CiTRIX®

Architecting the workspace for high security

Kurt Roemer
Chief Security Strategist, Citrix

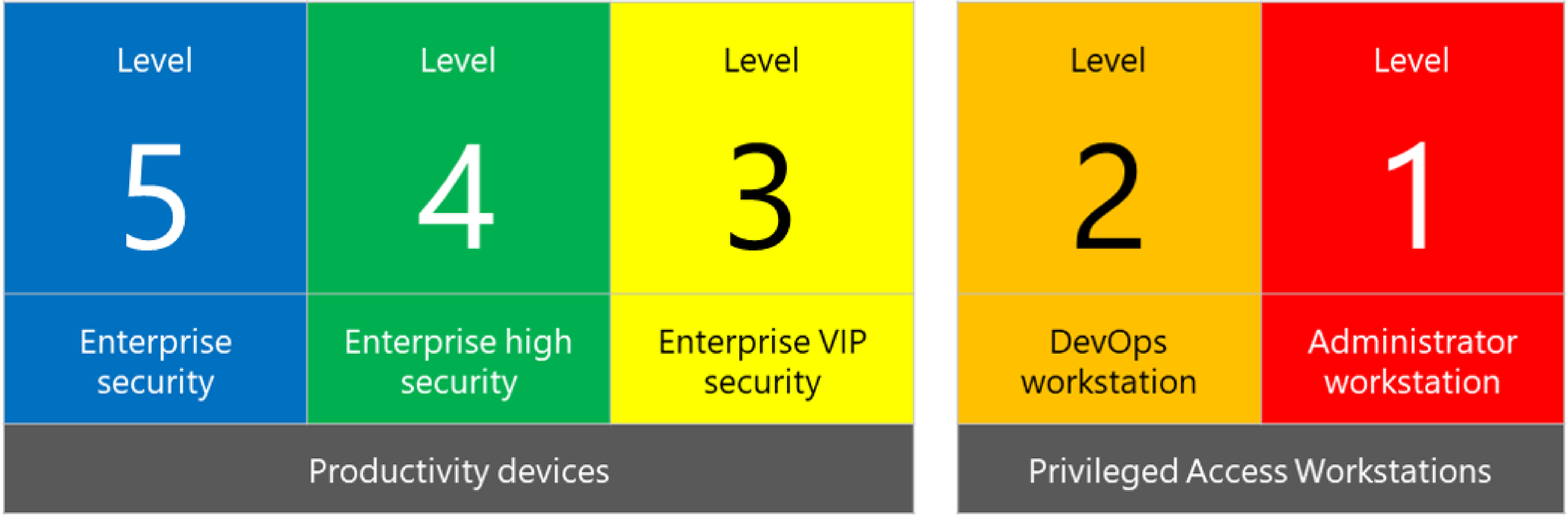
Mike Nelson
Solution Technologist, Rubrik

MAY 23, 2019

#CitrixSynergy #FutureOfWork @nelmedia

Our Virtual Guest Presenter – "Joan"

Microsoft SECCON Framework



Level 5	Level 4	Level 3	Level 2	Level 1
Enterprise security	Enterprise high security	Enterprise VIP security	DevOps workstation	Administrator workstation
Productivity devices			Privileged Access Workstations	

As a highly privileged user,
you have the power to
create, enhance and destroy
- and so does anyone
who can impersonate you,
use your tools, or otherwise
abuse your powers

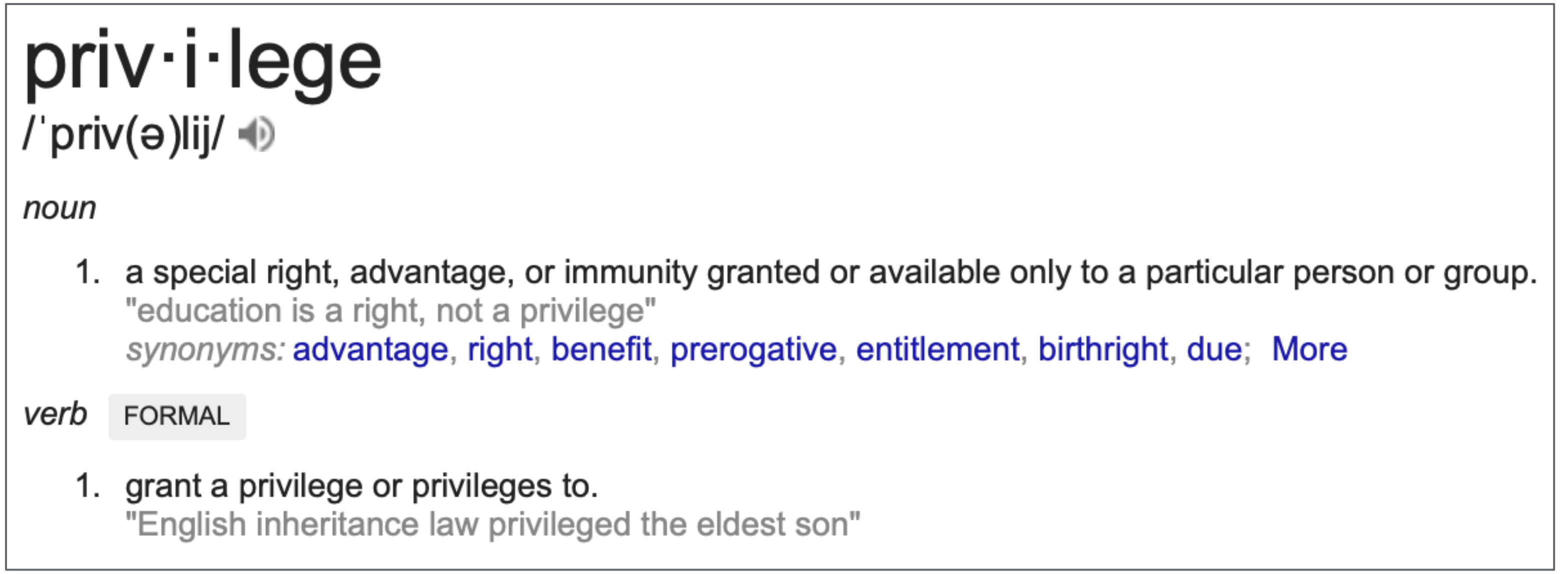
How can productivity and experience be optimized while protecting all the resources you’ve been entrusted with?

Topics of Discussion

- Defining and defending privilege
- Design considerations for a privileged workspace
- How to dynamically manage contextual trust
- Thoughts, tools and techniques focused on optimizing security, productivity and costs

What is Privilege?

And where do Privileged Workers have direct impact?



priv·i·lege

/ˈpriv(ə)lij/

noun

1. a special right, advantage, or immunity granted or available only to a particular person or group.
   "education is a right, not a privilege"
   synonyms: advantage, right, benefit, prerogative, entitlement, birthright, due; More

verb FORMAL

1. grant a privilege or privileges to.
   "English inheritance law privileged the eldest son"

Financials

Operations

Compliance

Reputation

Strategy

Safety

Who is Privileged?

IT Professionals Network Admins System Admins DBAs DevOps Citizen Developers App Owners Auditors

CSO/CISO Security Teams LoB Leaders Human Resources Legal Supply Chain 3rd Parties Board Members

Threats Targeting Privilege

- Phishing, Ransomware and Email Compromise
- ID Theft, Credential Stuffing and Password Spraying
- Botnets and APTs (Advanced Persistent Threats)
- Social Engineering and Recruiting Malicious Insiders
- Hacktivism and Cyberterrorism
- Cyberboarding, Apathy and Information Overload
- Cyberbullying, Social Reputation Damage and Deepfakes

Complexity is the Enemy of Security, Productivity and Cost

The *privileged workspace* brings meaning to work by automating and augmenting the context of work for highly privileged workers and teams

A (young) Sys Admin's Day

ASF
ASF

Thoughts by Some Really Smart People

"On paper, securing the Privileged Workspace is the easy part. It's the people part that is hard."

Brian – CISO, Insurance Industry

Thoughts by Some Really Smart People

> ***“Privilege causes problems. And depending on how those problems are handled, they very well could be career ending ones.”***

Denis – Independent Security Consultant and Author

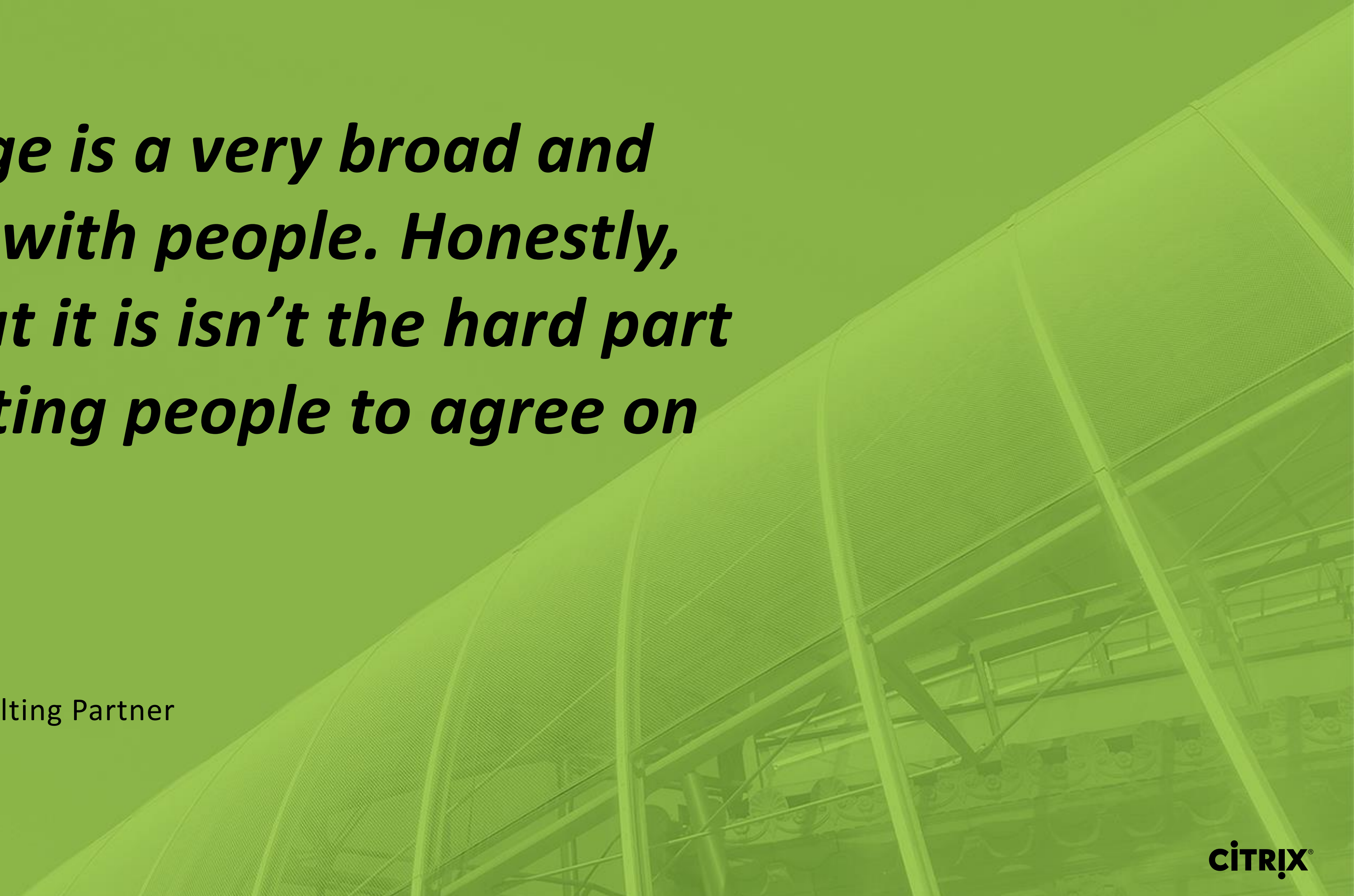
Thoughts by Some Really Smart People

“Everyone is privileged, from the basic user to the CTO. What matters is what data is being accessed, what app is being used, or what physical space they are in when it’s used.”

Vinesh – Systems Administrator, Hospital Healthcare

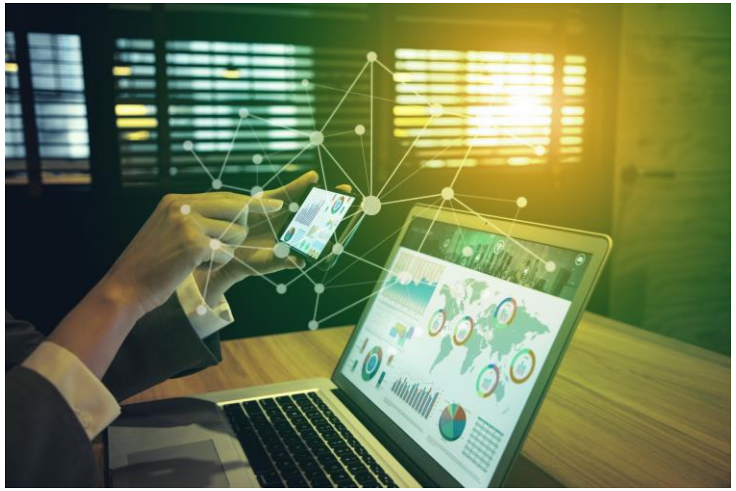
Thoughts by Some Really Smart People

"Security privilege is a very broad and diverse subject with people. Honestly, identifying what it is isn't the hard part for me, but getting people to agree on it is."



Mark – Lead Security Analyst, Consulting Partner

Design Considerations for a Privileged Workspace



- Integrates people, process, technology and strategy, bridging physical and cyber
- Business-outcome focused on optimizing security, productivity and costs
- Built upon a foundation of *Zero Trust*
- Identity-enabled and persona-enlightened
- Automated and augmented for superpowers
- Continuously evaluated for optimal service delivery and mission success
- Situationally aware and risk-appropriate with dynamic resource delivery management

Dynamically Deliver Resources

Direct

Allowing direct (native) access to resources has no intervening technologies to slow or impede productivity, at the loss of visibility and control

Proxies

Proxies intervene in the traffic stream and can provide useful features including content inspection, filtering, rewrites, redirects and brokering

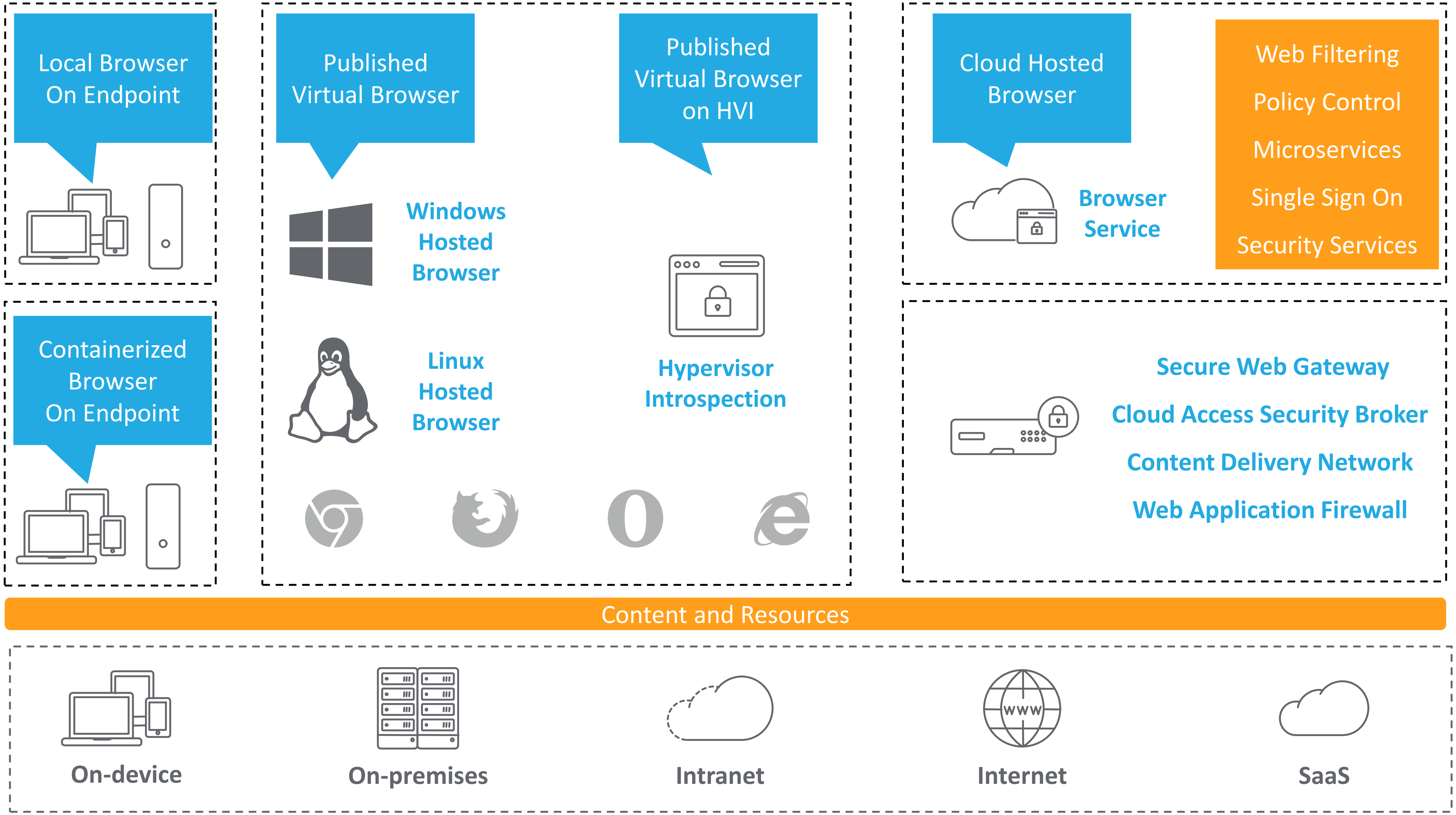
Virtualized

Virtualization provides for abstraction and isolation of resources across applications, browsers, desktops, operating systems and infrastructure

Containerized

Containers and enclaves protect applications, content and policies for mobile, distributed and offline use cases

Resource Delivery Example: Web Browsing



Local Browser On Endpoint

Containerized Browser On Endpoint

Published Virtual Browser

Windows Hosted Browser

Linux Hosted Browser

Published Virtual Browser on HVI

Hypervisor Introspection

Cloud Hosted Browser

Browser Service

Web Filtering

Policy Control

Microservices

Single Sign On

Security Services

Secure Web Gateway

Cloud Access Security Broker

Content Delivery Network

Web Application Firewall

Content and Resources

On-device

On-premises

Intranet

Internet

SaaS

The 5W's of Context

Who – is trying to get in?

What – are they accessing?

When – is this happening?

Where – in the world are they?

Why – do they need access?

Thoughts, Tools and Techniques

Deliver curated, personalized and prioritized insights

Intel - What's going on that's projected to impact current and planned work. From internal and external sources and services.

Threats - Current and evolving conditions, sources, expected consequences and forecasts for all relevant situations. Includes upstream threats and those from 3rd parties that will impact your ability to deliver.

Experience - What to expect throughout your workweek, including conditions, timeframes, dependencies, constraints and incidents. Insights on how to plan for the optimal experience and avoid disruptions.

Joan’s Interview Takeaways

- The Public Sector isn’t that much different from the Private Sector
- Layers of permissions, applications, processes, and policies
- Unfiltered access to privileged information, both personal and professional
- The Automation percentage *(20% is generous)*
- Life would just be easier with automation

Thoughts, Tools and Techniques

Evolve through Automation and Augmentation

- ***Automate the Mundane!***
- Guide work to be situationally risk-appropriate and contextually relevant
- Coach desired behaviors with personalized, interactive review and assistance
- Focus analytics on determining true ownership and appropriate privileges
- Sustain resilience against toxic disruptions and constant distractions
- Extend physical capabilities with robots, IoT, augmented reality and virtual reality
- It’s time to launch your *Digital Twin*!

Thoughts, Tools and Techniques

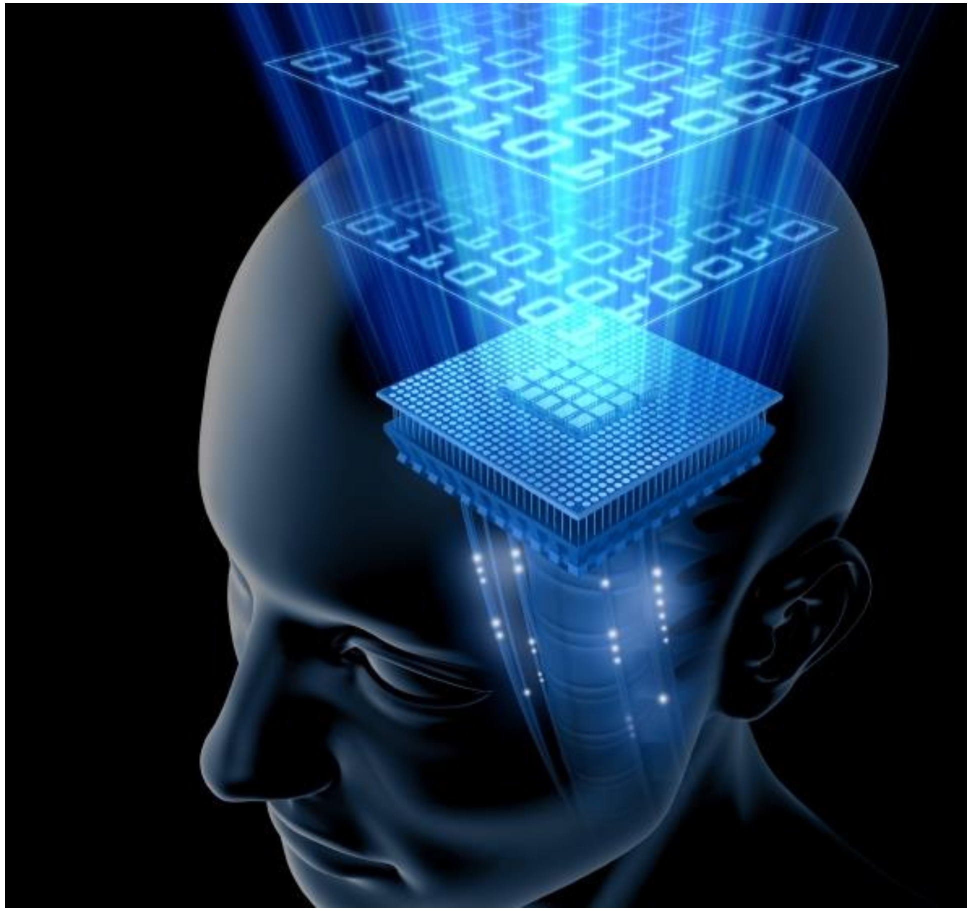
- ***You're too privileged for passwords – use MFA!***
- Focus beyond just ***access*** to managing lifecycle ***usage***
- Integrate DLP, IRM, PAM, PUM, UEBA, CASB, WAF
- Actively reduce and test the privileged attack surface
- Know when to change the locks and keys
- Consider Counterintelligence and Deception agents
- Containerize and virtualize email and hardened browsers
- Express *Configuration as Code* and embrace *Culture as Code*

Key Takeaways

- **Privilege is the currency of *Digital Transformation*.** The good guys know this – and the bad guys know this. Protect your privileges. And especially protect your highly-privileged workers.

- **Personas are the new perimeter.** Express aspects of your identity only relevant to your current mission, risks and rewards.

- Envision and embrace the Privileged Workspace as a massively disruptive force for transformation. **You now have *superpowers* – realize them soon and use them wisely!**



Thank You!

Kurt Roemer

www.linkedin.com/in/kurtroemer

Mike Nelson

@nelmedia

www.linkedin.com/in/nelmedia

https://www.citrix.com/content/dam/citrix/en_us/documents/ebook/envisioning-a-smarter-way-to-work.pdf

Envisioning a smarter way to work

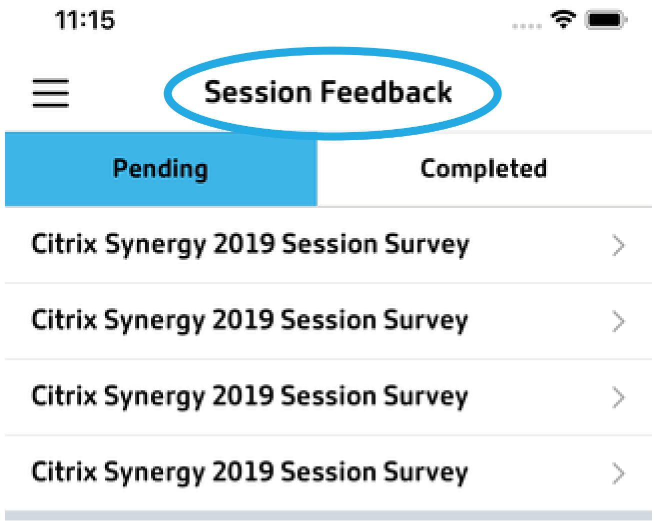
Guide, automate, and optimize work with an intelligent workspace

Before you leave…

- Conference surveys are available via email and in the Synergy mobile app starting Thursday, May 23 at 9:00a.m. ET
- Watch sessions on demand beginning Wednesday May 22, 2019 at www.citrix.com/SynergyTV
- Download presentations starting Monday June 3, 2019 from your *My Synergy* Account

Rate this session in the mobile app and play GameOn!

- Tell us what you think, we want to know!
  - Get 25 points!
- Surveys are based on entrance scanning
  - Once you scan into a session, that session will pop up on the mobile app
  - Scanning in allots you 2 GameOn points!
- The mobile app will show you pending feedback and completed feedback
  - Completing a survey allots you 23 GameOn points!



11:15

Session Feedback

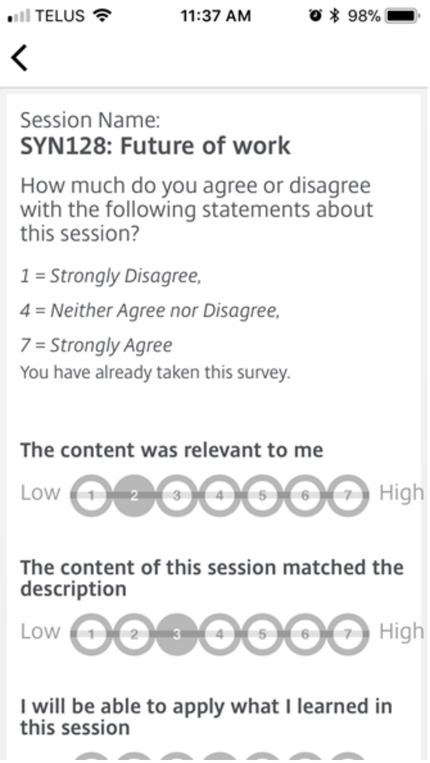
Pending | Completed

Citrix Synergy 2019 Session Survey

Citrix Synergy 2019 Session Survey

Citrix Synergy 2019 Session Survey

Citrix Synergy 2019 Session Survey



TELUS 11:37 AM 98%

Session Name:
SYN128: Future of work

How much do you agree or disagree with the following statements about this session?

1 = Strongly Disagree,

4 = Neither Agree nor Disagree,

7 = Strongly Agree

You have already taken this survey.

The content was relevant to me

Low 1 2 3 4 5 6 7 High

The content of this session matched the description

Low 1 2 3 4 5 6 7 High

I will be able to apply what I learned in this session

Tweet about this session with hashtags

#CitrixSynergy and #FutureOfWork

CITRIX®