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.
Security Challenges

Petya cyberattack cost $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 23, 2017 | 11:50 PM

"WannaCry" ransomware attack losses could reach $4 billion

"WannaCry" is a ransomware attack that hit global businesses, and the losses could reach $4 billion.

By Jonathan Berl | May 16, 2017 | 12:00 AM

CEO puts cost of recent IT outage at 80 million pounds

The CEO of a major company puts the cost of a recent IT outage at 80 million pounds.

BUSINESS WIRE | June 20, 2017 | 9:11 AM

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

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

Miles Bignell | May 20, 2016

How Much Will Today's Internet Outage Cost?

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

Adrienne Larese-Whelan | Oct 21, 2019

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

CTOs and CIOs should be more concerned about the cost of downtime for their businesses.

Forbes Technology Council
Operations Challenges
Questions, questions…

Think about how you find the answer
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?
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

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
Challenge #3:

Limited Visibility leads to Bad Data
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

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

**At any scale.**

- “single pane of glass” for all endpoints
- consistent capabilities for all use-cases
- “seconds & minutes”, not “days & weeks”

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**

<table>
<thead>
<tr>
<th>FORTUNE 100</th>
<th>&gt;50% Fortune 100</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12 of Top 15 U.S. Financial Institutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 Branches U.S. Armed Forces</td>
</tr>
<tr>
<td>1M+ devices</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ONE PLATFORM</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONE AGENT</td>
</tr>
<tr>
<td>ONE SERVER</td>
</tr>
</tbody>
</table>
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 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
Thank you

Learn more at Tanium.com