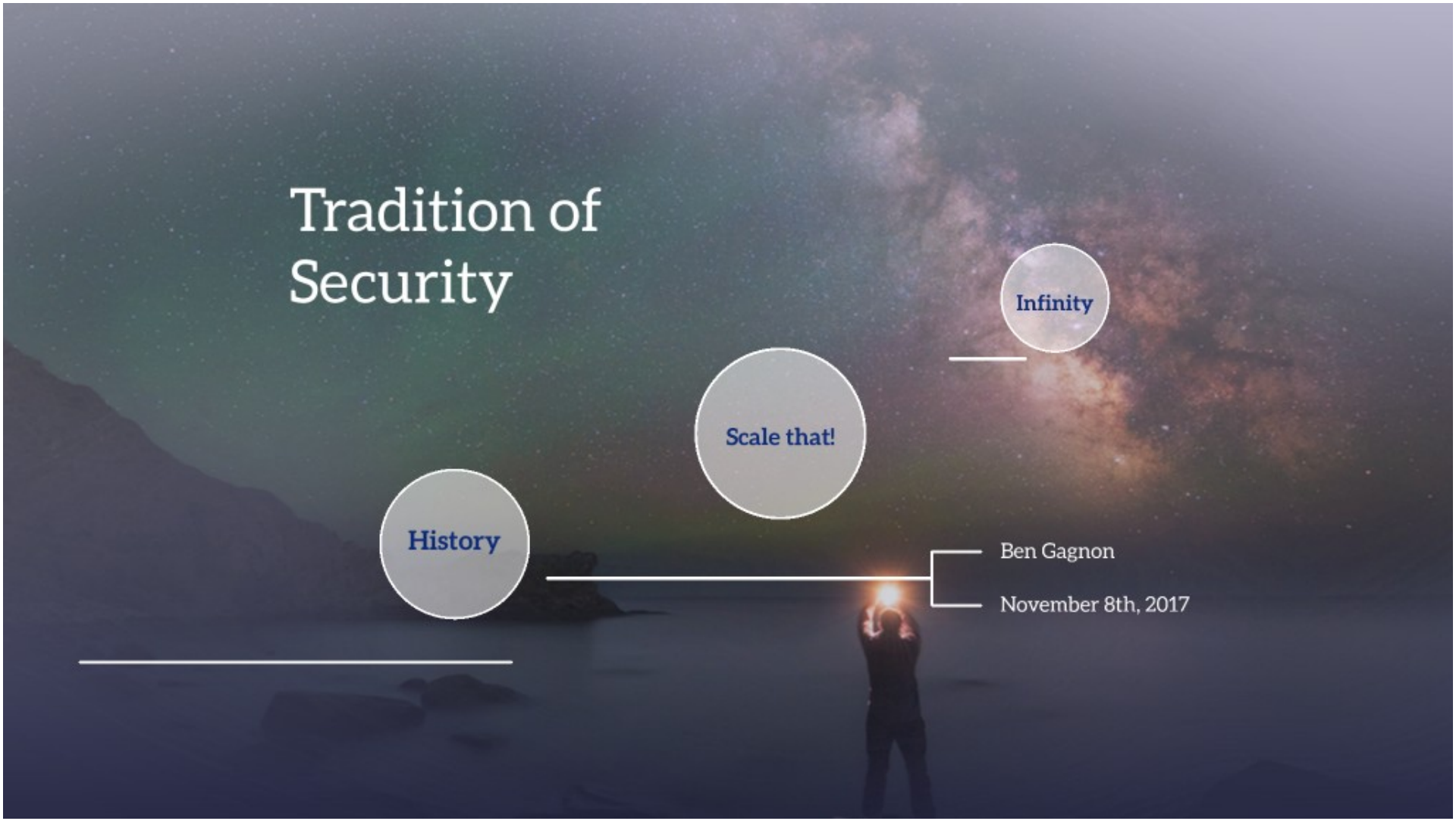
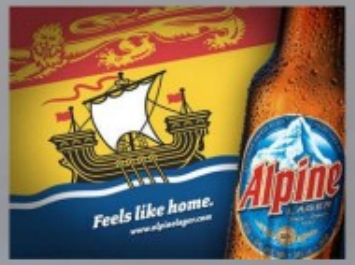

Tradition of Security
Infinity
Scale that!
History
Ben Gagnon
November 8th, 2017

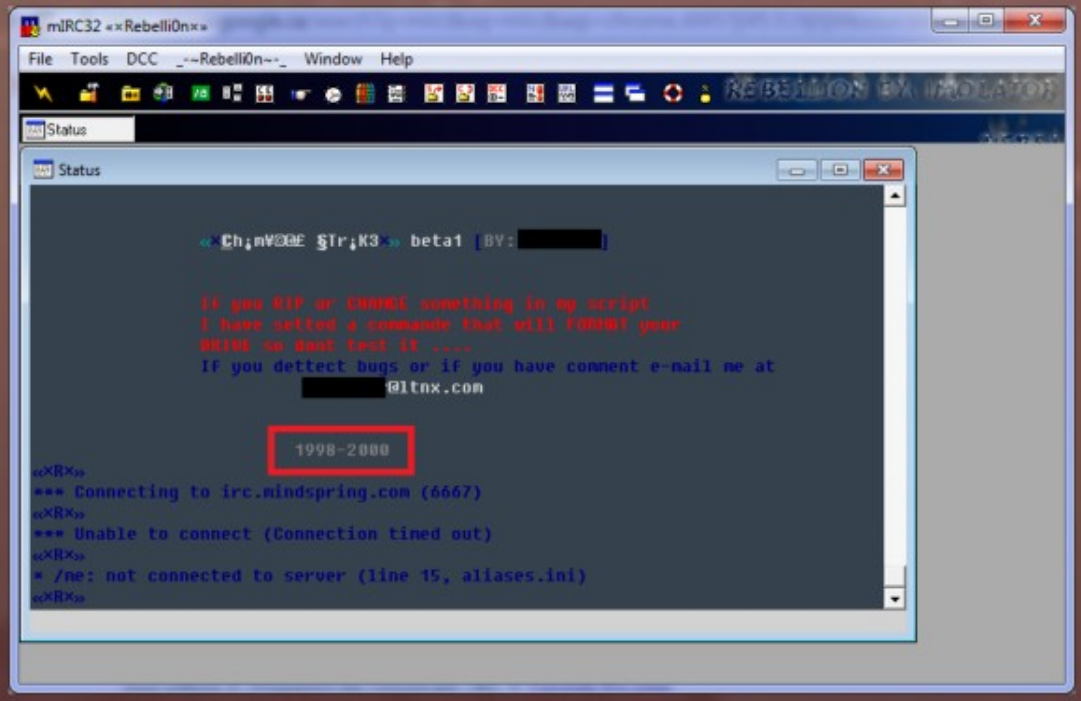
My history



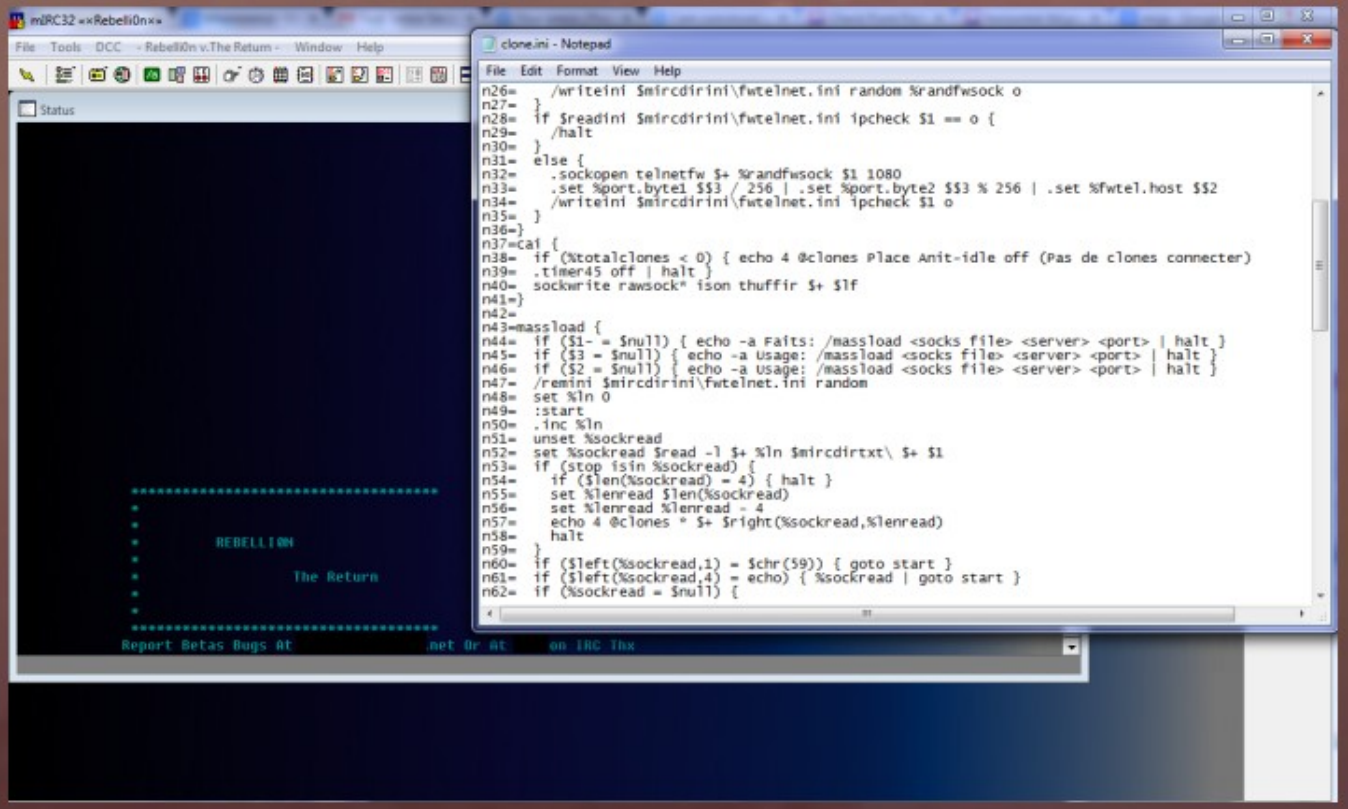
Before everything

Back to the future!

mIRC, 1998

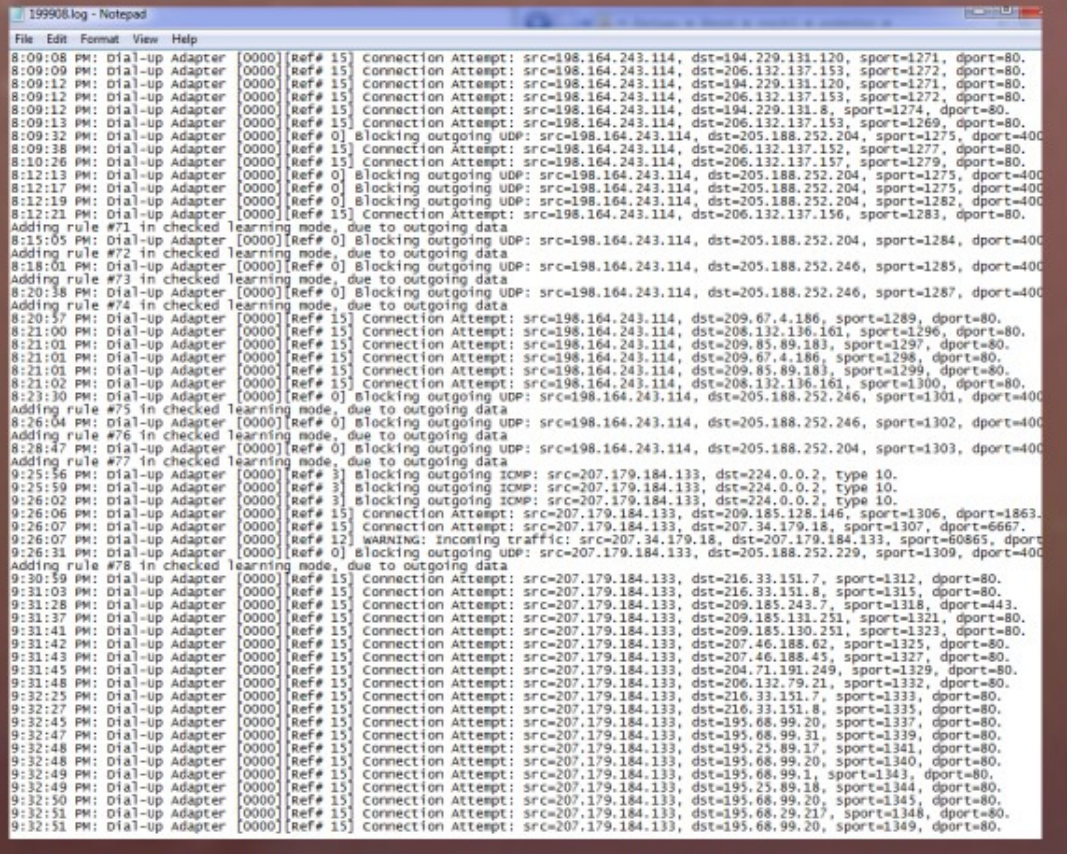

mIRC32 «×Rebelli0n×»
File Tools DCC _·~Rebelli0n~·_ Window Help
Status
Status
«×Ch¡mV@@E §Tr¡K3×» beta1 [BY: [redacted]]
If you RIP or CHANGE something in my script
I have setted a commande that will FORMAT your
DRIVE So dont test it ....
If you dettect bugs or if you have comment e-mail me at
[redacted]@ltnx.com
1998-2000
«×R×»
*** Connecting to irc.mindspring.com (6667)
«×R×»
*** Unable to connect (Connection tined out)
«×R×»
* /me: not connected to server (line 15, aliases.ini)
«×R×»

A year later, All out war.



Due care, due dilligence!

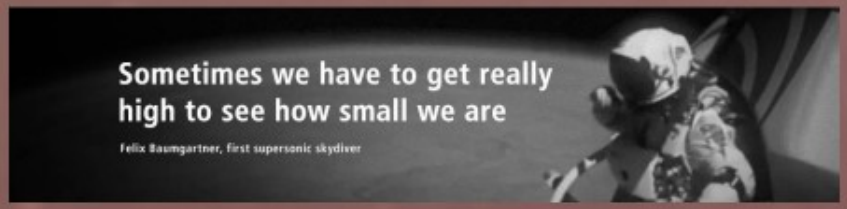
- Firewall
- IDS
- VPNs
- Proxy
- And more!



And then.


Windows
An error has occurred. To continue:
Press Enter to return to Windows, or
Press CTRL+ALT+DEL to restart your computer. If you do this,
you will lose any unsaved information in all open applications.
Error: 0E : 016F : BFF9B3D4
Press any key to continue _

In hindsight.



Knowledge

Control

Challenge

Power

Why?
o_0

Access

Control

Notoriety

Money

Lessons learned

Lack of time

Lack of expertise and resources

Illusion of security

Lack of focus

Lack of time

Lack of expertise and resources

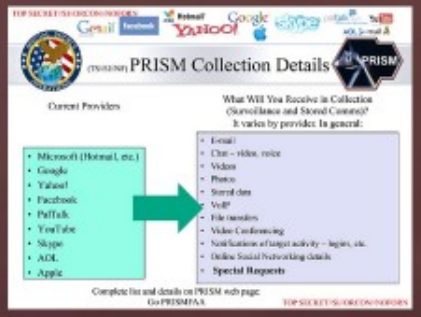
Security Expert with experience required!

I installed this once!

metasploit®

Illusion of security

Deloitte.



verizon

Lack of focus

Optimization is good until it's too much.

STRATEGIC PLANNING ASSUMPTION

More than 95% of firewall breaches are caused by firewall misconfigurations, not firewall flaws.

Today's challenges

Lack of time:

Long implementations
Change windows
Procedures

Lack of expertise and resources:

Hiring
Efficiency
Projects
Do it all.

Illusion of security:

New technologies
IOT
Shadow IT
New everything
Cloud
Mobility

Lack of focus:

C-Levels!

Where do we focus what we have to get the most benefit

Rather than.

Staying proactive and planning months or years in advance.

We know...

Verizon investigation report states:

YoY threats went up 40%

IDC Spending:

YoY growth of 9%

Yet, efficiency of IT Security went down!

The problem is getting worse

50% of reported breaches could not estimate # of records
16% of all breaches reported were of financial access
4% of breaches were encrypted data
40% increase over previous 6 months

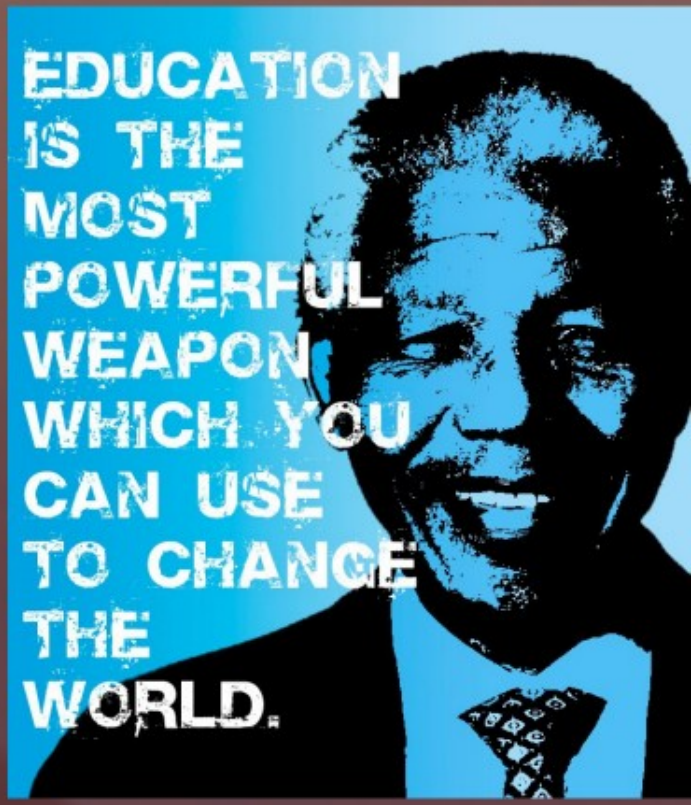
Breach statistics in financials NA 2016 (Gemalto)

3.04 million records per day
126 936 records per hour
2116 records per minute!

Education is key!

75% of execs think they are invicible
4 out of 5 are confident in their systems
17% would invest in cybersecurity training
28% would invest in mitigating financial losses

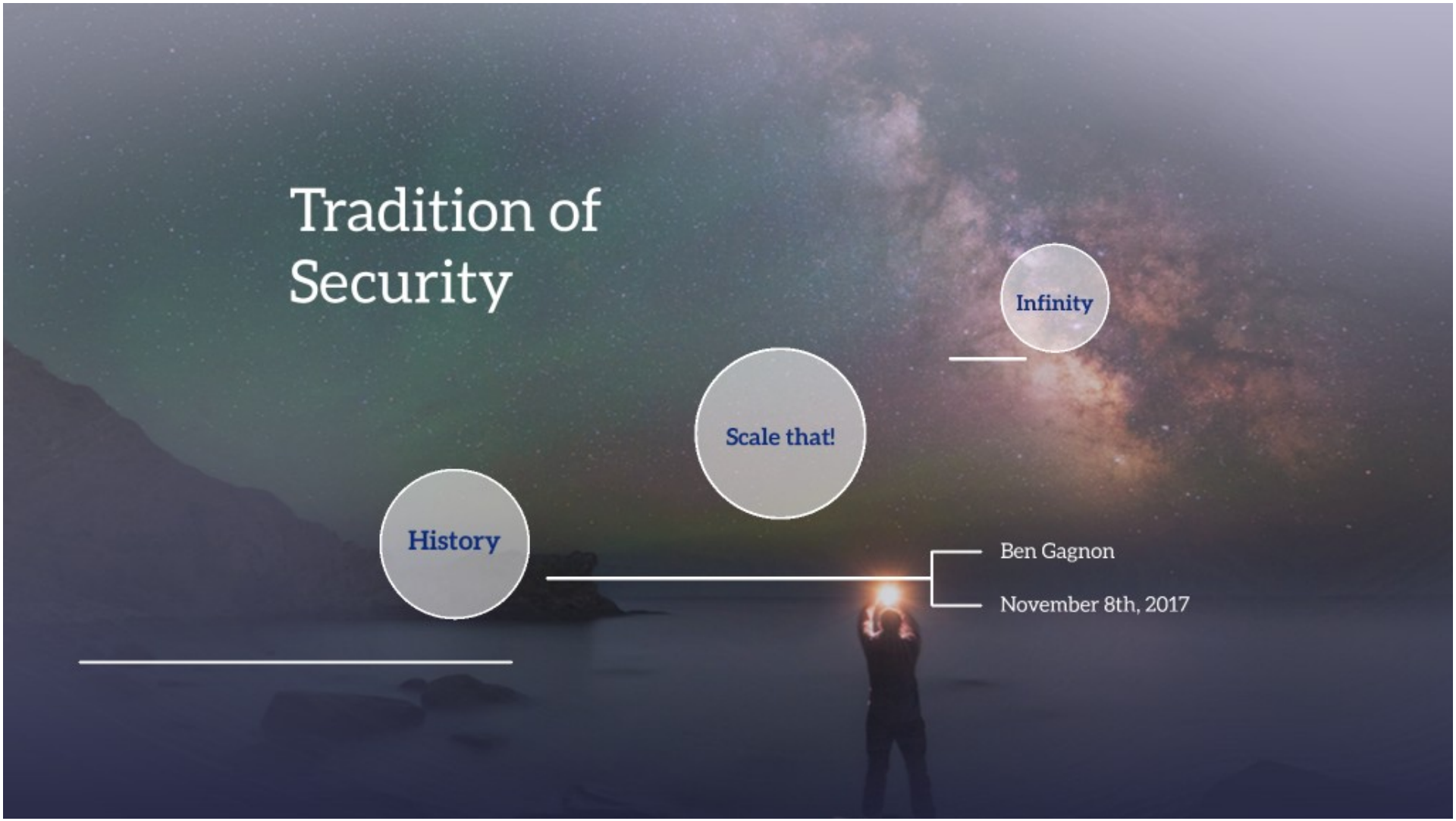
(Data from Accenture)



What happend?

Where did the 9% go?

Policy enforcement
Care and feeding
Continuity of evidence challenge
Best of breeds!


Tradition of Security
Infinity
Scale that!
History
Ben Gagnon
November 8th, 2017

Scale

Most traditional ways of doing security don't scale:

Logs
Detection (IDS,HIPS)
Policies
etc.

Solutions requiring human intervention inherently cannot scale!

Adoption

Consolidation

Cloud Adoption

Public and Private cloud services - IaaS, SaaS, PaaS

Application elements may reside in widely diverse infrastructure elements

Applications are no longer contained within a data center's four walls

What's stopping you?

Physical costs

More maintenance

More rack space and power

Increased application delivery times

Application and Service delivery

Increased complexity

Changes are prone to conflict

Game changer!

Detection only failures

Creates termendous human overhead

Slows the delivery of services due to disconnected nature

Technologies are not portable and do not integrate well in a SaaS, IaaS environments

A leaking example!

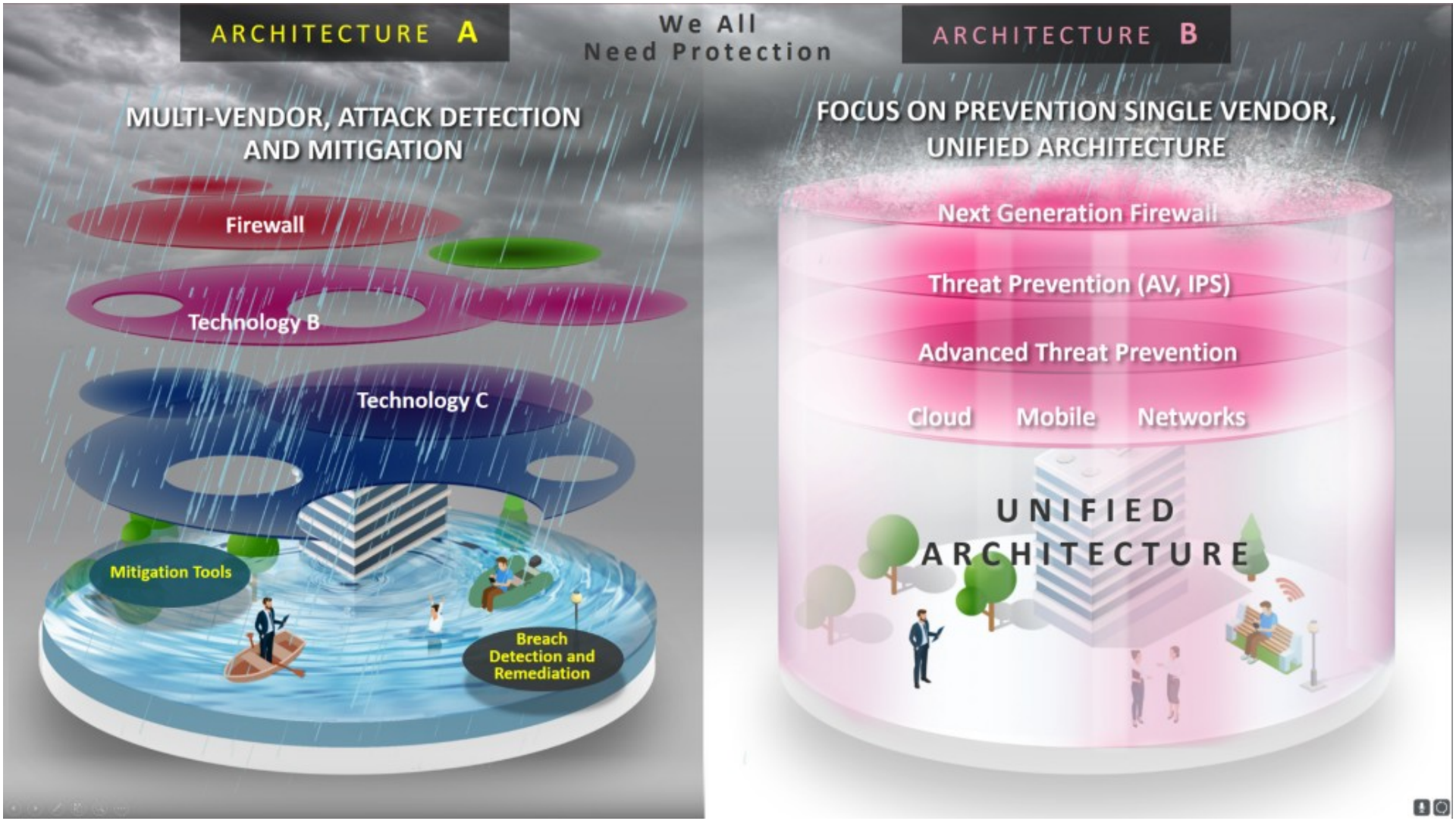
Kevin the roof is leaking!

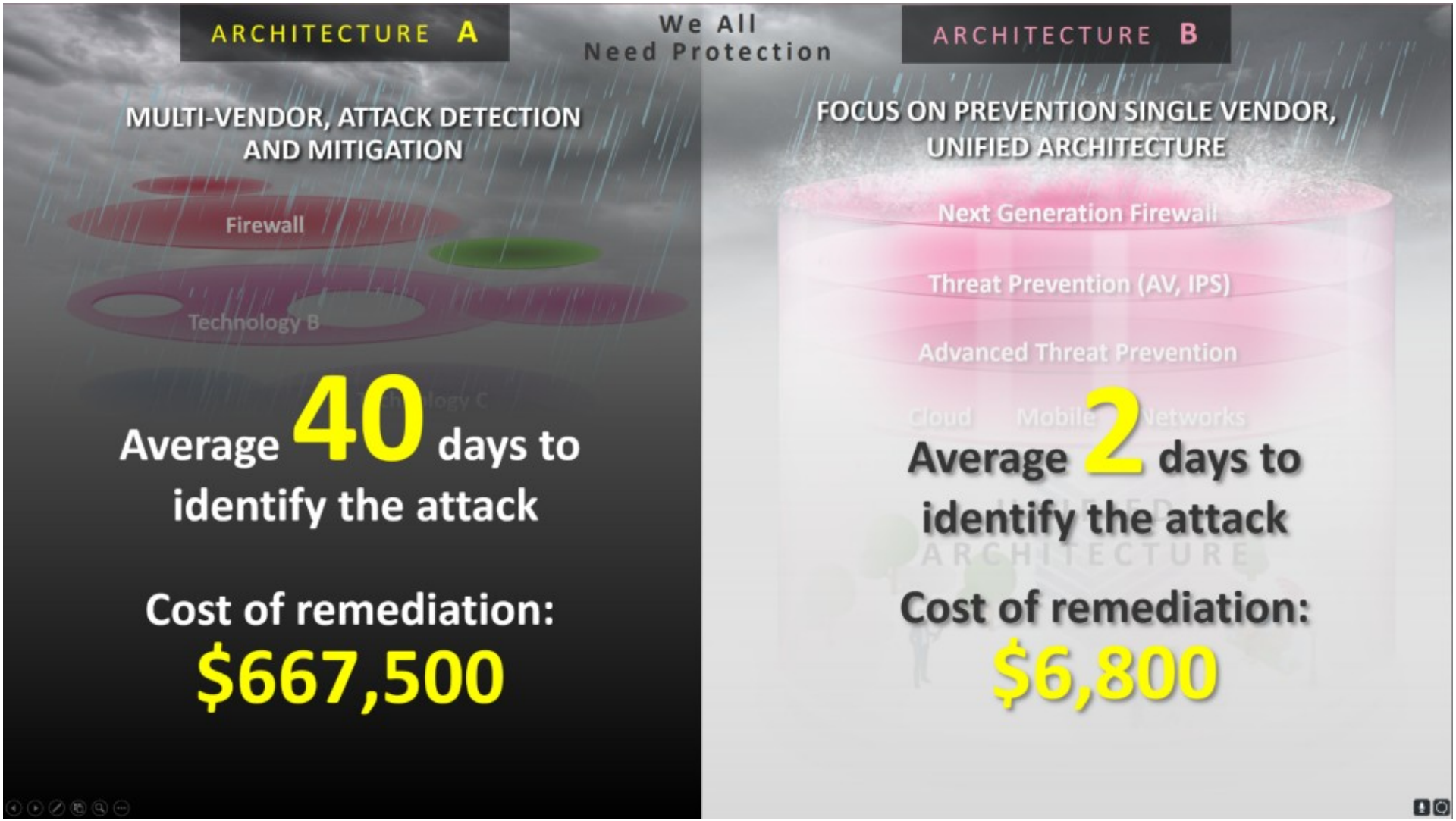
Focus on remediation?

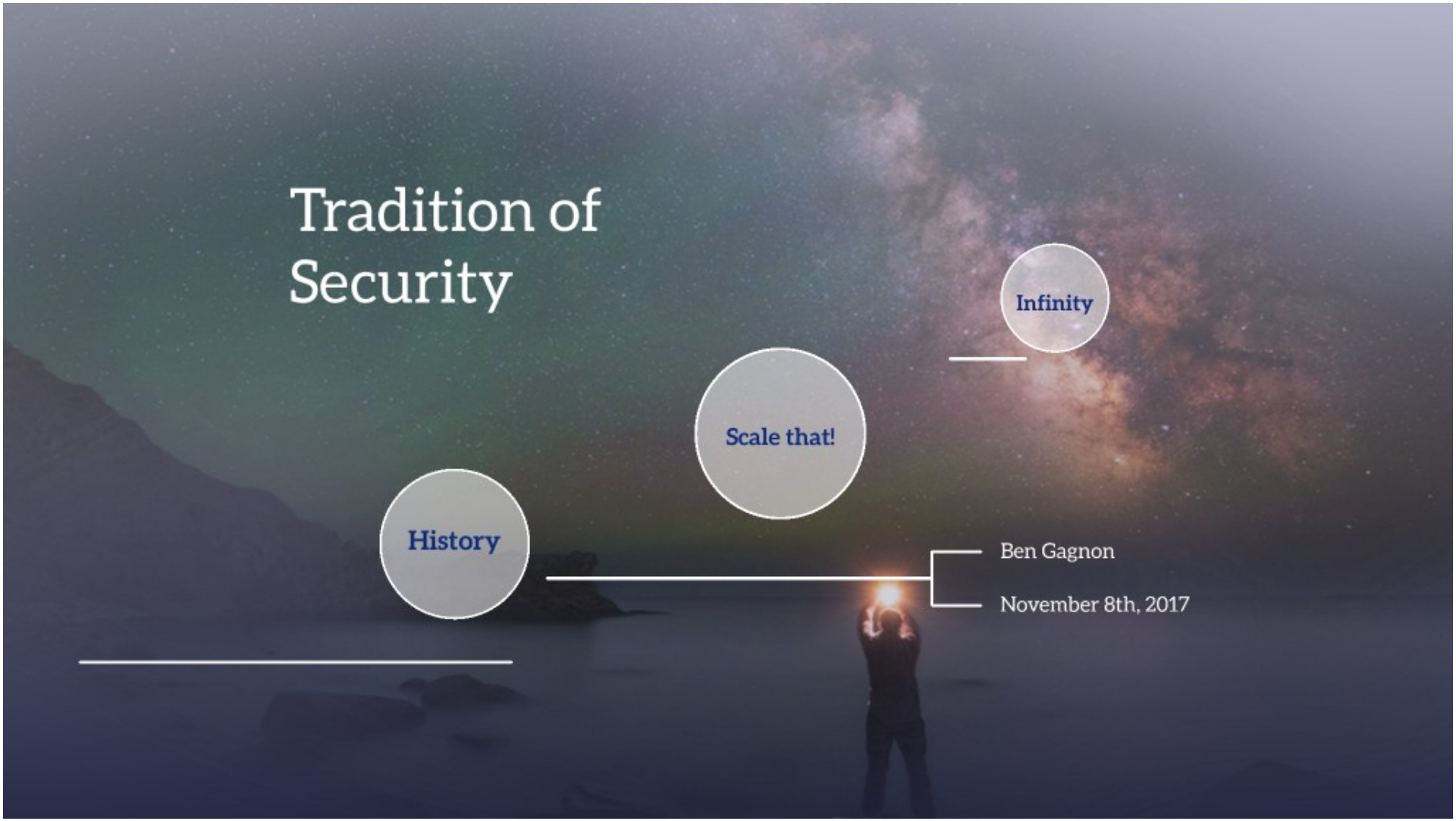
Patch with point solutions?

Focus on incident response?

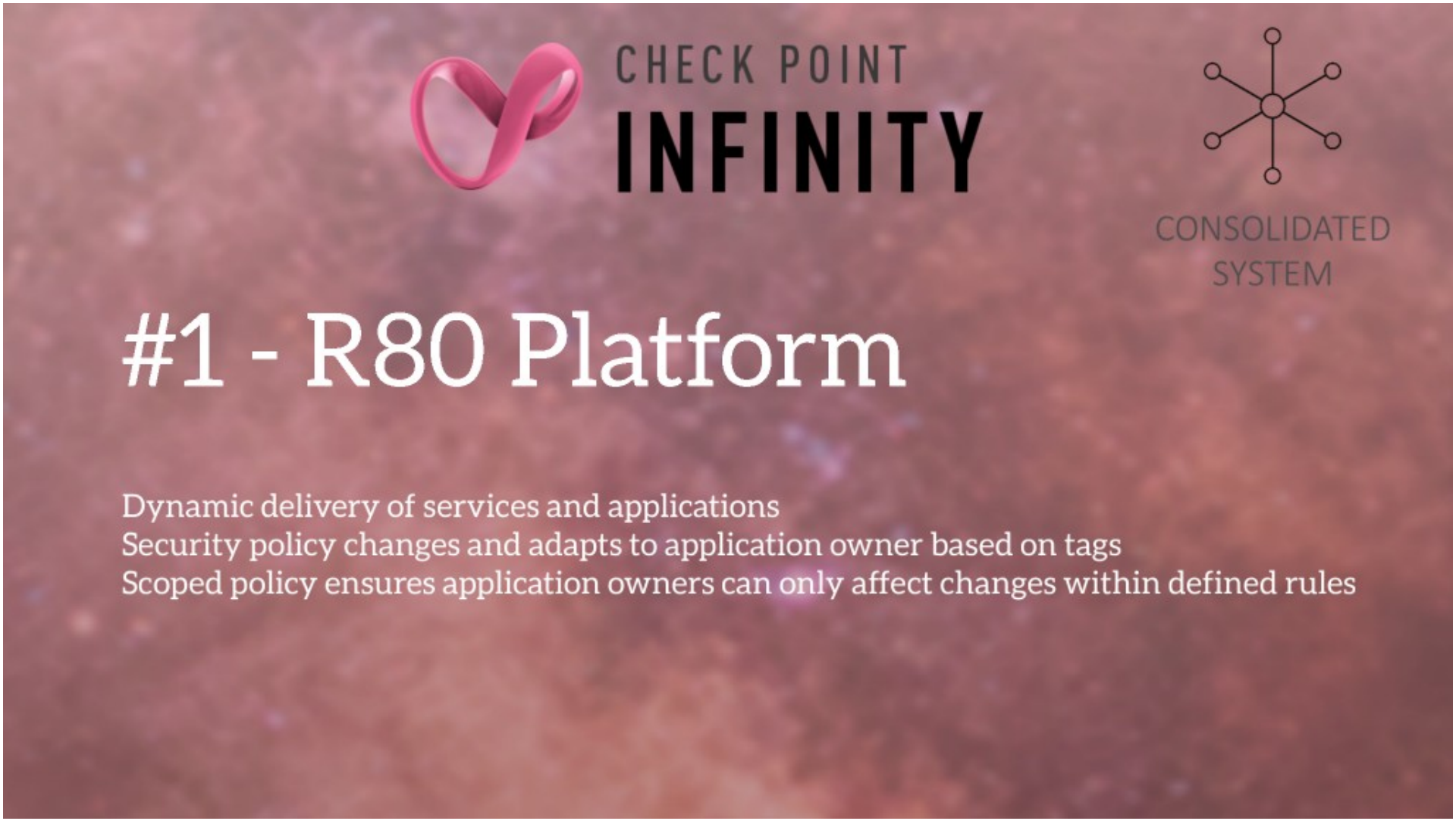
Pretend it isn't happening?


ARCHITECTURE A
We All
Need Protection
ARCHITECTURE B
MULTI-VENDOR, ATTACK DETECTION
AND MITIGATION
Firewall
Technology B
Technology C
Mitigation Tools
Breach
Detection and
Remediation
FOCUS ON PREVENTION SINGLE VENDOR,
UNIFIED ARCHITECTURE
Next Generation Firewall
Threat Prevention (AV, IPS)
Advanced Threat Prevention
Cloud
Mobile
Networks
UNIFIED
ARCHITECTURE

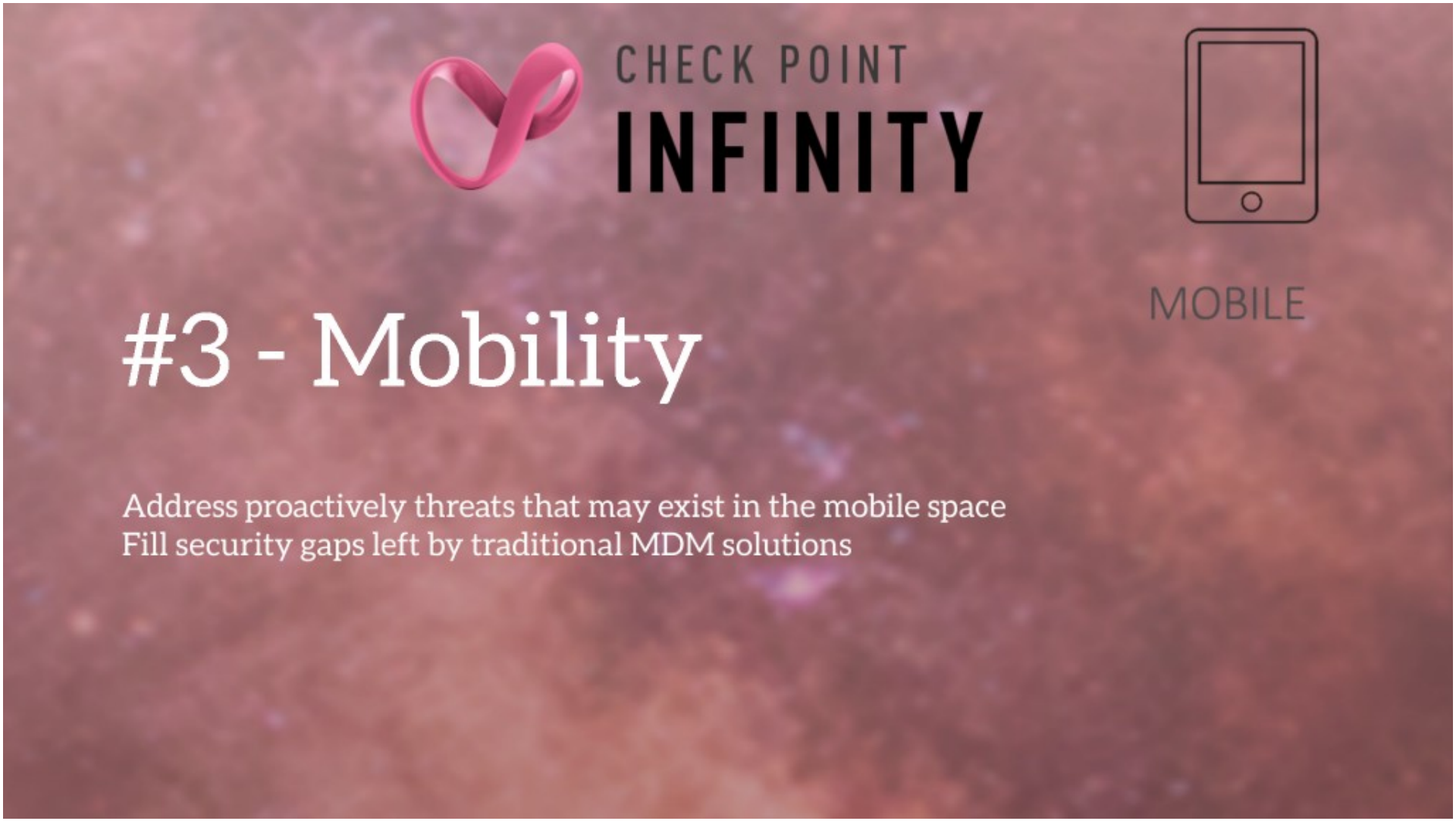

ARCHITECTURE A
We All
Need Protection
ARCHITECTURE B
MULTI-VENDOR, ATTACK DETECTION AND MITIGATION
Firewall
Technology B
Average 40 days to identify the attack
Cost of remediation:
$667,500
FOCUS ON PREVENTION SINGLE VENDOR, UNIFIED ARCHITECTURE
Next Generation Firewall
Threat Prevention (AV, IPS)
Advanced Threat Prevention
Cloud
Mobile
Networks
Average 2 days to identify the attack
Cost of remediation:
$6,800


Tradition of Security
Infinity
Scale that!
History
Ben Gagnon
November 8th, 2017


STRATEGY
#1
#2
#3
#4
TIMELINE
R80 Platform
Sandblast & Threat Extraction
Mobility
vSEC
CHECK POINT
INFINITY
Infinity
Thanks!

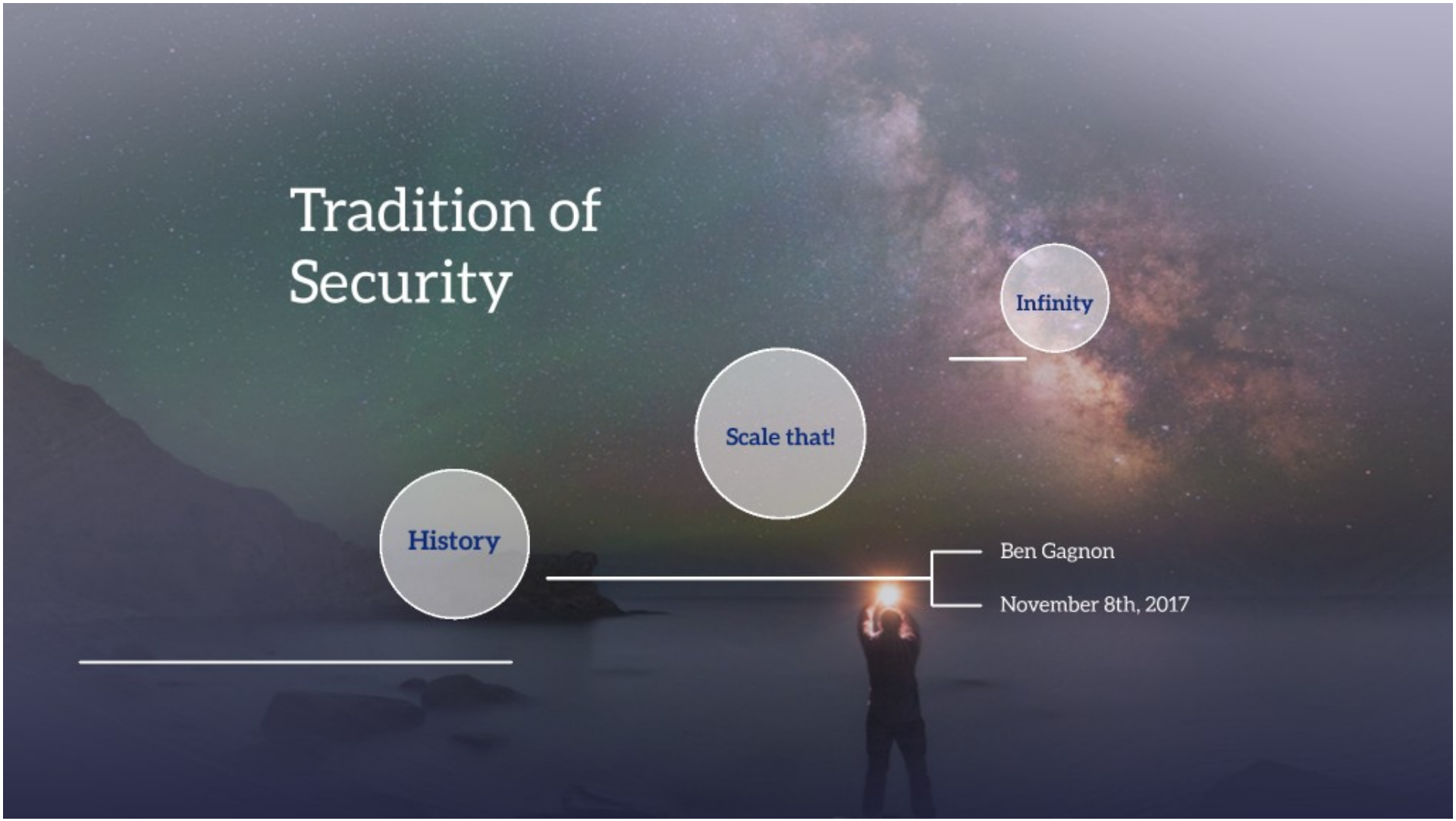

CHECK POINT
INFINITY
CONSOLIDATED
SYSTEM
#1 - R80 Platform
Dynamic delivery of services and applications
Security policy changes and adapts to application owner based on tags
Scoped policy ensures application owners can only affect changes within defined rules


CHECK POINT
INFINITY
THREAT
PREVENTION
#2 - Sandblast &
Threat Extraction
Pass known good
Proactively sanitize threats using unique approach
Provide unified policy management across entire architecture


CHECK POINT
INFINITY
MOBILE
#3 - Mobility
Address proactively threats that may exist in the mobile space
Fill security gaps left by traditional MDM solutions


CHECK POINT
INFINITY
CLOUD
#4 - vSEC
Private cloud security
Public cloud security
Dynamic and adaptive security across platforms and architectures
amazon web services™
vmware NSX
nuagenetworks
From Nokia
openstack
Microsoft Azure
CISCO
Google Cloud Platform


Benoit Gagnon, MBA, CISSP, CISA
bgagnon@checkpoint.com


Tradition of Security
Infinity
Scale that!
History
Ben Gagnon
November 8th, 2017