MFA

Multi Factor Authentication

About Raz-Lee Security

Founded in 1983, Raz-Lee Security is one of the world's leading independent owned cybersecurity and compliance solution providers for IBM i servers (AS/400).

Raz-Lee's flagship iSecurity suite guards organizations against insider threats and unauthorized external access to business-critical information hosted on their IBM i. We have developed cutting-edge solutions that have revolutionized analysis and fortification of IBM i servers.

We build solutions that work with other companies' technologies allowing organizations to monitor IBM i activity via SIEM or DAM dashboards.

Technology Business Partners

imperva IBM McAfee

Akamai RSA SEA SOFTWARE ENGINEERING OF AMERICA

RAZ-LEE iSecurity

About iSecurity Suite

Advanced Threat Protection

- **Anti-Ransomware**
- **Antivirus** / Malware protection
  - **ICAP** Optional Client/Server for Antivirus

Authentication & Authorization

- **MFA** Multi Factor Authentication
- Self **Password Reset**
- **Authority On Demand**

Protection

- **Firewall** FTP, ODBC…access
- Monitor CL **Commands**
- **Safe-Update** to protect production files

Evaluation, Reporting & Alerts

SIEM & DAM Support

Syslog, SNMP, CEF, LEEF

Visualizer

Business Intelligence for Security

Score Cards

for GDPR, SOX, PCI, HIPAA…

Security Investigator

Data Discovery, Authority Inspector, Assessment

Encryption

- DB2 **Field Encryption** (FIELDPROC)
- **PGP File Encryption**

Data Base Solutions

- **AP-Journal** DB Audit, Filter, Alerts, SIEM
- **DB-Gate** Native SQL to Oracle, MSSQL…
- **FileScope** Secured file editor

Auditing & Response

- **Audit** Journal, System Values, Status…
- Proactive re-**Action** in real time
- **Capture** screen activity
- **Compliance** of Users, Objects, IFS
- **Change Tracker** watch Production Libraries

RAZ-LEE iSecurity

MFA

Multi Factor Authentication

RAZ-LEE iSecurity

MFA Definitions

MFA Multi-factor authentication Helps organizations meet compliance standards and improve the existing security environment on IBM i. It requires a user to verify his or her identity with two or more credentials before gaining access to sensitive systems and data.

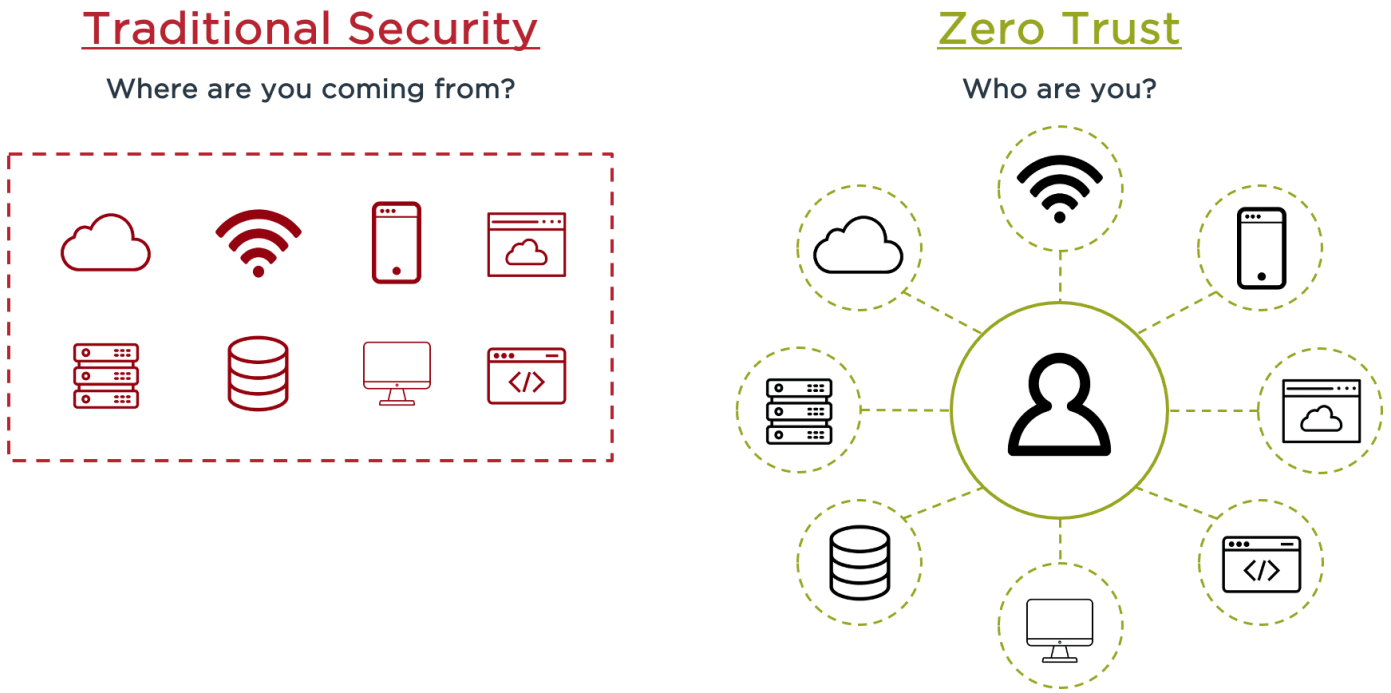
Multi-factor authentication (MFA)

- A powerful solution to enable Secure Sign On
- Used to achieve and maintain compliance with leading industry regulations such as PCI-DSS
- Lately it has also become a necessity to qualify for cyber insurance
- MFA significantly reduces the risk of system penetration, up to a remarkable 99%

Zero Trust Approach

Zero Trust is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction.

Rooted in the principle of “never trust, always verify,” Zero Trust protect modern environments and enable digital transformation by using strong authentication methods, leveraging network segmentation, preventing lateral movement and simplifying granular, “least access” policies.



RAZ-LEE iSecurity

MFA in iSecurity Implementation

MFA is actually satisfied by only two factors

- ✓ User/Password – IBM Standard
- ✓ One of the Following:
  - One-Time Password
  - TOTP
    - Time Based One-Time Password
    - Changes every 30 seconds
    - RFC 6238
  - Emergency Tokens – Six characters, at least one of which is alphabetic

TOTP tokens (RFC 6238), can be generated by the free Google Authenticator, Microsoft Authenticator, and many other software or hardware generators.

Token Generators

We use ANY Token generator, such as Google Authenticator on a mobile or by any hardware device

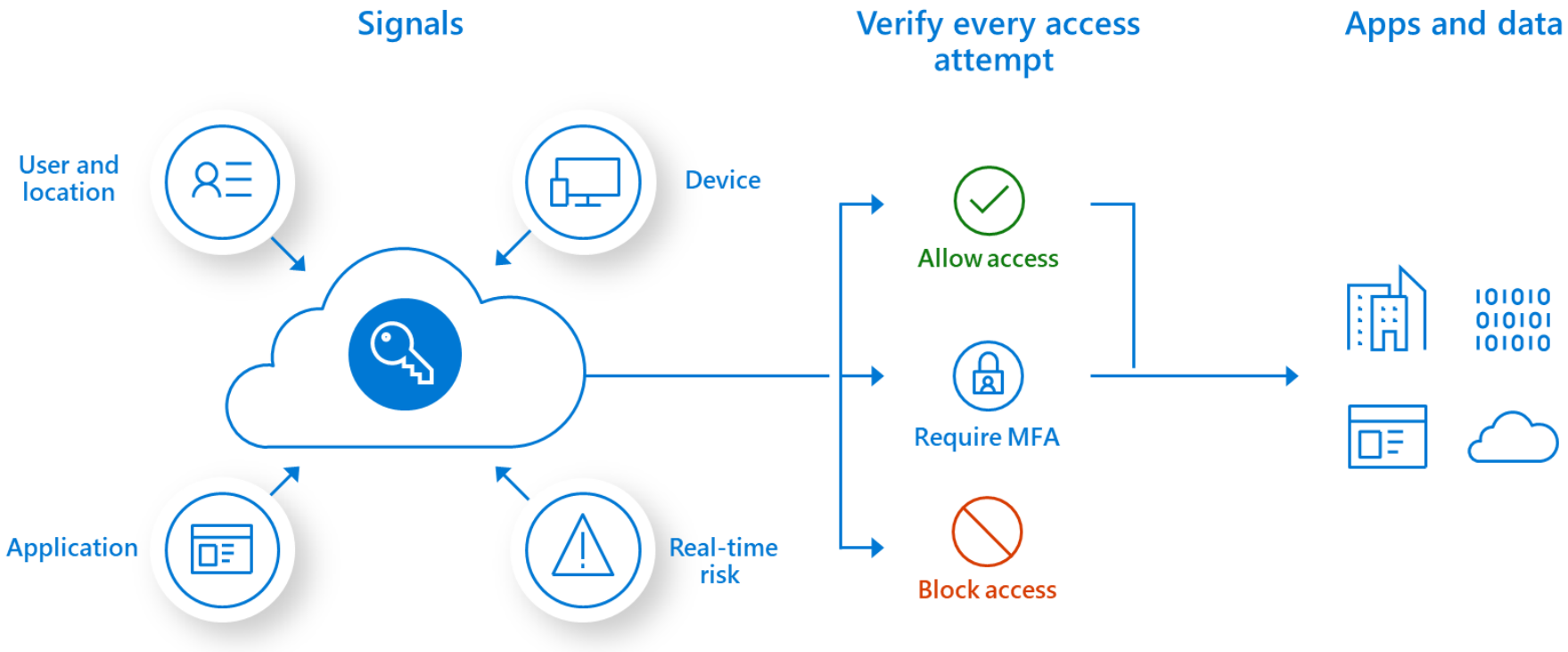
Token generator creates a six-digit codes.

- Codes change every 30 seconds.
- Codes are based on a random 26-characters password.
- The password is entered only once.

Password is usually passed as a QR code, or as a Character String.

Where are you from and Who are you?

Based on these two questions we can resume the workflow of iSecurity MFA



RAZ-LEE iSecurity

MFA Building Blocks – Person

Person

The term Person refers to a human being

Each person may have multiple user profiles on multiple systems

Once a Person has been verified by MFA as working from an IP, he is not bothered again when he signs on to other sessions on this or other systems with a user profile that belongs to him

This may be limited by time.

The term Sign On includes Regular Sign On, as well as TCP services such as FTP, ODBC, REXEC, IFS share

MFA Building Blocks - IP Group

IP Group

The regular IP Addresses from which a Person signs on can be grouped in an IP Group, e.g. one or more offices and home addresses.

With MFA, you can decide what the system should do when a person signs on from within or from outside of the IP Group. You can decide to use MFA only when signing on from the outside, or request MFA when signing on from within, and reject other attempts.

This behavior can be set differently for regular Signing On, FTP, ODBC, REXEC, IFS share etc.

Persons and Locations

Now we talk about the combination of Person + IP group, this is extremely important because we can block or allow a person to enter the system depending on his location, so we totally ensure not only that the person is who she says she is, also we know where that person is logging in from.

John

- New York
- Atlanta (2 User Profiles)
- Tel Aviv
- Home

MFA Required Inside

Otherwise Rejected

Nataly

- New York (3 User Profiles)
- Atlanta

MFA Not Required Inside

MFA Required Outside

Matthew

- Tel Aviv
- Home

MFA Not Required Inside

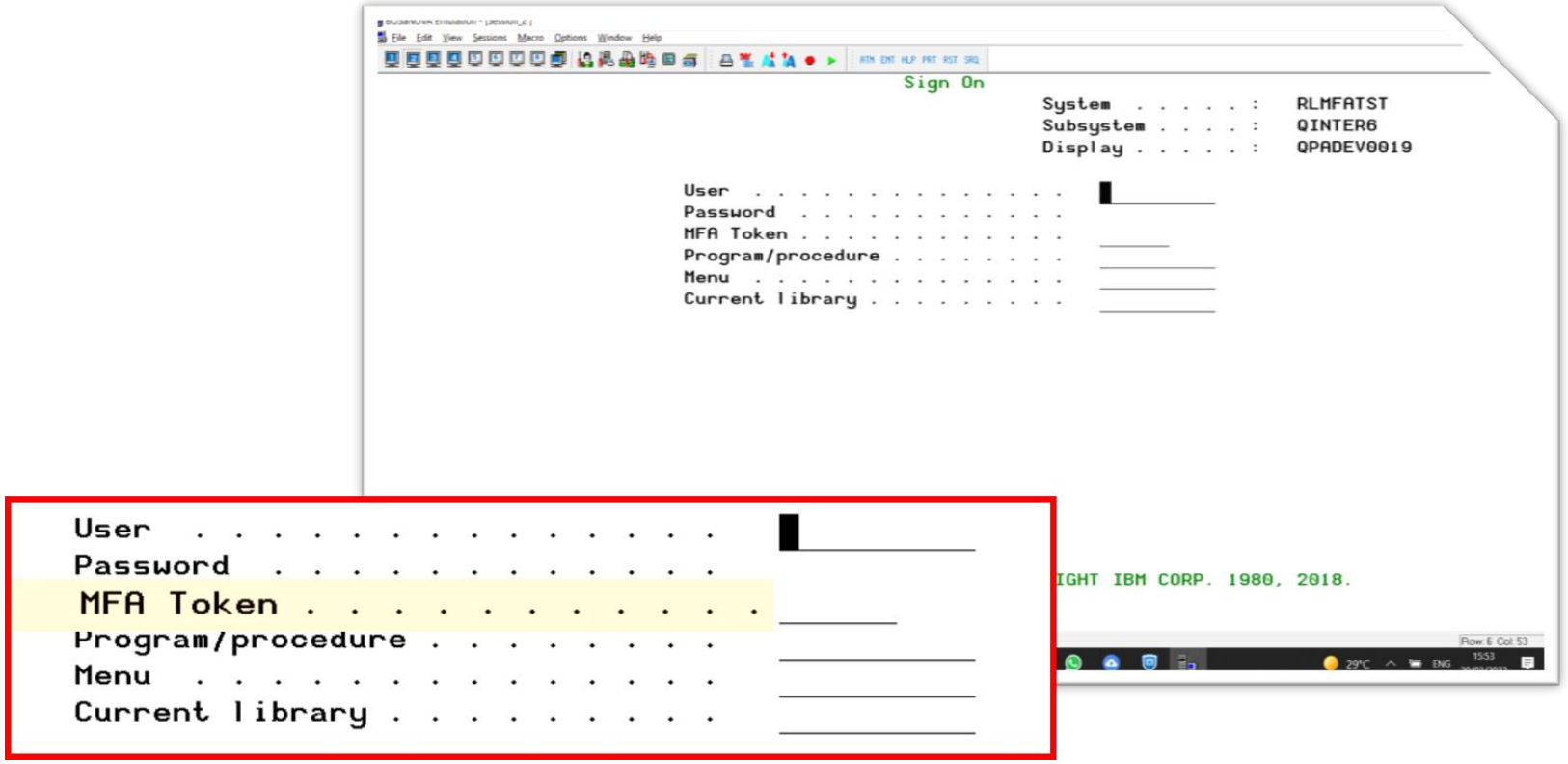
Otherwise Rejected

RAZ-LEE iSecurity

One Single Step Authentication

Single Step

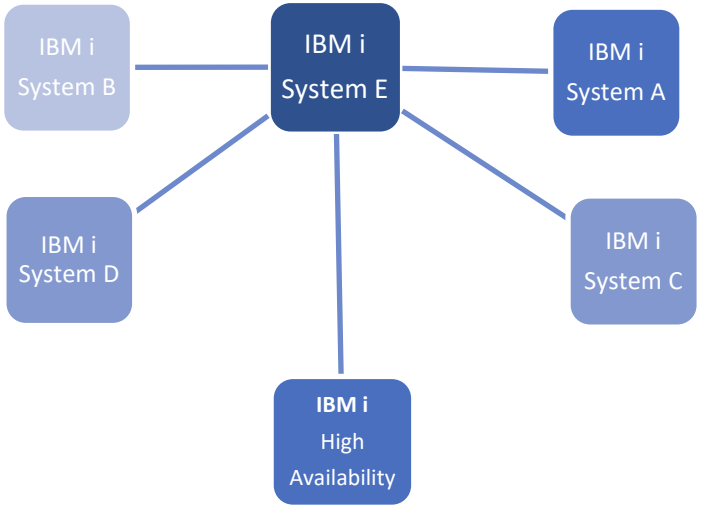
Single Step Authentication is considered safer. iSecurity MFA enables you to modify the IBM i standard Sign On screen by adding the MFA Token entry field, following the regular password



RAZ-LEE iSecurity

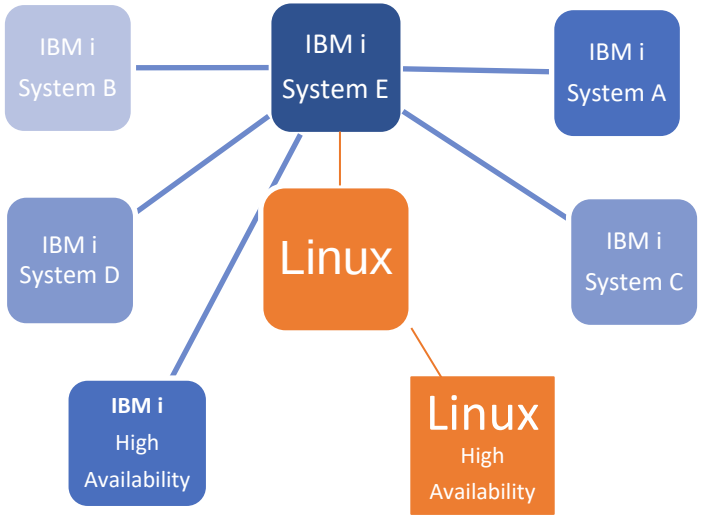
Simplicity

iSecurity MFA/PR/AOD



- ✓ Completely Native to the IBM I
- ✓ It installs and activates in minutes
- ✓ No need of additional hardware server
- ✓ No special Smartphone application is needed
- ✓ No special PC application is needed
- ✓ No knowledge of other OS is needed

Others' approach



- × Additional Hardware
- × Additional Software
- × Second Operating System
- × High Complexity

RAZ-LEE iSecurity

iSecurity MFA Advantages

- Organizational approach
- Considers Person (multiple user profiles on multiple systems)
- Considers origin IP address of the Sign On
- One MFA is good for all Person's activities, from same IP, for a specified time.
- Controls Sign On in one step. MFA Token is part of the standard Sign On screen
- Also controls:
  - FTP Server
  - FTP Client
  - File Server
  - DDM/DRDA
  - REXEC
  - ODBC
  - Remote Pgm/Cmd

Thank You

For more information about our company and products please visit

www.razlee.com