



Expectation vs. reality

Crushing user experience and productivity in the
name of security

Tatu Seppälä

Alexander Solaat Rødland



- ★ Data security
- ★ Insider risk

Power Platform
Governance
IAM / Entra ID
Generative AI



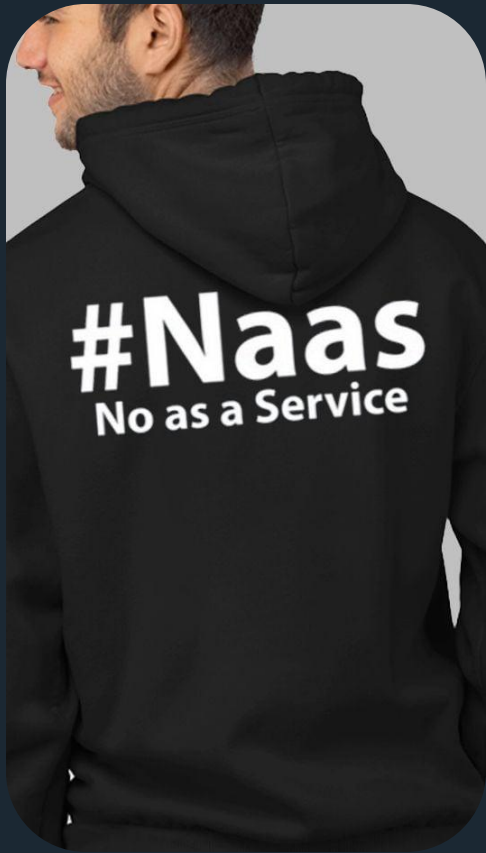
The Digital
Neighborhood



Tatu Seppälä
Security & Compliance Architect



Agenda



- > The hassle budget
- > The great disconnect
- > Unintended consequences
- > ~~Users~~ People are not stupid
- > The 2nd immutable law
- > ⚡ Call to action



Identity



Devices



Applications



Infrastructure



Networks



Data



Alex from IT

(The BlueScreen Brothers

Your Cloud ran into a problem and needs to restart.
Use the waiting time to check out the BlueScreen Brother YouTube Channel.
99% complete



For more information about this issue and possible fixes, visit:

<https://bit.ly/bstube>

If you call a support person, give them this info:
stop code: CRITICAL_NEED_OF_BLUESCREEN_BROTHERS

Why Software Sucks! With David Platt, Tatu & Alexander

Spill av (k)



0:05 / 56:47



HD



Why software sucks



BlueScreen Brothers

1,21k abonnenter

Abonner



0



Del



Lagre





Tatu Seppälä





"The **hassle budget** is the amount of security-related overhead that a user will **tolerate** in order to use a product."



-David S. Platt

"If there's one quality that defines human beings,
particularly of the computer-using variety, it's
laziness."

”Know thy user, for (s)he is not thee...”





"Eating your own **dog food** before releasing it to users helps your dog food taste slightly better than it otherwise would.

But it won't change it into cat food, and the dog food stage is too late to find that **your users really are cats.**"



“..it should be hard, damn it!”





BUSINESS



SECURITY



Why security (often) sucks

- No business alignment
- Policy **communicated** - but **not enforced**
- Policy **enforced** – but **not communicated**
- Disregard for natural human behavior
- Understaffed security teams
- **Secure score** ≠ **Actual security outcomes**



”It’s for *security reasons*..”





FIRE BAN!

Who can get an exemption? **NO ONE**

Yes, but... **NO ONE**

THE BAN ALSO APPLIES WHEN:

- you are careful
- you know several experts, or are an expert yourself
- it is raining, or you have put out the fire your whole life
- you're far from the police
- you have looked at a map
- there is a school / daycare nearby
- you feel that grilling it is part of a great trip

The answer is NO!



<https://brannmidt.no/balbrenning>



Lillestrøm
kommune

”Laziness trumps everything..”



💰 What's the cost?

..of a data breach?

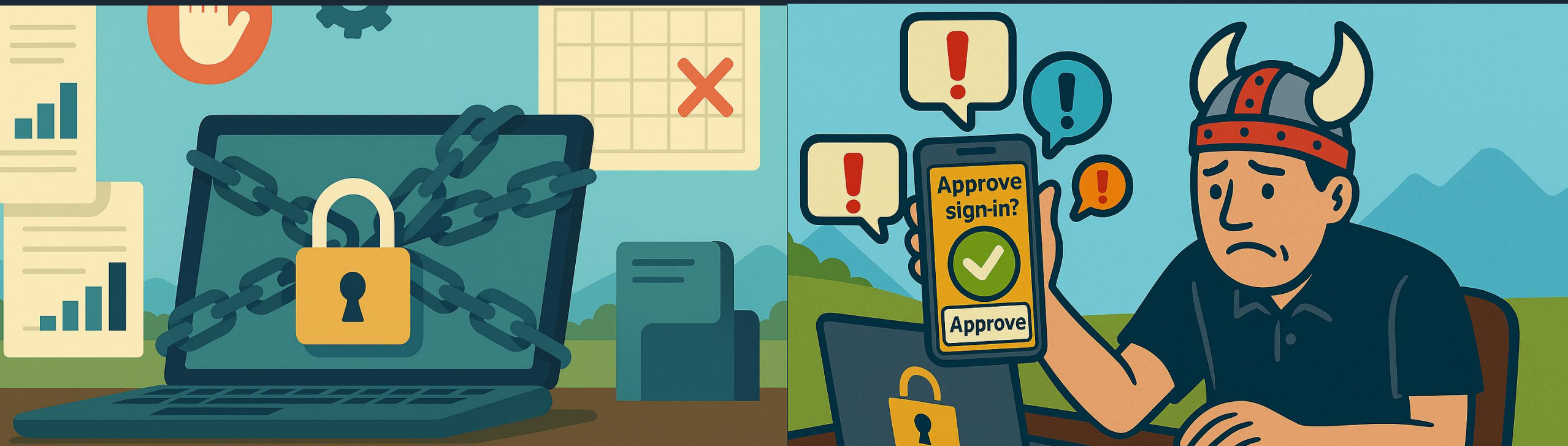
👉 Predictable

👉 Measurable



💰 What's the cost?

..of inflexible security measures not tailored to business requirements?



Shadow IT explosion





Security fatigue



Poor security culture



Stalling productivity & innovation

RESIGNATION LETTER



High turnover of talent



Demo

Dealing with pesky outdated devices full of security holes – the effective way



- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home > Apps

Apps | App protection policies

+ Create policy Refresh Columns Export

Overview

All apps

Monitor

By platform

Windows

iOS/iPadOS

macOS

Android

Policy

App protection policies

App configuration policies

iOS app provisioning profiles

S mode supplemental policies

Policies for Office apps

Policy sets

Other

App selective wipe

App categories

E-books

Filters

Help and support

Help and support

Policy	↑↓	Deployed	↑↓	Updated	↑↓	Platform	↑↓	Management
Unmanaged Android device MAM		Yes		2/19/23, 4:21 AM		Android		Apps on unma

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

Home > Apps | App protection policies > Intune App Protection

Intune App Protection | Properties

Unmanaged Android device MAM

Search

Overview

Manage

Properties

Help and support

Diagnose and solve problems

Policy saved

Unmanaged Browser

Unmanaged Browser

Org data notification

Start Microsoft To Do

app-launch

Access requirements

PIN for access

PIN type

Simple PIN

Select minimum PIN

Biometrics instead

Override biometric

timeout

Timeout (minutes)

Class 3 Biometrics

Override Biometric

biometric updates

PIN reset after num

Number of days

Select number of

maintain

App PIN when de

Work or school ac

access

Recheck the acces

(minutes of inacti

Conditional laun

Setting

Max PIN attempt

InPrivate

alexander@solaat.one

CONTOSO (SOLAAT.ONE)

Management type

↑↓

Apps

↑↓

Apps on unmanaged devices

39

Value

Action

5:06 AM

2/19/2023

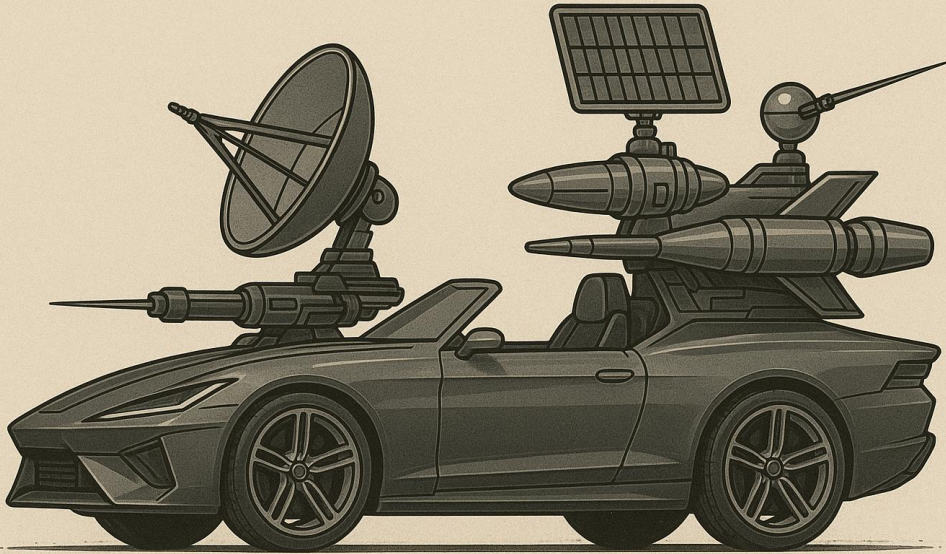
Value

Action

Which type of SecOps pro are you?

You got a problem?

We got you covered!



Users are **stupid** and should not be trusted with a magnetic sketcher!



WE DESIGN EVERY VOLVO TO LOOK LIKE THIS.



You're looking at a perfect Volvo. A Volvo that performed exactly as our safety engineers designed it to.

Its front and rear ends, for example, collapsed on impact. As a result, much of the crash energy was absorbed instead of being passed on to the passengers.

The car's middle section, however, didn't collapse. That's because the entire passenger compartment is surrounded by Volvo's unique "safety cage." Made of six box section steel pillars, this protective housing is strong enough to support the weight of six Volvos.

But the passengers of this car were also protected in ways you can't see. Because inside are such standard features as a driver's side Supplemental Restraint System, a collapsible steering column and, of course, 3-point seat belts, front and rear.

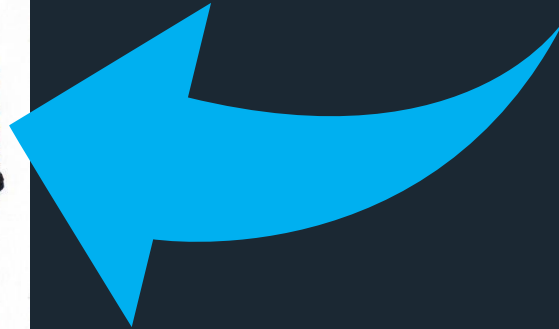
Every Volvo is designed to help protect its passengers in all these ways. And, as a result, will look remarkably similar to this one after being in the same type of accident.

If you're concerned about safety, you can't find a more beautiful car.

VOLVO
A car you can believe in.

CALL TOLL FREE FOR YOUR CATALOG OF 1991 VOLVOS: 1-800-221-9136. © 1990 VOLVO NORTH AMERICA CORPORATION.

Your security solution design goal



How much security do I need?

- Limit the impact of mistakes without breaking **business processes**
- A certain amount of risk can and must always be accepted
- **How much?** “It depends.”



Demo

When there is no clear path to share files with or collaborate with externals..



SharePoint

Search this library

HR

HR team

Private group | Confidential \ Internal only

Not following

1 member

+ New

Upload

Edit in grid view

Share

Sync

All Documents

Details

Documents

>

Recruitment strategy

Name

Modified

Modified By

Sensitivity

TC demo - Legal - NDA.docx

About a minute ago

ADM Tatu Seppälä

General

- Home
- Sites
 - Active sites
 - Deleted sites
- Containers
- Policies
- Sharing**
- Access control
- Settings
- Content services
- Migration
- Reports
- More features

Sharing

Use these settings to control sharing at the organization level in SharePoint and OneDrive.
[Learn more about managing sharing settings](#)

External sharing

Content can be shared with:

SharePoint

OneDrive

Most permissive	Anyone Users can share files and folders using links that don't require sign-in.
	New and existing guests Guests must sign in or provide a verification code.
	Existing guests Only guests already in your organization's directory.
Least permissive	Only people in your organization No external sharing allowed.

You can further restrict sharing for each individual site and OneDrive. [Learn how](#)

Granular sharing control in SharePoint Online (with container Sensitivity Labels)

Edit sensitivity label

- ✓ Label details
- ✓ Scope
- ✓ Items
- Groups & sites**
- ✓ Privacy & external user access
- External sharing & conditional access
- Private teams & shared channel settings
- Schematized data assets (preview)
- Finish

Define external sharing and conditional access settings

Control who can share SharePoint content with people outside your organization and decide whether users can access labeled sites from unmanaged devices.

☒ Control external sharing from labeled SharePoint sites

When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.

Content can be shared with

- ☐ Anyone ⓘ
Users can share files and folders using links that don't require sign-in.
- ☐ New and existing guests ⓘ
Guests must sign in or provide a verification code.
- ☐ Existing guests ⓘ
Only guests in your organization's directory.
- ☒ Only people in your organization
No external sharing allowed.

☐ Use Microsoft Entra Conditional Access to protect labeled SharePoint sites

You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions.



Granular sharing control in SharePoint Online (with container Sensitivity Labels)

The screenshot displays the Microsoft Teams interface. On the left, the 'Chat' sidebar shows a list of teams and channels. The 'Bifrost Bridge' channel is selected. The main area shows the channel's file list. A file named 'Business data.csv' is visible, with a sensitivity label 'Confidential \ Inter...' applied. The interface includes standard Teams navigation elements like 'Unread', 'Channels', 'Chats', and 'Unmuted' buttons, as well as a top navigation bar with 'Posts', 'Files', and 'Notes' tabs.

Chat ... 🔍 📄 ▼

Unread Channels Chats Unmuted ▼

Teams and channels

- Valhalla
- 1 🦊 Loki's Lounge
- 2 🗣️ Asgard announcements
- 3 🌈 Bifrost Bridge**
- 4 ✂️ Viking Ventures
- 5 🌸 Freya's Feedback
- 6 🛡️ Shield Wall Support
- 7 🏆 Valhalla Victories
- 8 🏰 Odin's Office
- Example shared channel 🌐
- Shared channel demo 🌐
- Test shared channel 🌐
- Legal team
- Lounge
- Johtoryhmän tiimi
- Johtoryhmän keskustelut
- Leadership team

3 🌈 Bifrost Bridge Posts Files ▼ Notes ➕

Confidential \ Inter... 🗨️ ▼ 🗂️ ...

+ New ▼ 📄 Edit in grid view 📄 Open ▼ 📄 Share 🔗 Copy link ...

☰ All Documents ▼ ✕ 1 selected 📄 Details 🔍

3 🌈 Bifrost Bridge

✓	📄	Name ▼	Modified ⓘ ▼	Modified By ▼	Sensitivity ▼	+ Add column
✓	📄	Business data.csv	...	📄	☆	About a minute ago ADM Tatu Seppälä



Granular sharing control in SharePoint Online (wo/ container Sensitivity Labels)



Connect to SharePoint Online

```
Connect-SPOService -Url https://<your-tenant>-admin.sharepoint.com
```

Get all site collections

```
$sites = Get-SPOSite -Limit All
```

Loop through each site and disable external sharing

```
foreach ($site in $sites) {  
    Write-Host "Disabling external sharing for site: $($site.Url)"  
    Set-SPOSite -Identity $site.Url -SharingCapability Disabled  
}
```

```
Write-Host "External sharing has been disabled for all SharePoint sites."
```

Enable sharing for specific sites

```
Set-SPOSite -Identity <siteurl> -SharingCapability ExternalUserSharingOnly
```



"Security only works if the **secure** way
also happens to be the **easy** way."

-The 2nd immutable law of security

Demo

“AI services are blocked until risk management measures are in place”, said the CISO..





Recycle Bin



Work - Edge



Q3-25
Budget
forecast



Adobe
Acrobat



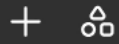
ENG
FI



16.40
31/05/2025

What can I help with?

Ask anything









Files - Dropbox

https://www.dropbox.com/home

Dropbox

Search

Home

All files

Recents

Starred

Photos

Signatures New

Shared

Upload

Create

Drop files here to upload, or use the 'Upload' button

Click to upgrade

Sales and Marketing - Monthly R

https://m365x36864533.sharepoint.com/sites/SalesAndMarketing/Shared%20Documents/Forms/AllItems.aspx?...

Global Sales Global Sales Retail Operations Sales and Marketing Retail

Sales and Marketing

Public group Not following 20 members

+ New

Upload

Edit in grid view

Share

All Documents

Documents > Monthly Reports

Name	Modified	Modified By	+ Add column
Australia Sales.xlsx	October 13, 2022	Megan Bowen	
Brazil Sales.xlsx	October 13, 2022	Megan Bowen	

English

New

Purview ... English

Search English

Confidential document

1 item | 1 item selected 64.5 KB | Error



"That which is easy to do *will* be done frequently, **whether it should be or not**"

MORDAC, THE PREVENTER
OF INFORMATION
SERVICES.

SECURITY IS MORE
IMPORTANT THAN
USABILITY.



scottadams@aol.com

www.dilbert.com

IN A PERFECT WORLD,
NO ONE WOULD BE
ABLE TO USE ANYTHING.



11-16-07 © 2007 Scott Adams, Inc./Dist. by UFS, Inc.

To complete the
log-in procedure,
stare directly
at the sun.





Have you ever tried sitting down with your security people with a box of donuts?

⚡ Call to action

- > 🧑‍💻 Develop a healthy interest in your business users. **They are not stupid** and have meaningful things to accomplish with their digital tools.
- > 👁️ When blocking an action with technical controls, stop to think two steps ahead – **how is the user likely to respond?**
- > 🙋 **Don't be "the department of no"** - remember that security is about enabling business to work securely

 If you blocked yourself into trouble,
you can't block yourself out of it! 



”Excuse me sir!”

Comments or
questions?

Connect with me!

