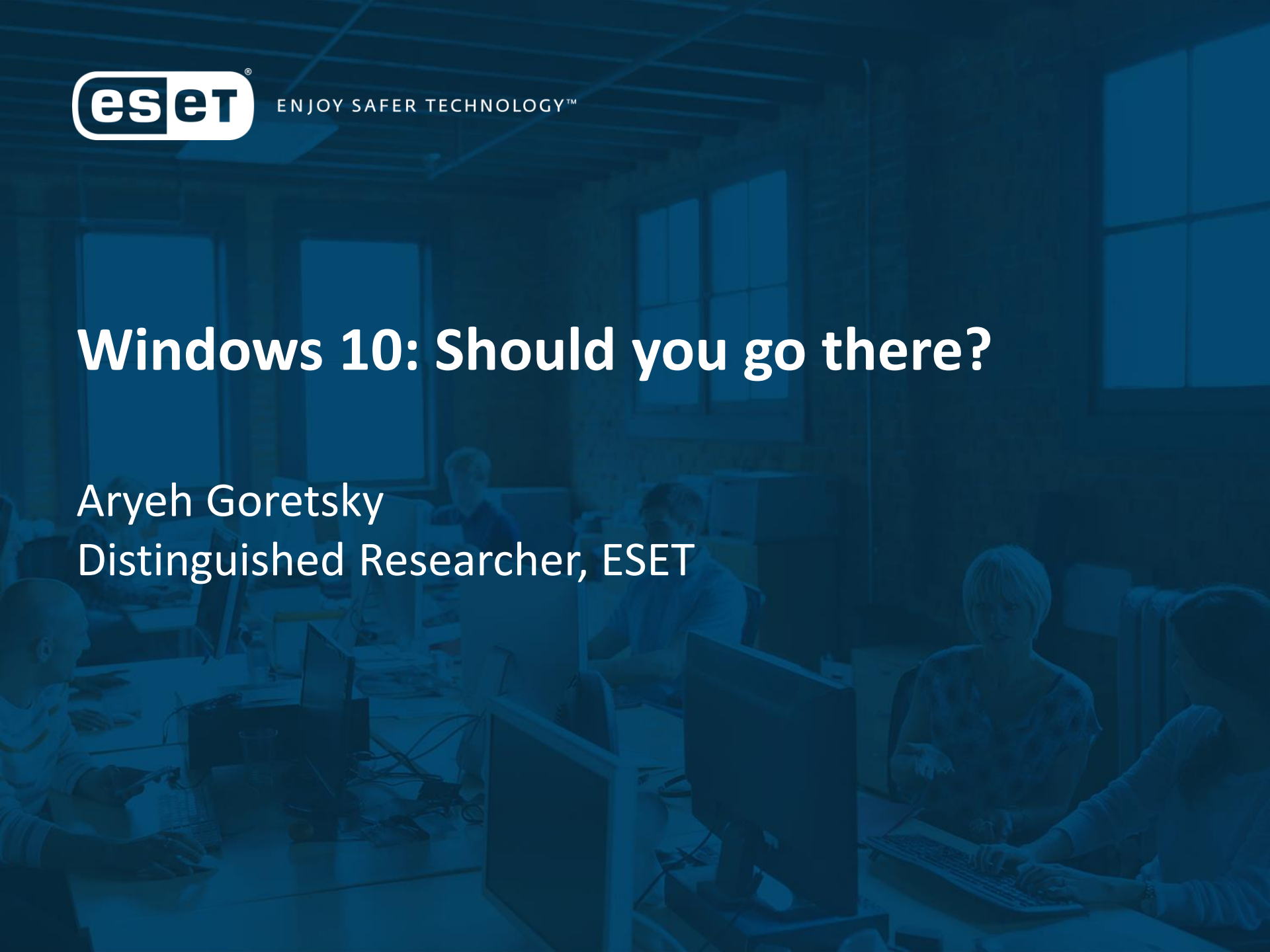


Windows 10: Should you go there?

Aryeh Goretsky
Distinguished Researcher, ESET

ENJOY SAFER TECHNOLOGY™

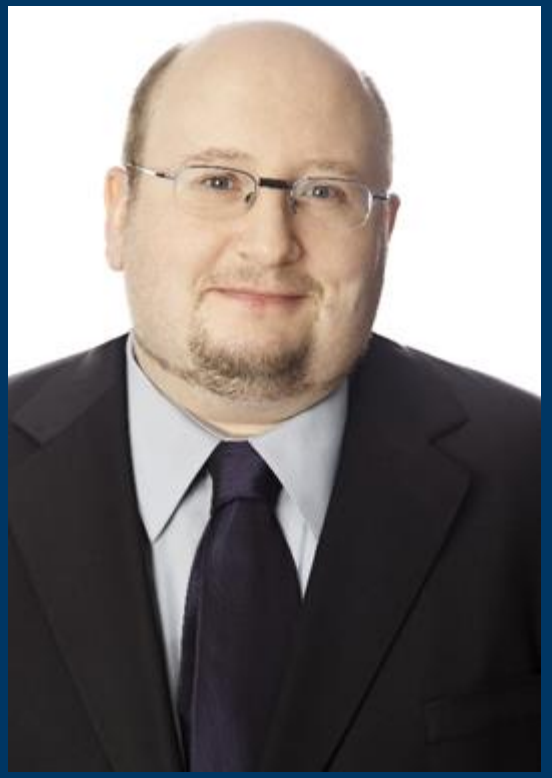
Aryeh Goretsky

Distinguished Researcher

Aryeh is ESET's Distinguished Researcher and has been with the company for ten years.

A twenty-six year veteran of fighting viruses, today he is responsible for threatscape monitoring, investigations and working with researchers in and outside of ESET globally.

He was the first employee at McAfee and is a veteran of several software and networking startups. He has received industry awards from Microsoft, Lenovo and *Securing our eCity* for his efforts to help make computing safer.



#ESETCast

ENJOY SAFER TECHNOLOGY™

Agenda

- Windows 10 Has Arrived
  - Rooting out the best branch for you
  - Windows Updates
- Security Improvements
- Privacy Questions
  - telemetry
- Q&A session

ENJOY SAFER TECHNOLOGY™

Not on the agenda

- I am not a Windows licensing guru
  » Check with Microsoft or your VAR on pricing changes
- This is not a deep dive into Windows 10's security features
- This is not a deep dive into Windows 10's privacy features

  » See articles on our blog We Live Security and ESET's forthcoming white paper on Windows 10 for that

Windows 10 Has Arrived

- The last version of Windows… at least for a while
- Meant as replacement for Windows 7 in the enterprise
- Free for home & SOHO users
  (*i.e.*, license that came with PC, not managed by Active Directory…)
- Might be free upgrade for business users

Upgrading to Windows 10?

- ❑ Windows 10 rolled out to most/all PCs
- ❑ in process of upgrading to Windows 10
- ❑ planning on upgrading to Windows 10
- ❑ no plans to upgrade to Windows 10
- ❑ looking to migrate to Linux, Mac OS X, etc…

Windows 10: Ch-ch-changes

- Introduces Windows users to concept of branches
- OS upgrade model (XP→7, 7→8.1, etc.) replaced with update model (akin to Service pack model)
- Windows 10 will receive updates (bug fixes, security fixes, etc.) and upgrades (new features) over life of OS
- Basically, rolling model to reduce fragmentation, get all PCs on one OS

Editions, Builds & Branches

- Windows 10 has editions
  - Home, Pro, Enterprise, Education, Embedded, etc.
- Windows 10 has builds
  - Build 10240 RTM (release to manufacturing)
  - Build 10586 TH2 (Threshold 2 release)
- Windows 10 has branches
  - WIP (Windows Insider Program), CB (Current Branch), CBB (Current Branch for Businesses), LTSB (Long Term Servicing Branch)

Editions, Builds & Branches

- **Editions**
  - **Nothing really new here**
    (Windows 8.1, 8, 7, Vista all had different editions)
- **Windows 10 has builds**
  - **Nothing really new here, either**
    (think Service Packs)
- **Windows 10 has branches**
  - **Are simply the order in which you get builds**

Windows 10: The Branches

- **Meet the branches**

	Name	Description
WIP	Windows Insider Program	experimental features, large telemetry collection released ~4-6 months after internal testing
CB	Current Branch	release to home/SOHO, basically beta for CBB released ~4 months after WIP
CBB	Current Branch for Business	release to businesses, stable version released ~4 months after CB
LTSB	Long Term Servicing Branch	security updates only, no new features, no telemetry collected intended for low-churn and embedded systems

Windows Insider Program Branch (WIP)

WIP is geared towards power users, hobbyists, experimenters

- For Windows 10 Home and Pro
- Bleeding edge code
- Frequently updated
- Get to see newest features first
- Get to see newest bugs first ☺

Current Branch (CB)

CB is geared towards consumers

- For Windows 10 Home, Pro Editions
  - *e.g.,* home and SOHO users
- Not joined to Active Directory domain
- Offers little to no management of updates and upgrades
  - Pro versions can temporarily defer updates
  - Limited ability to block driver updates (new)

Current Branch for Businesses (CBB)

CBB is geared towards businesses

- For Windows 10 Pro, Enterprise, Edu Editions
- joined to Active Directory domain
- Management of updates and upgrades
  - Windows Update for Business (set of GPOs)
  - System Center, WSUS, Intune, etc.

Long Term Servicing Branch (LTSB)

LTSB is geared towards enterprises with specific need for change control

- Requires enterprise licensing
- Security updates only
  - No new features, support for new HW, etc.
- No Cortana, Edge; limited Modern Apps
- No telemetry collection
- Designed for kiosks, PoS, other low-interactivity systems *(1 app, 0-1 users…)*

Which branch is best?

- **Home user or SOHO?**
  - **CB and CBB *(subject to licensing)***
- **Medium and large business**
  - **CB *(betas, pilot programs & test groups)***
  - **CBB *(75-85% of users are going to be here)***
  - **LTSB *(kiosk, POS, embedded systems)***

Windows 10: Updates

In Windows 10, updates are downloaded from catalog.update.microsoft.com, which is a *little* different than Microsoft Windows Update

- **unmanaged PCs (home PCs, not on a domain)**
  - **Home: receive all, no ability to defer**
  - **Pro: receive all, limited ability to defer**
  - **ability to roll-back bad drivers**
- **Updates for AD-joined PCs**
  - **Managed by WSUS**
  - **Windows Update for Business**
  - **Can defer updates and upgrades**

Windows 10: Updates

Ultimate goal?

Get everyone on same build of Windows 10.

Problem with branches, early code access:

- Consumers may get early updates containing code that isn't well-tested
- Enterprises may be vulnerable to exploits already patched for consumers

Windows 10: Security Improvements

- **Virtualization-Based Security**
  (formerly Virtual Secure Mode)
- **User Authentication Improvements**
  (Windows Hello, Passport, Credential Guard)
- **Edge Web Browser**
- **Windows Defender**

Virtualization-Based Security

- Moves OS kernel, LSASS (security subsystem) into hypervisor (Hyper-V)
- Implements Hypervisor Code Integrity (HVCI)
- These parts of OS no longer subject to certain classes of attack
- Specific HW requirements:
  - x64, UEFI, IOMMU, TPM 1.2/2.0, VT-x/VT-d extensions

User Authentication

Enterprise-grade logins for all?

- Windows Hello can use biometrics (facial, iris, fingerprint), PIN, and traditional password
- Microsoft Passport – new login system based on FIDO Alliance specs
- Credential Guard (requires VBS)
  - Mitigates PtH / PtT attacks
- Long term goal: replace enterprise PKI

Microsoft Edge Web Browser

New web browser built from scratch for Windows 10

- No ActiveX, BHOs, VBScript or other binary extensions
- Adobe Flash and PDF rendering “built in”
- Less code = smaller attack surface
- Designed to “fail fast” as an attack mitigation
  - Crash and restart instead of trying to continue running buggy/potentially malicious code

Windows Defender Updated

- Context-sensitive scanning based on origin
  - Files from Internet aggressively scanned
- Detection of memory-only malware
- Windows Defender Cloud Protection
  - Data from endpoints, MSRT, etc.
- Uses the same engine and signatures as System Center Endpoint Protection (SCEP)
- Always installed
  - Activates when 3rd-party AV expires
  - Can be snoozed but not disabled

Windows 10 and your Privacy

Windows 10 gathers more data on program and user behavior than previous Windows versions. Data collected includes:

- **Spelling (spellchecker)**
- **URLs (SmartScreen, Windows Defender…)**
- **handwriting**
- **voice recognition**

Windows 10 and your Privacy

Windows 10's data collection is

- **Comparable to Android and iOS**
- **Used to power services like system spellchecker, Windows Defender, Cortana, Bing, etc., not third parties**
- **Cannot be disabled completely (except LTSB)**

Windows 10 and your Privacy

Windows 10's "Asimov" telemetry is based on WER. Collects information about:

- Crashes (OS, third-party device drivers…)
- Device ID and type (anonymized)
- Microsoft OS and app performance
- Hung applications
- Security settings state

In short, no Personally Identifiable Information (PII) is collected and data is used to fix/improve systems running Windows.

Windows 10 and your Privacy

Final thoughts:

If you are an IT professional or a “power user” and you turn off telemetry collection, Microsoft will end up collecting data from home and non-technical users.

And develop future software, accordingly.

Did everyone enjoy Windows 8?

Recommendations - Consumer

Yes, you should upgrade if:

- **Your hardware supports it**
- **Your software supports it**

Remember, upgrade is only free until July 29, 2016. After that, $100-200US (depending upon version and region)

Recommendations - Consumer

Before you upgrade

- **Make at least one backup of all valuable data**
  - **Test it, preferably by restoring somewhere else**
- **Update all the things**
  - **Install all OS updates and patches**
  - **Install all device driver updates**
  - **Update applications, utilities**

- **Pro-Tip: See *Backup Basics* article**

Recommendations - Business

Now is the time to begin testing Windows 10 for your business

- **Verify application compatibility**
- **Identify any hardware or software that may need to be replaced (Windows XP?)**
- **Training (IT staff and users)**
- **Any software contracts that need to be renegotiated?**
  - **Make sure Windows 10 editions, branches and builds you need are supported**
  - **Covers support for future versions of Windows**

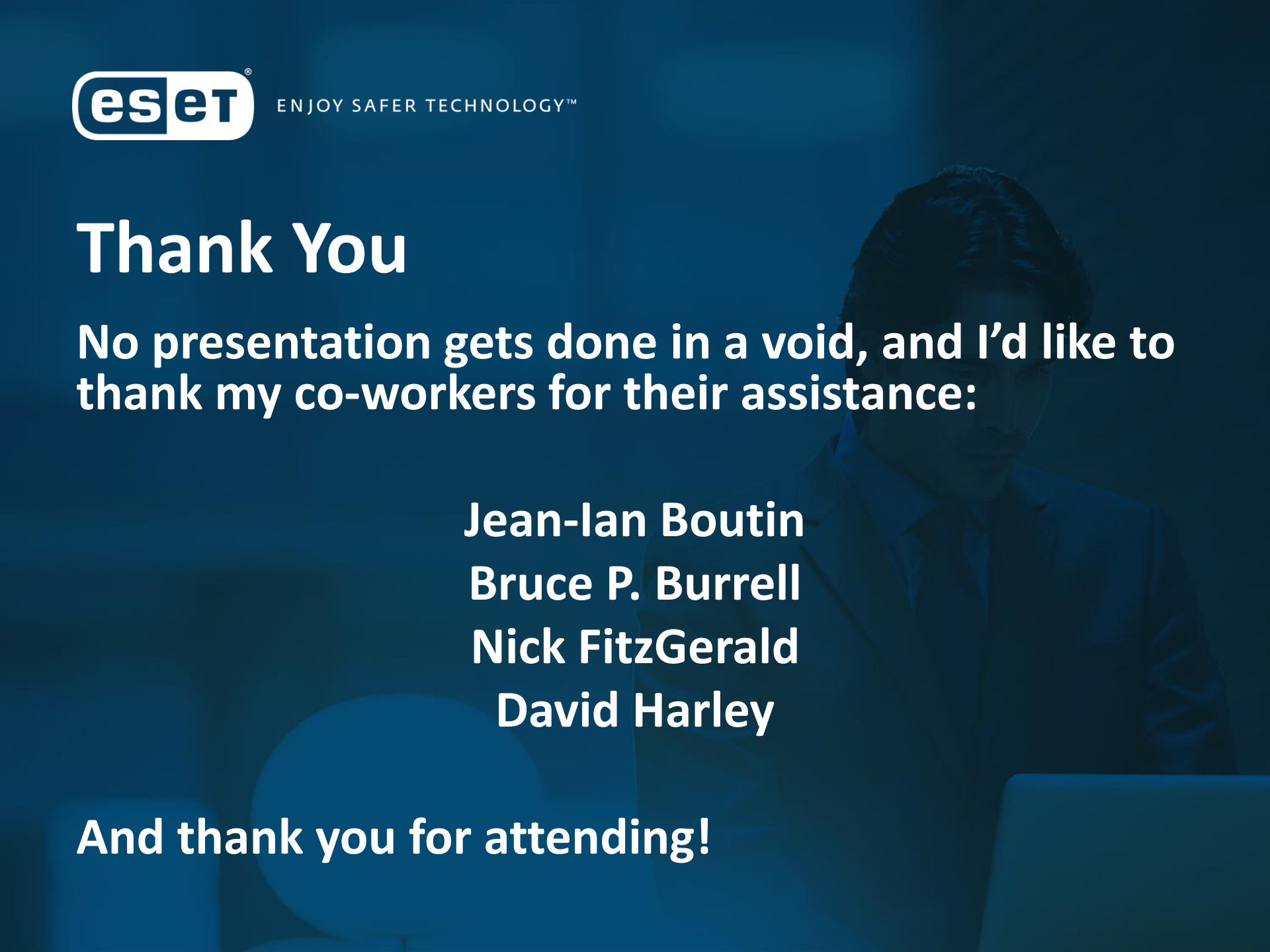
I would like to request one of the following

- ❑ Contact from ESET Sales
- ❑ Technical Demo
- ❑ Business trial
- ❑ Information on becoming a Reseller Partner or MSP
- ❑ None of the Above

Q+A Discussion

Bibliography

- Microsoft Help, *Defer Upgrades in Windows 10*
- Microsoft Knowledgebase, *How to temporarily prevent a Windows or driver update from reinstalling in Windows 10*
- Microsoft Help, *Windows Hello and Privacy FAQ*
- Consumers Digest, *Windows Hello: An eye opener*
- FIDO Alliance, *About the FIDO Alliance*
- Microsoft TechNet, *Credential Guard*
- Microsoft TechNet, *Device Guard Overview*
- We Live Security, *Backup Basics*
- We Live Security, *Windows 10, Privacy 0*
- We Live Security, *Will Windows 10 Leave Enterprises Vulnerable to Zero Days?*



Thank You

No presentation gets done in a void, and I'd like to thank my co-workers for their assistance:

Jean-Ian Boutin

Bruce P. Burrell

Nick FitzGerald

David Harley

And thank you for attending!

ENJOY SAFER TECHNOLOGY™

Aryeh Goretsky

WWW.ESET.COM
WWW.WELIVESECURITY.COM

aryeh.goretsky@eset.com

@goretsky *(personal)* / @esetna / @welivesecurity

/u/goretsky *(personal)* / r/eset & r/welivesecurity *(unofficial)*

fb.com/goretsky *(personal)* / fb.com/esetglobal

Discography

An incomplete listing of albums listened to during the creation of this presentation:

- Fatboy Slim - *Halfway Between the Gutter and the Stars*
- The Hooters - *Both Sides Live*
- Information Society - *Hack*
- Israel Kamakawiwo'ole - *Alone in Iz World*
- Jan Hammer - *Drive*
- Klaus Doldinger - *Das Boot (original soundtrack)*
- London Philharmonic - *Greatest Video Game Music, Vol.1*
- Snap! - *The Madman's Return*
- Steely Dan - *Aja*
- Tommy Emmanuel - *The Journey*
- Yes - *90125*