



 **DigitalAlliances**
continue collaboration

CISO Alliances UK&I
March 4th 2021

In Partnership with



Food For Thought/Topics Discussed

CISO Alliances
Digital Alliances
continue collaboration

"Complete Endpoint Security: Five Critical Steps"

UK&I

Thursday 4th March 3pm (GMT/BST)
www.alliances.global
james@alliances.global

BeyondTrust

Session Leader:
Morey Haber – CTO & CISO BeyondTrust

Moderator:
Mike Jones – H4unt3d Hacker Podcast

Session Leader:



Morey Haber
CTO & CISO BeyondTrust



Session Synopsis :

5 critical steps to complete endpoint Security

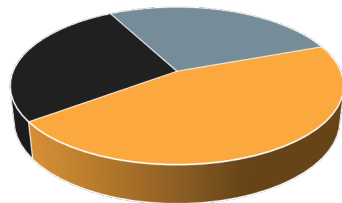


70% of successful breaches started at the endpoint in 2019. Since then, a global pandemic has caused a large-scale shift to remote work – a perfect storm for privilege abuse. As a result, malware has increased by 30,000% in 2020. This is especially concerning when many companies still rely on antivirus software (AV) or Endpoint Detection and Response solutions (EDR) alone to secure endpoints. In this visionary session, we will be highlighting which two overlooked steps can mitigate the 60% of modern threats that are missed by AV, and why the need for organizations to move from a reactive to a preventative approach is more important than ever.

Food For Thought/Topics Discussed

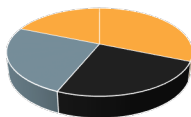
Community Pre Alliances intelligence :

What has been your
number 1 security
project in 2020?



- Secure Remote access
- MFA
- Privileged account & session management

What is your
privilege
management
covered by?



- GPO
- PAM
- EPM
- Temp admin access


Does the solution
mentioned cover your
Unix & Linux
environment?

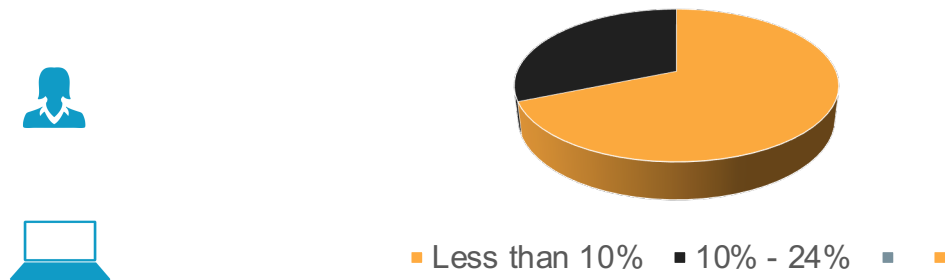



- Yes
- No
-
-

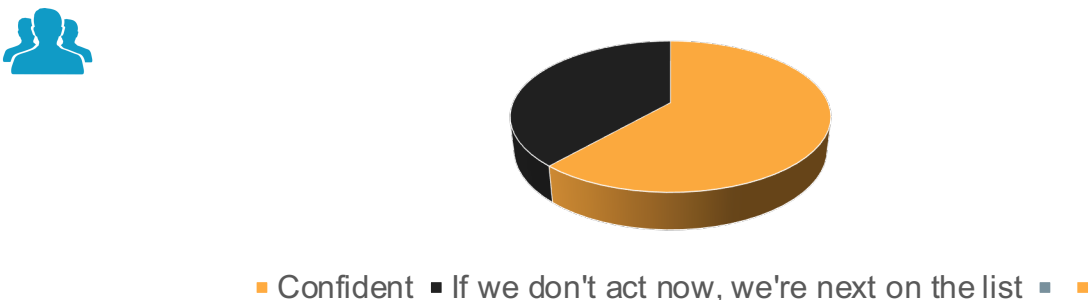
Food For Thought/Topics Discussed

Community Pre Alliances intelligence :

 How many users in your company still have local admin rights?



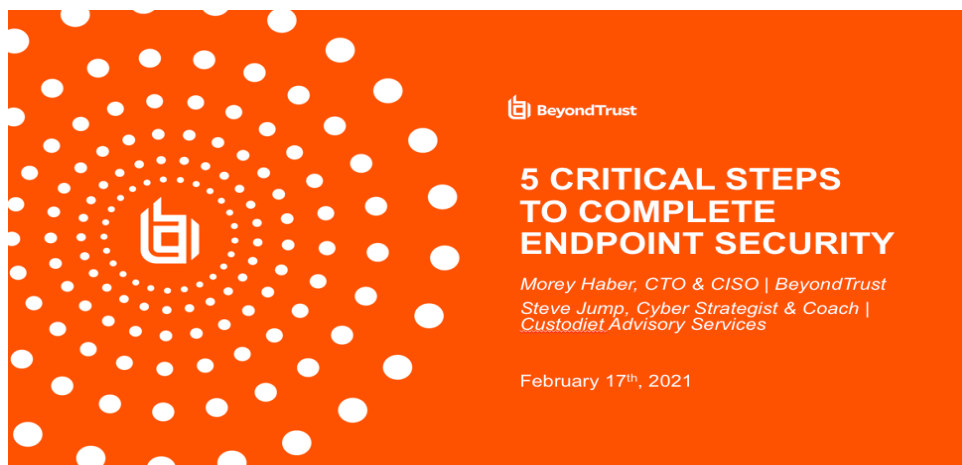

How confident are you, that your organization won't be a victim of ransomware in 2021?



 Digital Alliances

continue collaboration

Session Slides



Morey J. Haber
CTO & CISO, BeyondTrust

- 20+ years security experience
- Articles on Forbes, SecureWorld, CSO Online, etc.
- Author of 3 Cybersecurity Attack Vector books (all available from Apress Media)
 - Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations (2 Editions)
 - Identity Attack Vectors: How to Build an Effective Identity Governance Program
 - Asset Attack Vectors: How to Implement a Successful Vulnerability Management Strategy



 **DigitalAlliances**

continue collaboration

Session Slides

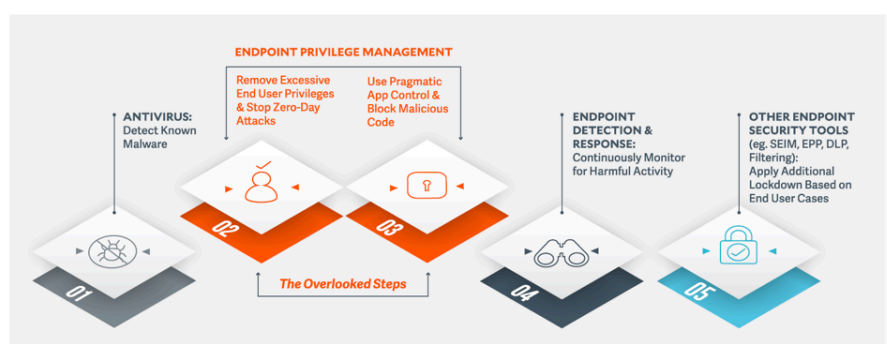


5 CRITICAL STEPS FOR COMPLETE ENDPOINT SECURITY

Shifting from a Reactive to a Preventative Approach

5 Critical Steps of Complete Endpoint Security


a preventive approach to endpoint security



DigitalAlliances

continue collaboration

Session Slides



ANTIVIRUS
Detect Known Malware



**ENDPOINT
PRIVILEGE
MANAGEMENT**
Remove Excessive End User Privileges
& Stop Zero Day Attacks

Overlooked Step!



**ENDPOINT
PRIVILEGE
MANAGEMENT**
Use Pragmatic Application Control &
Block Malicious Code

Overlooked Step!

 **DigitalAlliances**

continue collaboration

Session Slides



04

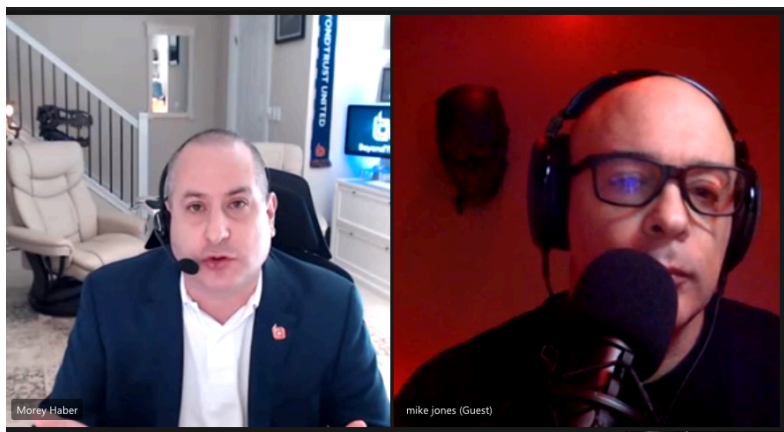
**ENDPOINT
DETECTION &
RESPONSE**

Continuously Monitor for Harmful Activity

05

**OTHER
ENDPOINT
SECURITY TOOLS**

Apply End User Lockdown Based on End User Cases



 **DigitalAlliances**

continue collaboration

Endpoint Security and You.



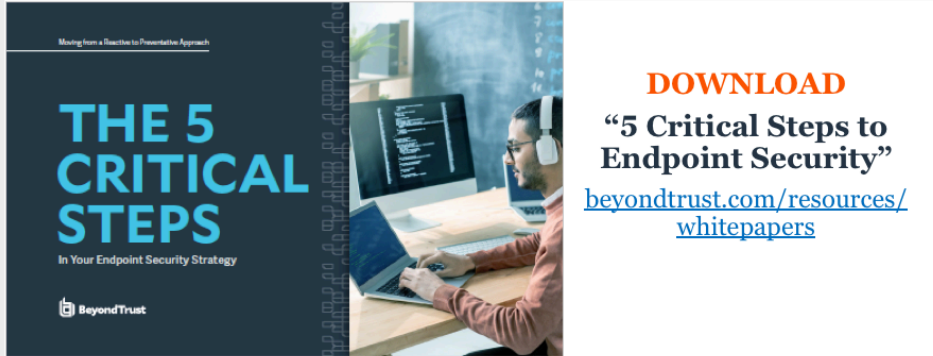
- 70% of attacks start at endpoint.
- Phishing, Social engineering and Zero dates are top of the list for attacks.
- Organisations are starting to remove admin rights from users, 77% of users in 2019 had admin rights compared to 56% of users in 2020.
- Biggest challenge to BeyondTrust is company growth.
- Biggest threat to endpoint security is attacks against office 365 and emails. Attacking emails to either forward on to third parties or getting into sent boxes and resending emails with edited links.
- Adding AI to an existing network that is bad, won't fix anything. If the network is bad then AI will assume that it is normal as it's been there since it has.
- Working from home has opened up even more challenges and the competition with operating systems has added to this.
- 3rd party applications at home as causing issues on unsecured networks.



Questions from the Community

- What happens when we go back to office life and everything has now been setup for working at home?
- Will we have the same growing pains going back to office life as we did when working from home started?
- What is everyone's view on working from home and VPN's?
- Will the SolarWinds attack be just the start of similar attacks?

Next Steps....



Supportive Links



<https://www.beyondtrust.com/resources/videos/protect-remote-endpoints-from-attacks-malware>



<https://www.beyondtrust.com/blog/entry/how-trusted-application-protection-builds-on-application-control-endpoint-privilege-management>

<https://www.beyondtrust.com/blog/entry/least-privilege-the-most-effective-approach-to-endpoint-security>



<https://www.beyondtrust.com/resources/videos/endpoint-privilege-management>