



How to Answer the Hard Questions about your IT Infrastructure

IT-SA Conference - October 2019 - Nürnberg

Simon Mullis, Director of Security Strategy – EMEA, Tanium
[@smullis](#)

Today, every company is a
technology company.



Petya cyberattack cost [redacted] \$135 million in revenue

Third-quarter revenue for the global pharma giant was drastically reduced in part by the temporary production shutdown, higher demand than planned and lost sales in certain markets due to the virus.

By Jessica Davis | October 21, 2017 | 12:00 PM

f t in

Customers of UK bank [redacted] still unable to access accounts four weeks after 'glitch'

Analysts say the chaos caused by an IT upgrade will cost the bank tens of millions in fines and compensation.

Niles Brignall | Sun 30 May 2016

f t d g

By JONATHAN BERR MONEYWATCH | May 16, 2015, 5:00 AM

"WannaCry" ransomware attack losses could reach \$4 billion

How Much Will Today's Internet Outage Cost?

Some companies lose tens of thousands of dollars for every minute of a DDoS attack.

ADRIENNE LAFRANCE | OCT 21, 2016

TECHNOLOGY

BUSINESS NEWS | JUNE 15, 2017 / 8:11 AM / A YEAR AGO

[redacted] CEO puts cost of recent IT outage at 80 million pounds

TWITTER | f

Why CTOs And CIOs Should Care More About The Cost Of Downtime

Forbes Technology Council

APR 06, 2016, 10:00AM • 479 views • 4 comments

Security Challenges

Data Centre • **Cloud**
AWS's S3 outage was so bad Amazon couldn't get into its own dashboard to warn the world
Websites, apps, security cams, IoT gear knackered
By Shaun Nichols in San Francisco 1 Mar 2017 at 03:00 122 SHARE

Customers of UK bank [redacted] still unable to access accounts four weeks after 'glitch'
Analysis say the chaos cause by an IT upgrade will cost the bank tens of millions in fines and compensation
Miles Brignall | Sun 30 May 2016

Millions of [redacted] Customer Records Exposed in Third-Party Data Leak
Dell Cameron | 03:17 12 12pm • Filed to DATA BREACH

threatpost
Cloud Security | Malware | Vulnerabilities | Privacy
Verizon Wireless Internal Credentials, Infrastructure Details Exposed In Access
[redacted] Private PGP Key Leak a Blunder, But It Could Have Been Worse

BUSINESS NEWS
JUNE 15, 2017 / 8:11 AM / A YEAR AGO
[redacted] CEO puts cost of recent IT outage at 80 million pounds
1 MIN READ

Why CTOs And CIOs Should Care More About The Cost Of Downtime
Forbes Technology Council
Apr 06, 2016, 09:00am • 879 views • 4 comments

Operations Challenges



Questions, questions...

Think about how you find the answer



Hardest
Questions:

1. How can we align IT infrastructure investment to business outcomes?
2. How can we empirically measure the progress of our IT Transformation program?
3. How much will it cost to “be compliant”?
How long will it take?




Hard Questions:

1. Have we seen any of these TTPs? Anywhere? In the last few months?
2. Are we PCI-DSS compliant (i.e. >TLS1.1) across the whole org?
3. How can we apply a critical out-of-band patch without impacting service?

Who would you ask?

How quickly could you determine the answer?



The “Easiest” Questions?

1. How many endpoints do we have?
2. What applications are installed, are they configured within policy?
3. Are they all patched and up-to-date, right now?
4. Who is on the network? What are they doing?

How up-to-date is this info?

How many different systems / teams would have differing results?

IT Hygiene

The process of continuously identifying assets, risks, and vulnerabilities across an environment and fixing them with speed and scale.

The IT Hygiene Cycle

Identify & manage risk through one continuous workflow.

Discover assets.

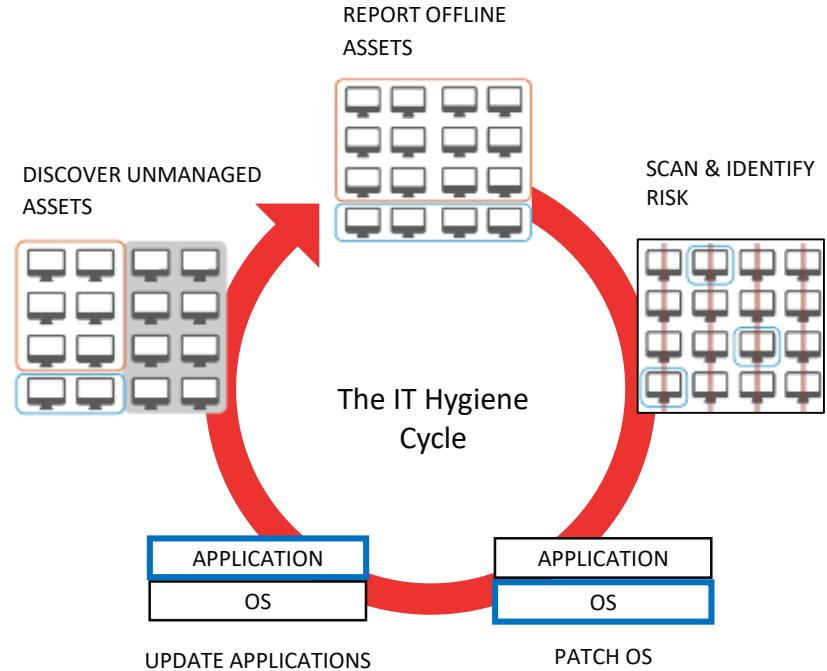
Get a comprehensive, accurate view of assets across your IT environment.

Identify risk.

Uncover gaps which weaken your organization's security posture.

Remediate gaps.

Take corrective action across your endpoints with speed at scale.



The changing nature of IT



Increasing
Endpoint Variety



Growing
Network Scale



Emerging Security &
Compliance Policies

Challenge #1:

Tool Proliferation

20

On average, teams use more than 20 tools to secure and operate their environments.

Source: Tanium, "Why best of breed may not be best"

Challenge #2:

Organizational Silos



Source: MyHubIntranet

Challenge #3:

Limited Visibility

leads to

Bad Data

Asset Management



Jim Schwar

@jimDFIR

Follow

Replying to @MalwareJake

CISO: How many windows hosts do we have?

AV Guy: 7864

Desktop Management: 6321

EDR Team: 6722

CMDB Team: 4848

SIEM Team: 9342

1:55 PM - 8 Feb 2018

516 Retweets 978 Likes



Challenge #4:

Fragmented Workflows



For every vulnerability patched, organizations lose 12 days to coordinating activities across teams.

Source: O. Soglow, New Yorker, 1940
Source: Today's State of Vulnerability Response:
Patch Work Demands Attention, Ponemon

Objective for Managing IT Ops & Security

Provide **consistent, foundational, real-time** visibility and control across endpoints in **any compute environment**.

Objective for Managing IT Ops & Security

“single pane of glass” for all endpoints

consistent capabilities for all use-cases

“seconds & minutes”, not “days & weeks”

Provide **consistent**, **foundational**, **real-time** visibility and control across endpoints in **any compute environment**.
At any scale.

Scaling from 10K to 100K to millions of endpoints in same environment

any computer, anywhere – DC, PoS, public or private cloud, back of a taxi – agnostic to location or service provider



The proven platform for endpoint visibility and control.

Speed at Scale

Designed to simplify and accelerate IT

Breadth of Visibility

Real-time visibility across your endpoints.

Precise Control

Confidently take action and verify results.

COMMITTED
TO CUSTOMER
SUCCESS

FORTUNE
100

>50%
Fortune 100



12 of Top 15 U.S.
Financial
Institutions



4 Branches
U.S. Armed Forces

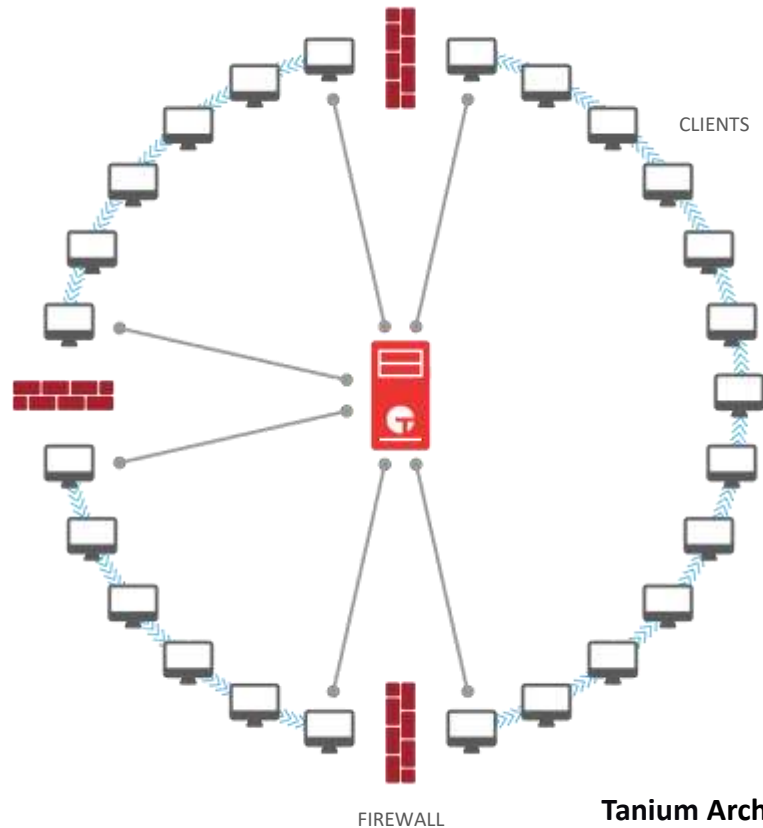
1M+ devices

Operating on
networks with >1M
devices

ONE PLATFORM
ONE AGENT
ONE SERVER

Proven on the world's largest and most complex networks.

- Faster and more reliable than legacy platforms
- Scale without massive hardware investments
- Reduces reliance on congested WAN links
- Connect off-network machines (cloud, roaming)



Tanium Architecture

Tanium Platform and Product Portfolio



Core



Interact



Trends



Connect

Operations



Discover



Asset



Map



Patch



Deploy



Performance

Risk



Comply



Integrity
Monitor



Reveal

Security



Threat
Response



Protect

Call to Action



- ✓ Address the fundamental requirements across all of IT
- ✓ Prioritise a single Source of Truth
- ✓ Simplify & accelerate IT - both Security & Ops!
- ✓ Don't buy a tactical solution for a strategic problem

Be sure you can answer the "easy questions"

*Tanium - Unternehmensweite Echtzeit-
Risikobewertung: Finde das schwächste Glied in
der Kette (Live Beispiele) Vortragssprache Deutsch*

9th October - 09.15/09.45 - Knowledge Forum F99





@smullis



<https://www.linkedin.com/in/smullis/>

Thank you

Learn more at [Tanium.com](https://www.tanium.com)