IBM SECURITY DAYS EVENT

NDB

DIGITALL88 IBM Platinum Partner | telelink BUSINESS SERVICES IBM Platinum Partner | CNSYS IBM Gold Partner



ZERO TRUST - THE NEW NORMAL, ACHIEVED WITH IBM SECURITY VERIFY PRIVILEGE

telelink
BUSINESS SERVICES



AGENDA

- What is Zero Trust
- Privileged problems
- The Solution

Konstantin Tomanov
Director Information Security
Konstantin.Tomanov@tbs.tech

telelink BUSINESS SERVICES

Zero Trust

What is Zero Trust?

Zero Trust is the term for an evolving set of network security paradigms that:

- move network defenses from wide network perimeters to narrowly focusing on individual or small groups of resources.

- no implicit trust granted to systems based on their physical or network location (i.e., local area networks vs. the Internet).

- access to data resources is granted when the resource is required.

- authentication (both user and device) is performed before the connection is established.


NIST

PUBLICATIONS

Zero Trust Architecture

Published: August 10, 2020

Author(s)

Scott W. Rose, **Oliver Borchert**, Stuart Mitchell, Sean Connelly

telelink BUSINESS SERVICES

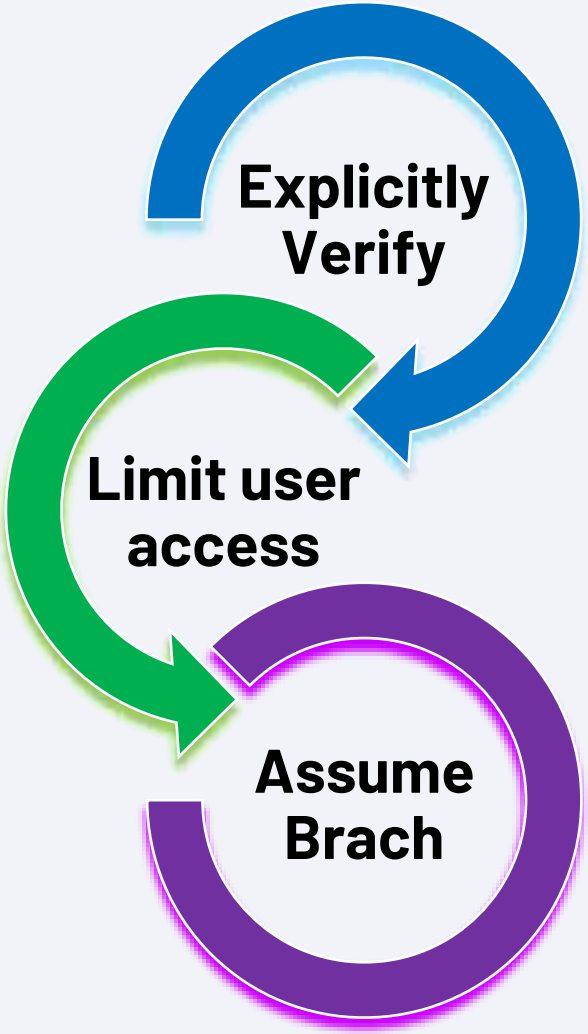
Principles of Zero Trust

Never trust, always verify

Principle of Least Privilege

Don’t rely on perimeter-based controls

Assume Breach !!!

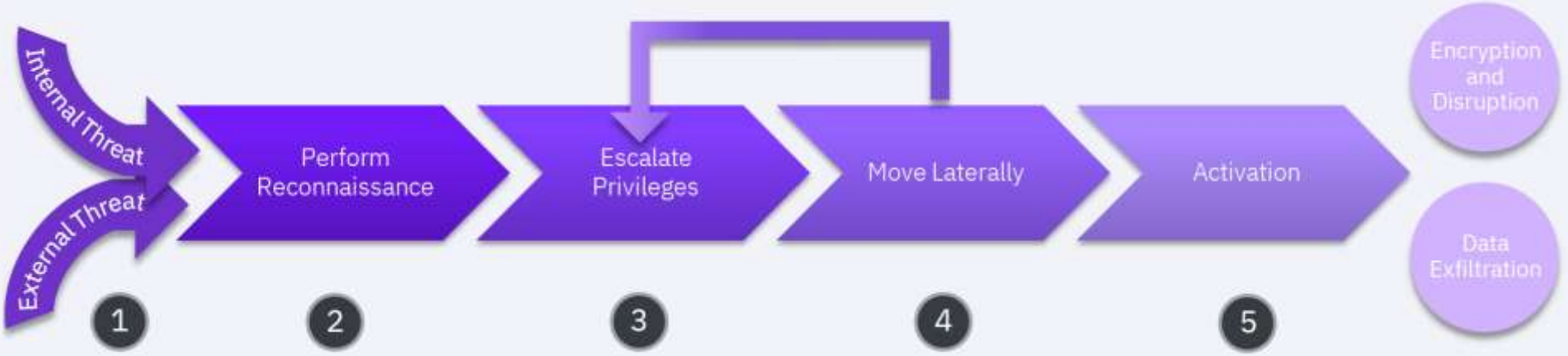


telelink
BUSINESS SERVICES

Assume Breach

IBM Platinum Partner

Ransomware, insider threats, and other persistent attacks are highly sophisticated and can go undetected for weeks or months



telelink BUSINESS SERVICES

Why the new normal?

Zero Trust Comes Into The Mainstream In Europe (Forrester)

Over a third of businesses have a Zero Trust strategy. According to the Forrester Analytics Business Technographics® Security Survey, **2020**, about **25%** of security decision-makers in Europe had a Zero Trust implementation as a major priority. In contrast, Forrester's Security Survey, **2022**, shows that over **66%** of the same group have begun developing a ZT strategy.

Gartner predicts

Gartner predicts spending on zero trust network access (ZTNA) solutions will grow **from $820** million this year **to $1.674** billion in **2025**, attaining a 26% Compound Annual Growth Rate (CAGR)

telelink BUSINESS SERVICES

Why the new normal?



MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM › PRESIDENTIAL ACTIONS

*„The Federal Government must adopt security best practices; **advance toward Zero Trust Architecture**; .... and **invest in both technology and personnel** to match these modernization goals."*



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

*"This memorandum sets forth a Federal **zero trust architecture** (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives **by the end of** Fiscal Year **2024** in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns."*

telelink BUSINESS SERVICES

Privileged PROBLEMS

telelink
BUSINESS SERVICES

The "Traditional Ones"

IBM Platinum Partner

Non-human accounts used by IT staff which often have unfettered access to critical data and systems i.e. Domain Admin, root.

Exist everywhere in nearly every connected device, server, hypervisor, OS, DB, or application: on-premises & cloud.

Represent one of the **most vulnerable** aspects of an organization's IT infrastructure.

Shared accounts and access, lack of tracking and monitoring.

*Privileged accounts represent the largest security threat an organization faces today. Forrester estimates that at least **80%** of data breaches have a connection to compromised **privileged credentials**, such as passwords, tokens, keys and certificates."*

Source: Forrester : Privileged Access Management Forrester Wave

telelink BUSINESS SERVICES

The "Modern" One

IBM Platinum Partner

ChatGPT is being used by Cybercriminal to create Malware.

According to cybersecurity specialists, cybercriminals have begun leveraging OpenAI's artificially intelligent chatbot ChatGPT to quickly construct hacking tools...

Analytics Insight

Armed With ChatGPT, Cybercriminals Build Malware And Plot Fake Girl Bots

Cybercriminals have started using OpenAI's artificially intelligent chatbot ChatGPT to quickly build hacking tools, cybersecurity researchers warned on Friday. Scammers are also testing ChatGPT's ability to build other chatbots designed to impersonate young females to ensnare targets, one expert monitoring criminal forums told Forbes.

Forbes

telelink BUSINESS SERVICES

THE SOLUTION

IBM Security Verify Privilege

telelink
BUSINESS SERVICES

The solution

IBM Platinum Partner

- Zero Trust is not a product, but tools can definitely help
- Think holistically
- More than just network security

Enabling the **right user**
under the **right conditions**
to have the **right access**
to the **right data**

Identity & Access Management with IBM Security Verify

- Access management (SSO, MFA)
- Identity governance
- Secure privileged access

telelink BUSINESS SERVICES

Quickly discover, control, manage, & protect privileged accounts

IBM Platinum Partner



ESTABLISH VAULT

Setup secure encrypted vault, permissions, users, and structure

RUN DISCOVERY

Discover all of your unknown privileged accounts

PROTECT SECRETS

Store and Rotate your sensitive accounts within Secret Server

DELEGATE ACCESS

Implement RBAC, Access Requests and other controls

CONTROL SESSIONS

Add session launching, proxies, monitoring, and recording

telelink BUSINESS SERVICES

Password vaulting

IBM Platinum Partner

Features	Benefits
Stores privileged credentials in an encrypted, centralized vault	Delegate access securely and efficiently.
Provides granular access on per need-to-know basis	Eliminate weak passwords and password reuse.
Manages the credentials lifecycle	Reduce the risk of unauthorized privilege escalation.
On Premises or Cloud	Protect privileged service accounts.
	Define organizational tree structure for credentials.

telelink BUSINESS SERVICES

Privileged Accounts Discovery

IBM Platinum Partner

Features

Gain a single, comprehensive view of all your Windows or Unix privileged accounts

Receive reports to help assess the security of your privileged passwords and highlight potential risks

Re-run discovery at any time to identify new privileged accounts and confirm compliance with security policies

Benefits

Automate the discovery of accounts

Define and onboard privileged users

Automate reporting for auditing purposes

telelink BUSINESS SERVICES

Credential policies

IBM Platinum Partner

Features	Benefits
Provides a set of rules applicable all at once to multiple secrets. Including, but not limited to, automated password changing and verification, required check out, session proxying, command restrictions and more.	Define different security settings for different teams or credential types. Enhance local and domain credentials' security through regular changes. Control administrative activities through command black and whitelisting. Know exactly when, how, and why privileged accounts are being used.

telelink BUSINESS SERVICES

Access approval

IBM Platinum Partner

Features	Benefits
Built-in workflow engine for approval processes.	Increased visibility and oversight for all privileged accounts, especially those accessed sporadically for special projects and by third parties.
Native ticket system integration, e.g., ServiceNow or BMC	Approve ad-hoc access requests for a limited time-period.
Double-lock capabilities for additional authorization.	Use single or multiple steps approval process.
	Protect highly sensitive data.

telelink BUSINESS SERVICES

MFA & Remote Access

IBM Platinum Partner

Features	Benefits
Support for any TOTP application that uses the TOTP RFC6238 algorithm, such as Microsoft or Google Authenticator.	Enforce additional authentication to critical systems and privileged accounts from anywhere.
Support for FIDO2/Yibikey tokens.	Choose from wide variety of software/hardware tokens.
Integration with Duo Security.	Improved and secure usability for remote workers and third-party contractors with nothing but a browser.
Second factor authentication support for both the user portal and usage of privileged credentials within.	Control and audit external access.
Remote Access Service for secure VPN-less access for external parties.	

telelink BUSINESS SERVICES

Monitor and record privileged sessions

IBM Platinum Partner

Features	Benefits
Real-time view of all privileged user sessions. Terminate risky or unauthorized sessions, or send a message directly to the user Keystrokes recorded and available for quickly searching during the playback of sessions. Activity heatmap to pinpoint moments of activity that auditors would like to review during the entire session.	Maintain a full audit and video trail for used privileged accounts. Quickly identify sessions and operations of interest within the session. Enhanced troubleshooting and investigations. Comply with industry, government and organizational regulations.

telelink BUSINESS SERVICES

Privileged Behavioral Analytics

IBM Platinum Partner

Features

Machine learning and behavior pattern recognition.

Suspicious and anomalous activity detection.

Real-time alerting.

Risk scoring.

Enhanced graphical visualization of privileged activity within the environment.

Benefits

Detect breaches before they happen.

Reduce security risks and coordinate streamline response procedures.

Analyze distribution and access of privileged accounts across your organization.

Prioritize the alerts that matter the most.

telelink BUSINESS SERVICES

A successful PAM program

IBM Platinum Partner



telelink BUSINESS SERVICES

A successful PAM program

IBM Platinum Partner

Insight
Do you have visibility into your privileged access management gaps?

Prevention
Can you adequately secure privileged credentials?

Detection
Can you detect inappropriate privileged account use?

Response
Can you take action when a suspicious event involving a privileged account occurs?

Recovery
Can you recover privileged credentials after a breach or system failure?

telelink BUSINESS SERVICES



THANK YOU!

Konstantin Tomanov
Director Information Security
Konstantin.Tomanov@tbs.tech