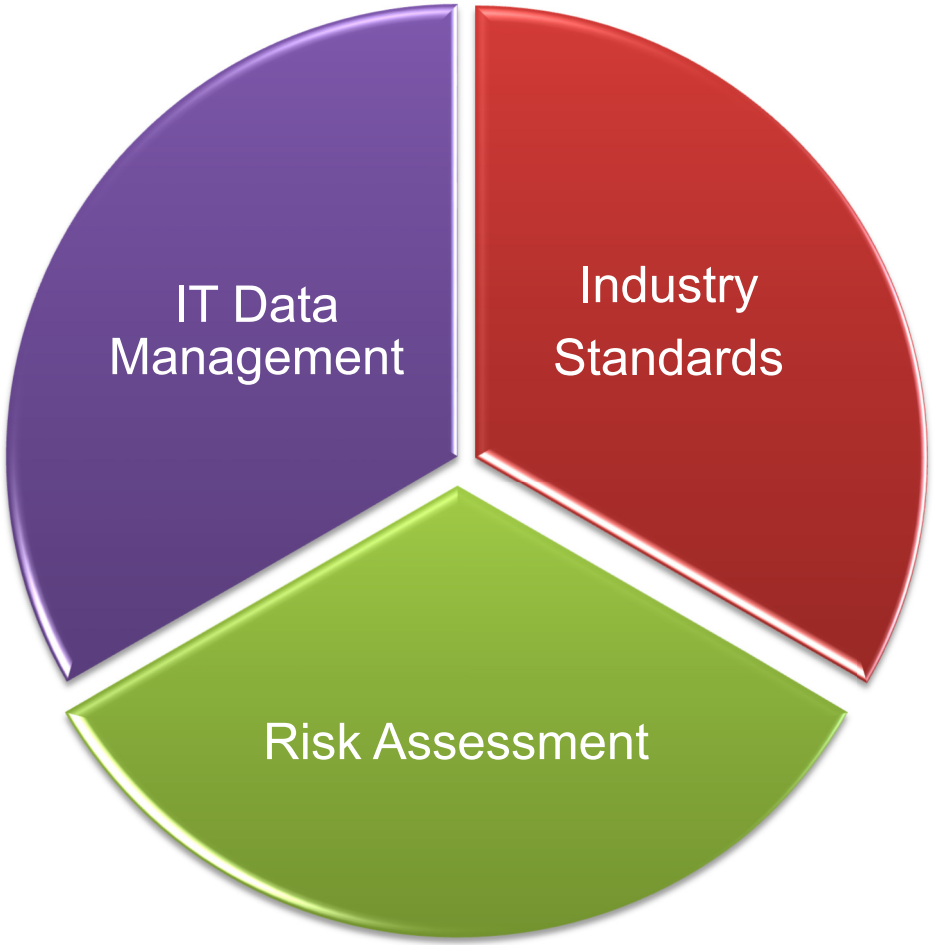
- Update Reality
  - Upgrade some things every 5-7 years.
  - Patch as operations and applications will allow
  - Migrate only if there is a strategic advantage.
  - Many maintenance outages over many years!

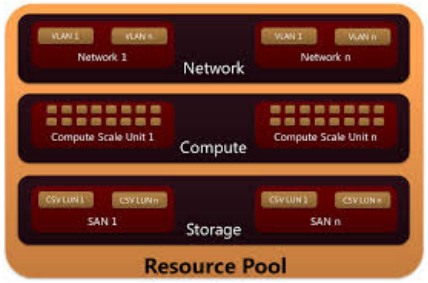
NIF is still running some hardware that was installed during facility commissioning.
How do you manage these conflicting pressures?

Revisit how to think about the whole IT problem, not just the existing physical infrastructure

Access,
Behavior,
Credentials

Hardware,
Software,
Configuration,
Vulnerabilities

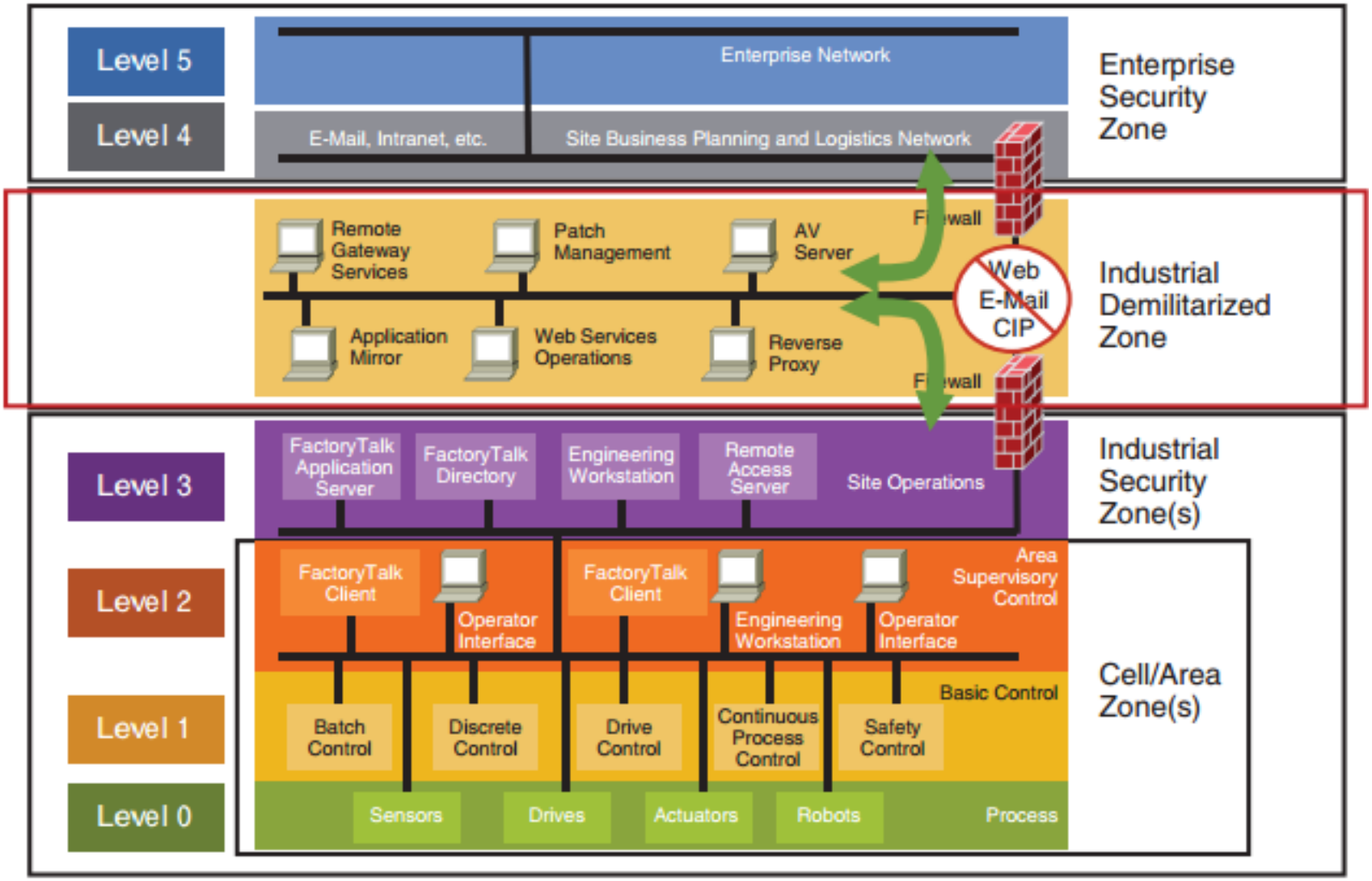




$$$

Are all the assumptions made when infrastructure was originally conceived, still valid?

Purdue Enterprise Reference Architecture uses network segmentation to separate access layers

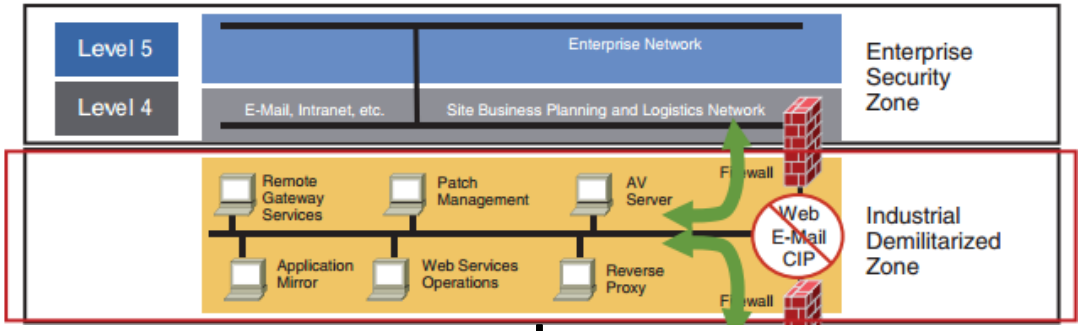


Revalidate the network design against the Industry Standard

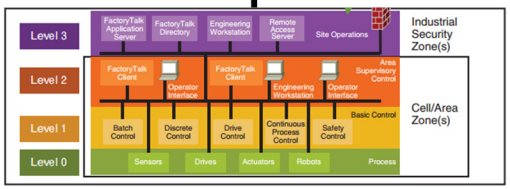
One of the considered options for NIF Cyber Security Network Model is to separate each of the environments below the DMZ

L5: Institution
(VPN/Email/Apps)

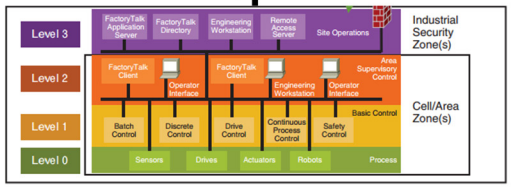
L3 NIF DMZ
(Developer, SysAdmin, Priv Access Admins for ICS/ICCS)



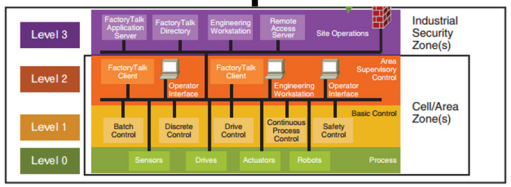
L4 NIF&PS IT Data Center
(Web Apps/File Access)



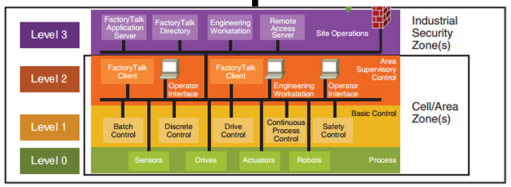
Dev/Int/QA



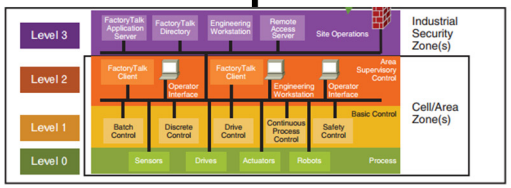
Production



Dev/Int/QA SCADA



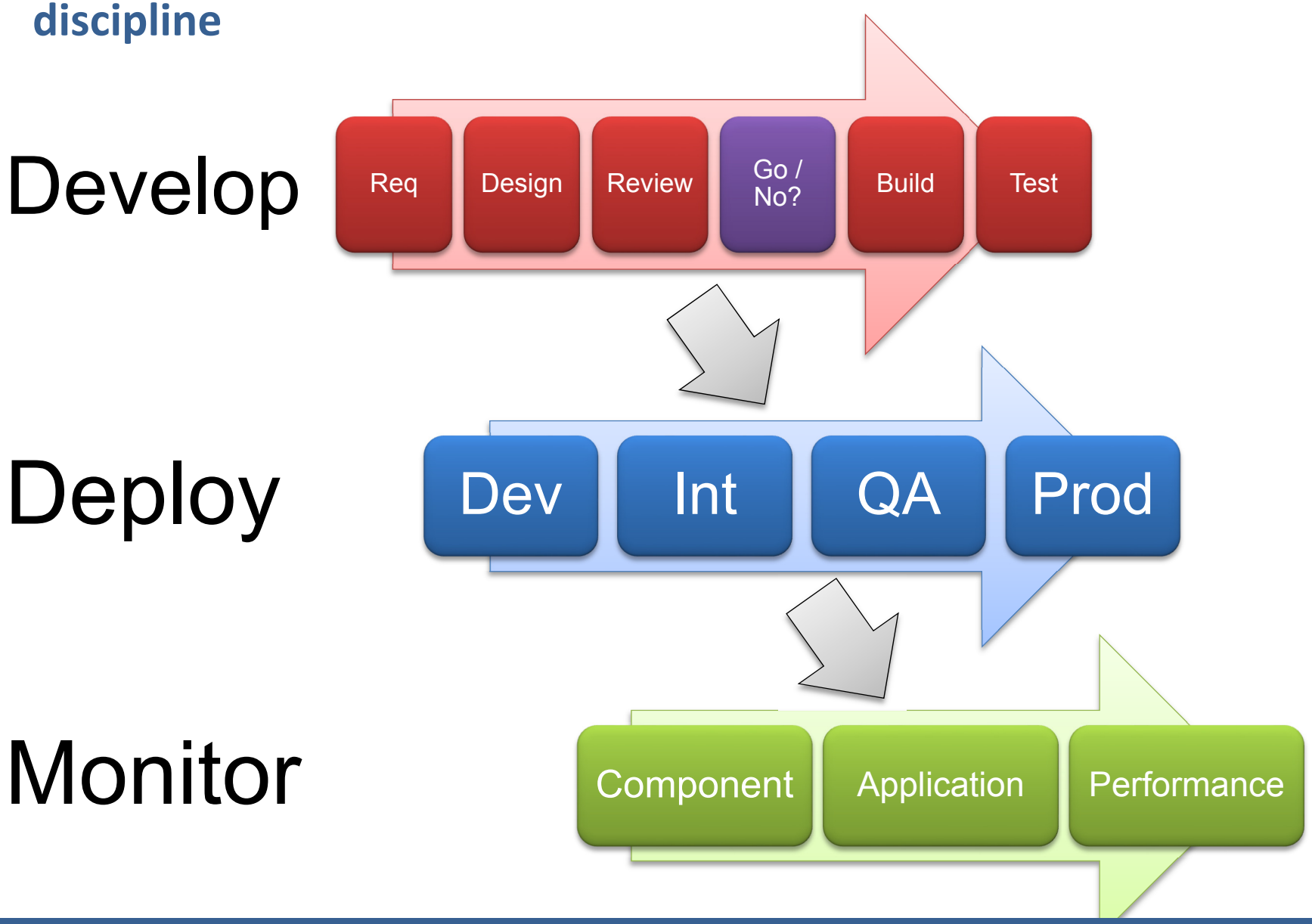
Auxiliary Facilities SCADA



B581 SCADA

Ease of user access may need to change due to risks associated with it

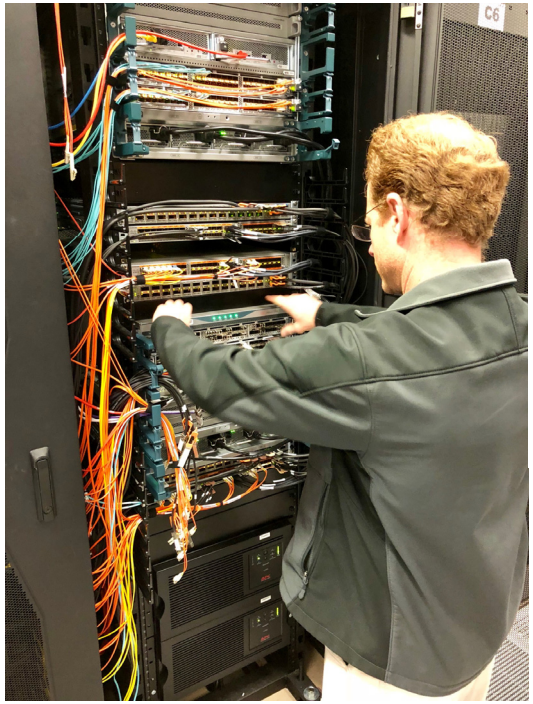
Change the IT product delivery lifecycle to an Engineering discipline



Deliver IT solutions following standard SW / HW development practices

Homogenization and simplification via standardization of IT components

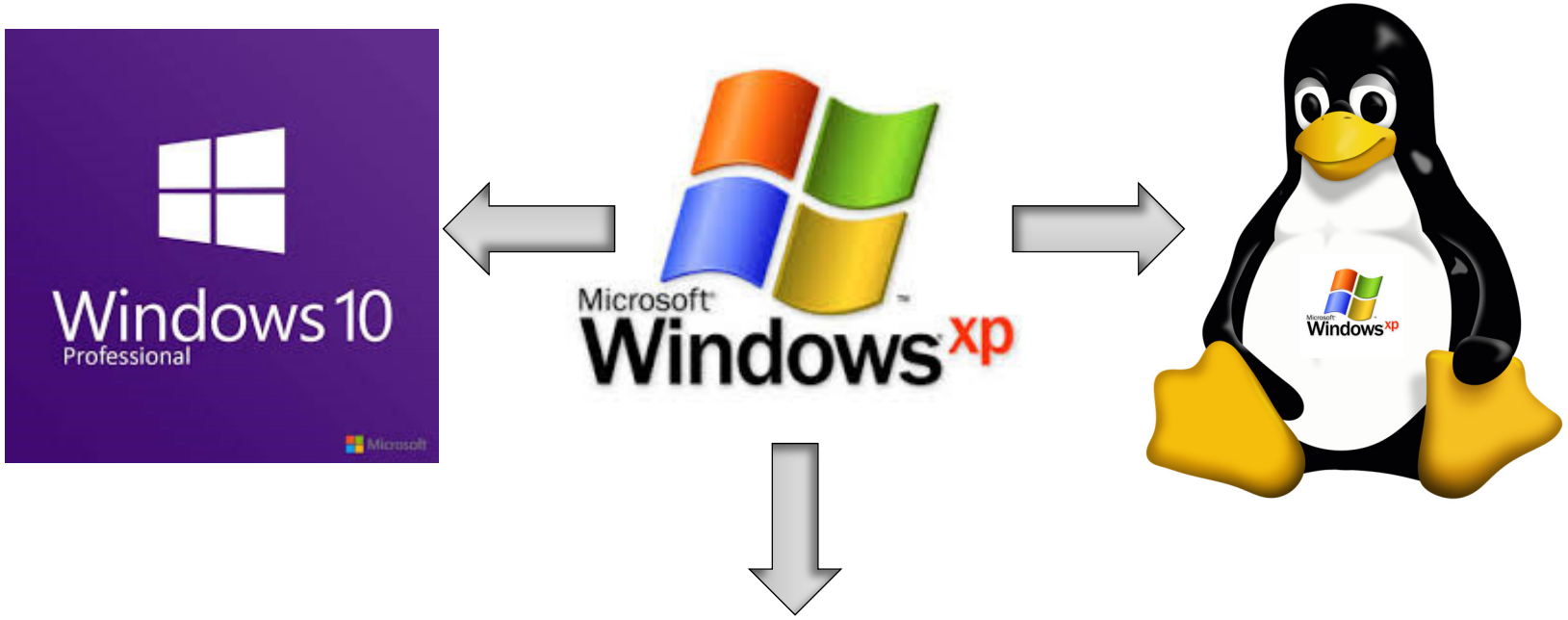
- Before:
  - Servers hand built by highly skilled Sys Admins
  - Multiple versions of equipment creating a sparing / replacement problem
  - Complex patching sequence due to variance
  - Every environment is different, lowering agility and increasing training needs



- After:
  - Servers built automatically to a common design
  - Component based “plug in” architecture
  - Simplification, thus quicker and more reliable patching
  - Knowledge applies to all environment and projects
  - Free skilled Sys Admins to work on “value added” activities

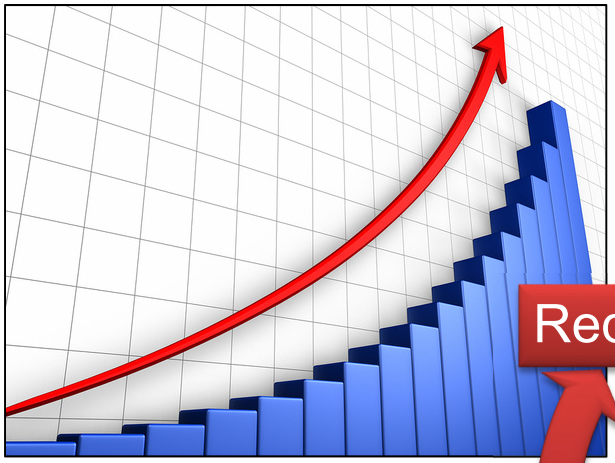
Reduce the effort to maintain the Data Center; move focus to optimization

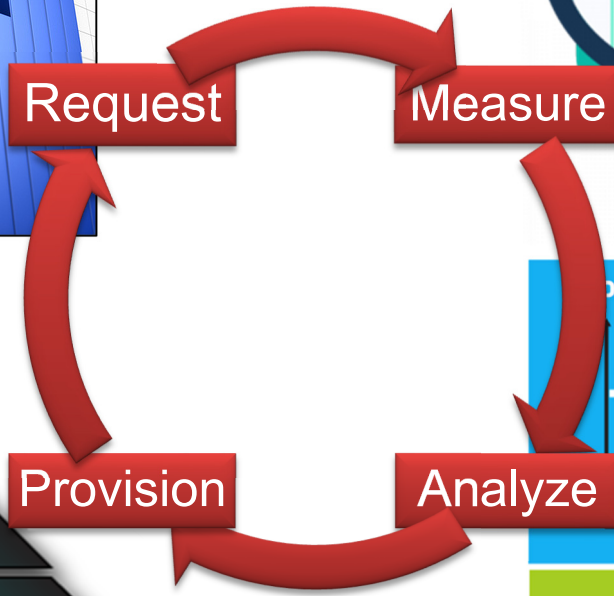
Collaborate with users where IT can not be migrated to standard components

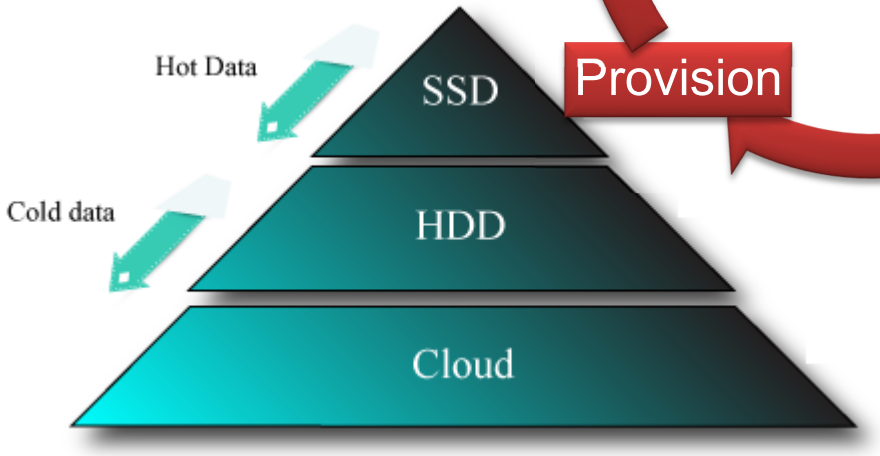


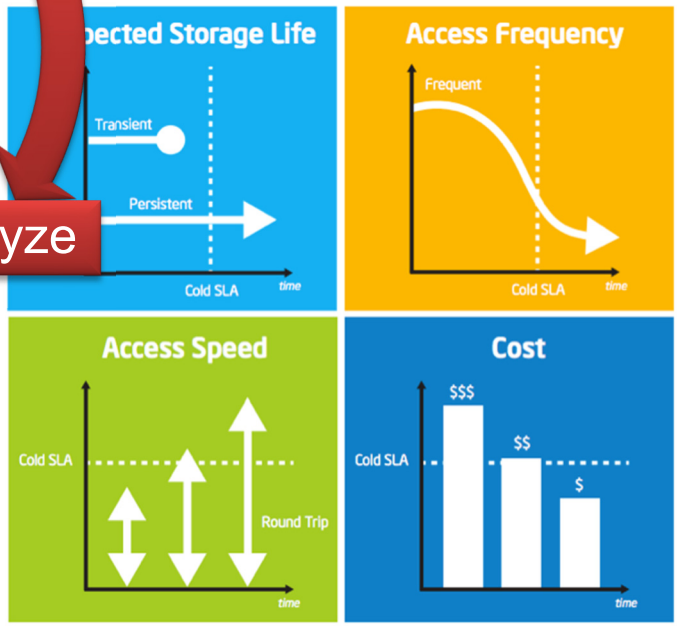
Provide a graded approach solution to minimize risk and maximize business value

Storage is increasingly one of the biggest cost drivers in the data center



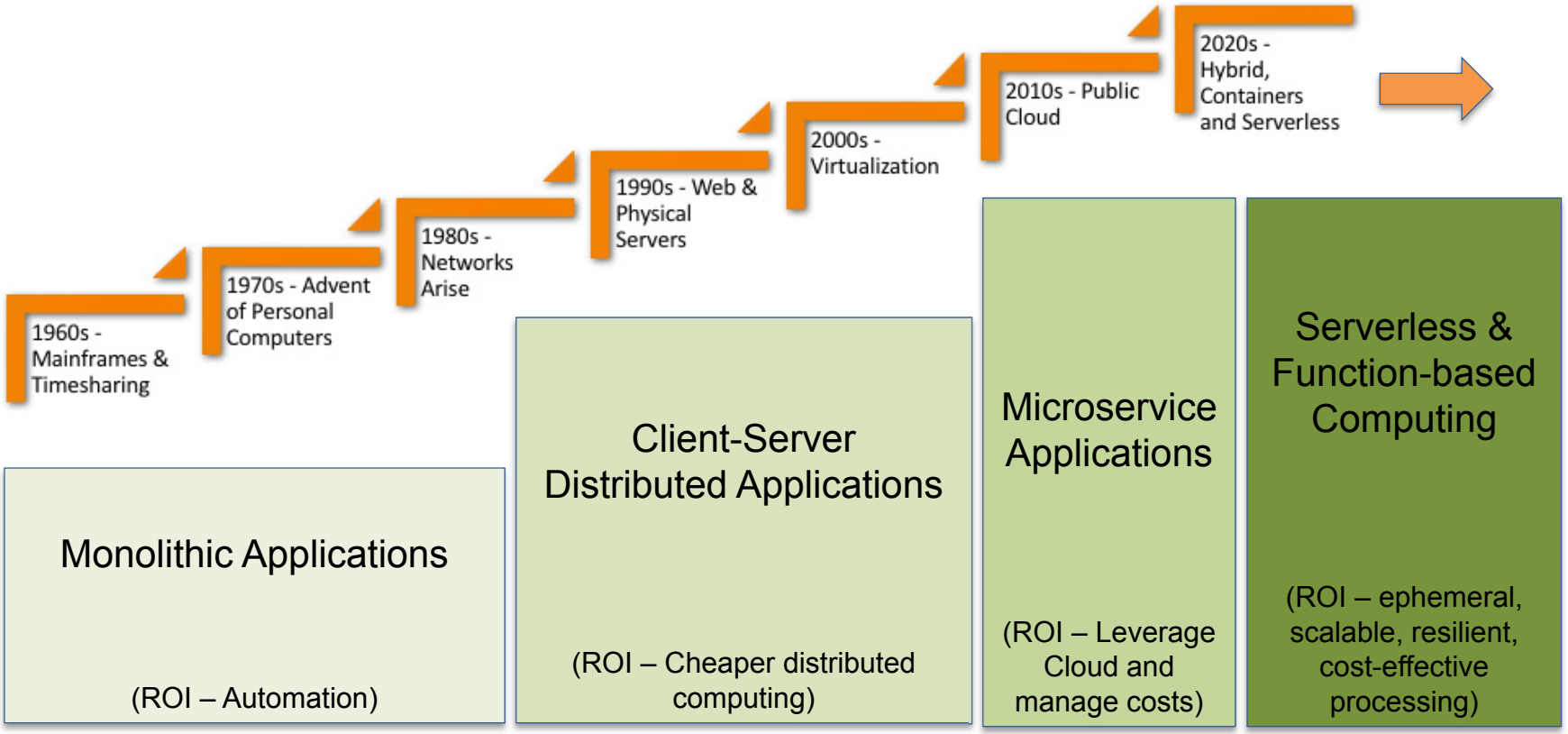






Analysis of data is required in order to optimize the use of all storage options

Updating the Mid Tier – Is Docker/Kubernetes yet another paradigm or a computing evolution?



With each evolution it is getting more difficult to realize the ROI

Modernizing legacy applications is not a simple lift and shift to the Cloud

- Not all legacy applications are right for the cloud
- Stay away from refactoring old applications that are built using very old languages and databases
- Stay away from applications that were poorly designed as they take a greater amount of work
- Stay away from applications that tightly coupled to the data store – unless we are willing to move that too

V

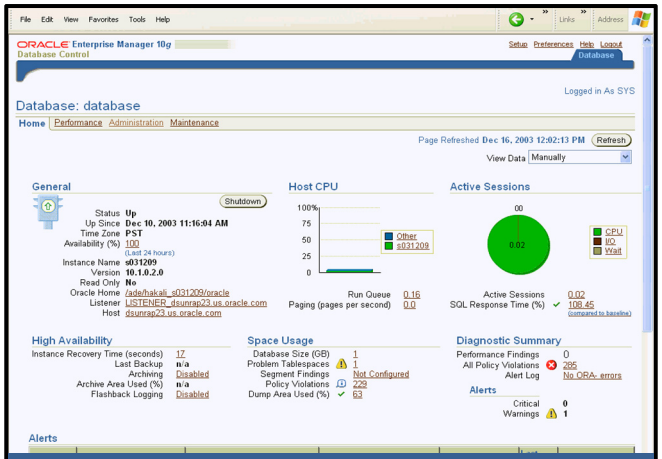
If the ROI works, and the use case fits, then migrating may be a great idea

Take a DevOps philosophy when working with the SW teams

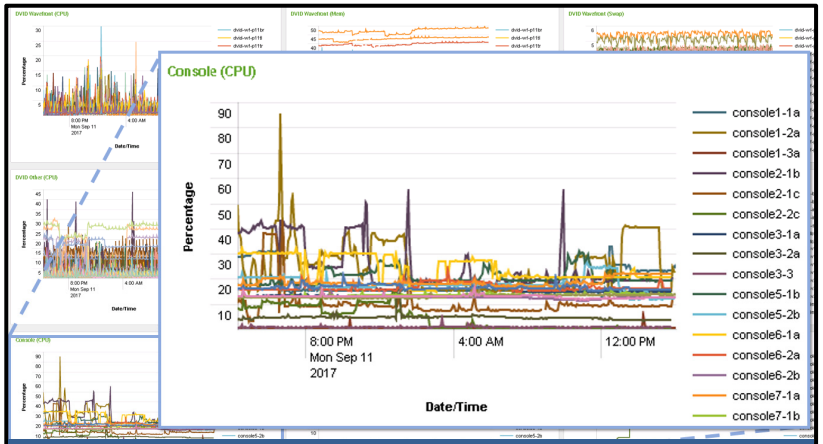
- The Mid tier is common source of attack vectors
- Demanding updates from SW does not work!
- Integrate with the SW team
  - Understand their issues
  - Be part of the solution rather than be another issue to resolve
- Have IT work on the mid-tier
  - Leave SW to do their own work
- Work the SW team to:
  - Prioritize the updates that they need
  - Introduce the tools they want to use

Help the software teams help themselves to improve IT security

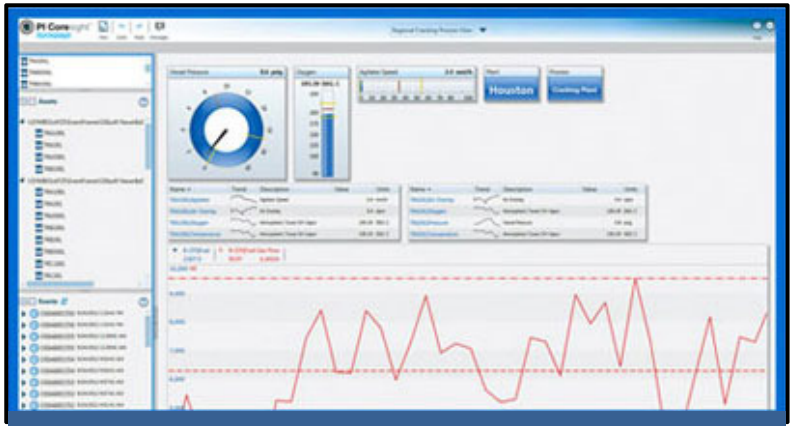
Monitoring & analysis tools need to be chosen to address specific needs of consumers



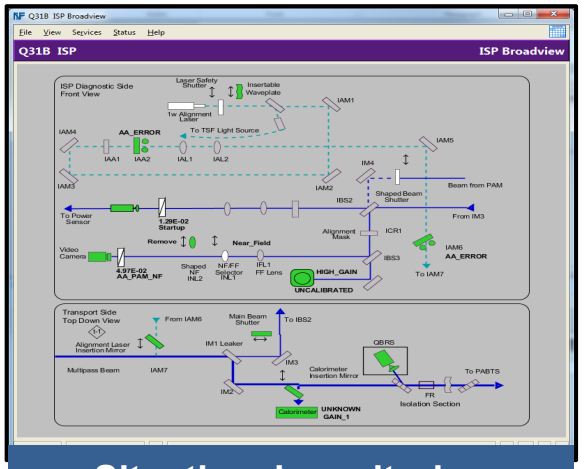
Tactical infrastructure monitoring



Strategic analytical analysis



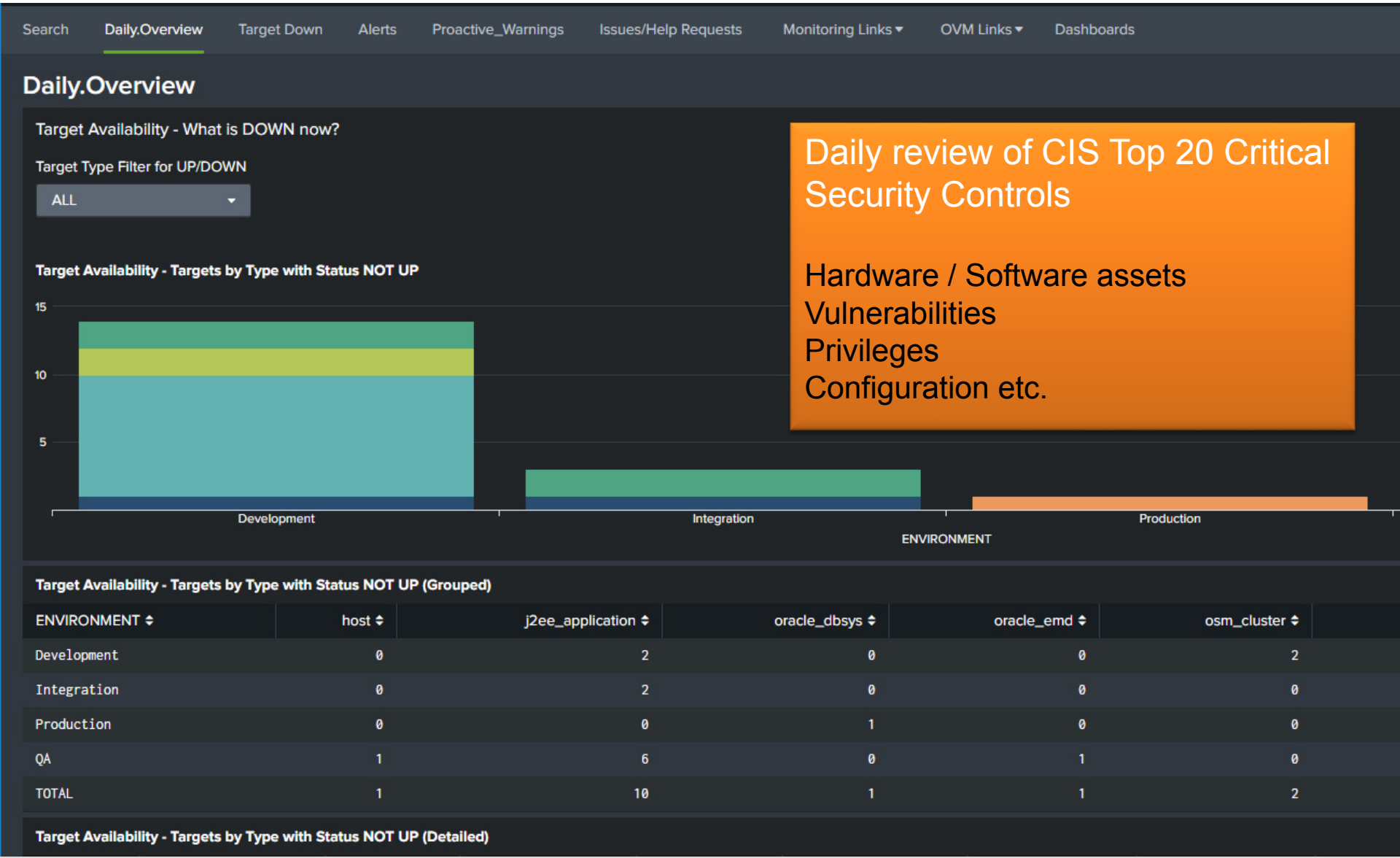
High data rate trend analysis



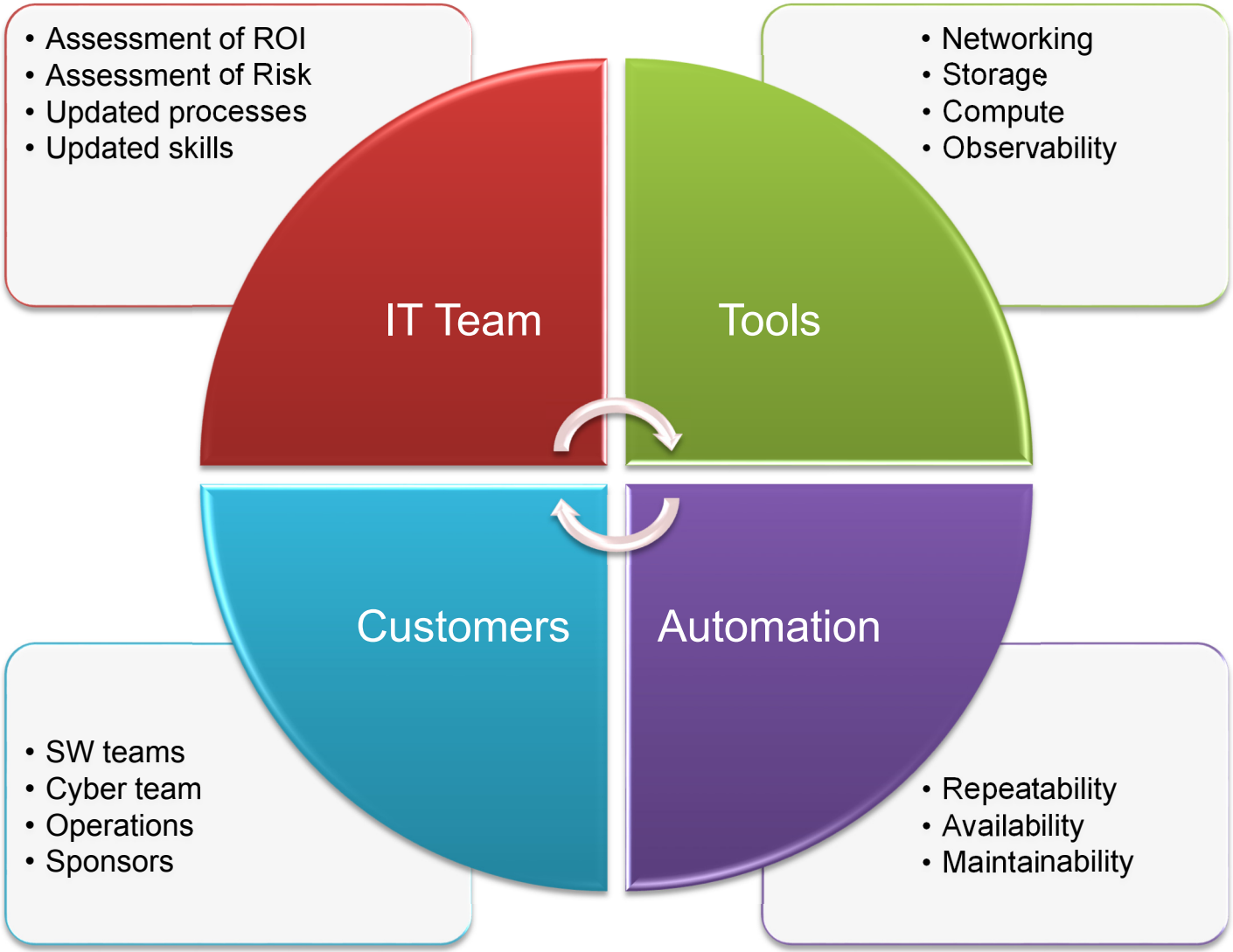
Situational monitoring

Difficult to find a single tool that addresses the needs of everyone

Whatever gets monitored needs to be reviewed and then appropriate actions generated



Evolving the infrastructure is hard but not impossible



All stakeholders need to work together to maximize investment

Lawrence Livermore
National Laboratory