Cisco Duo

Zero Trust: Secure by Design

Jeff Yeo, CCSP, CISSP, ITIL, COBIT
Regional Technical Solutions Architect, ASEAN
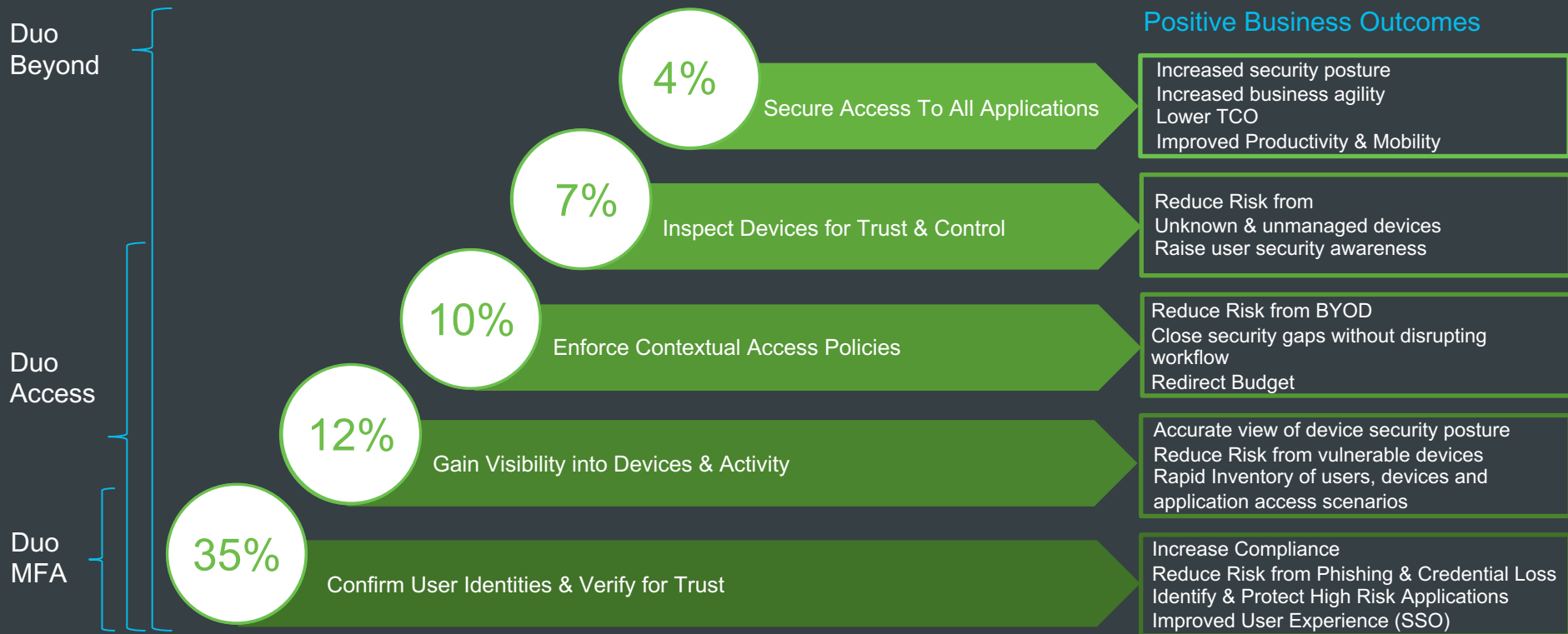jefyeo@cisco.com
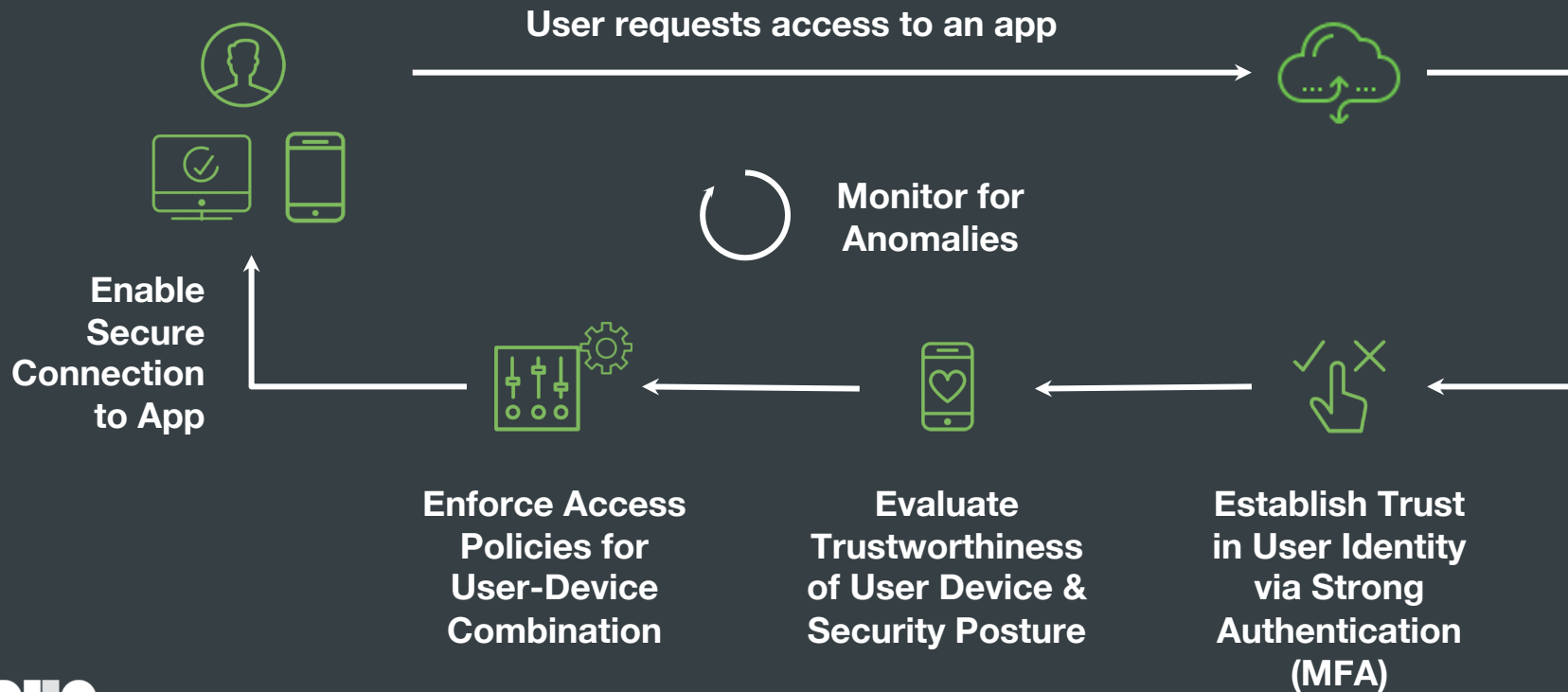
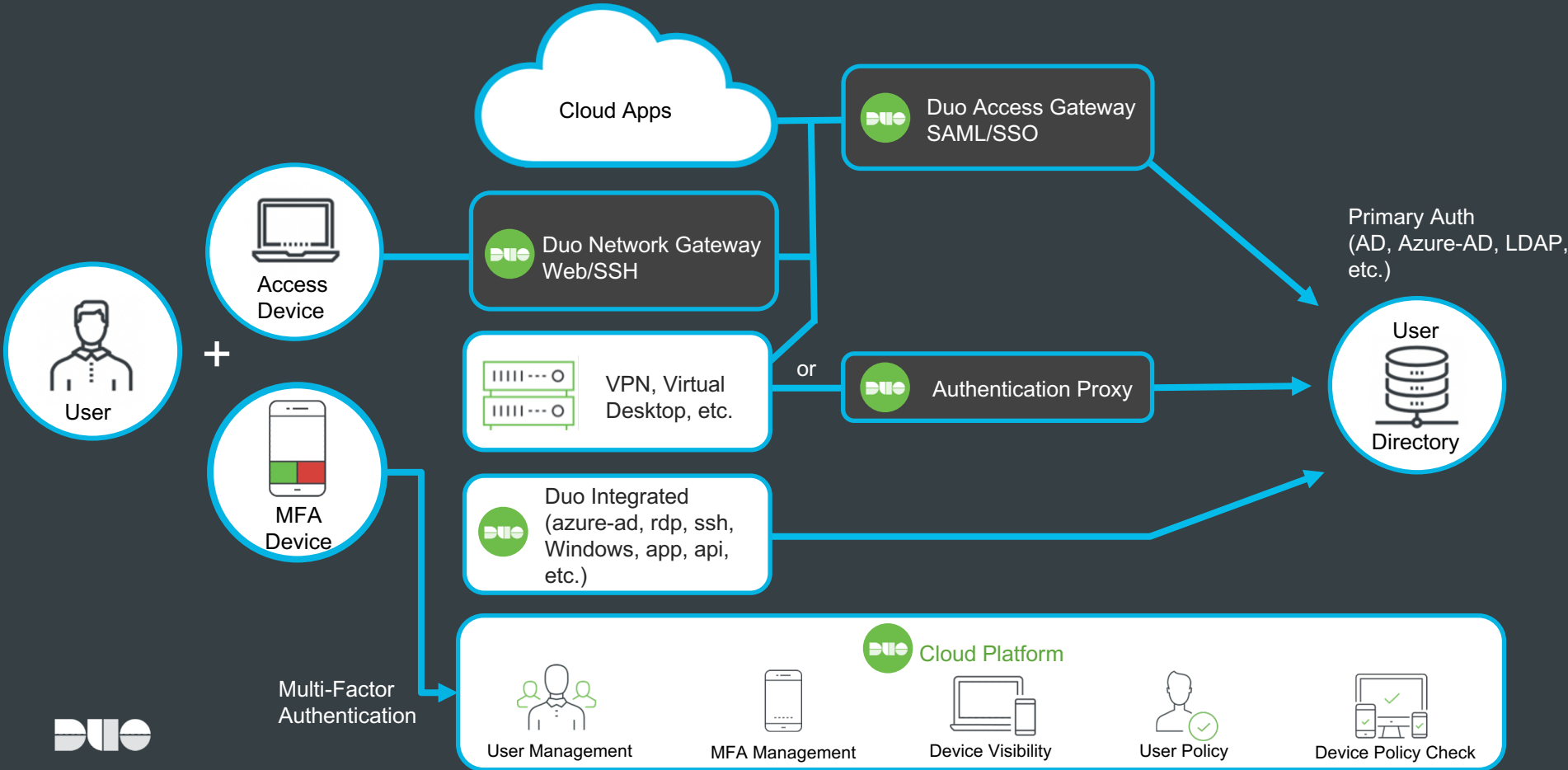# How does Duo help customers get to a zero-trust setup?

Duo 5 Phase Maturity Model for Zero Trust

Duo Beyond

Duo Access

Duo MFA

Positive Business Outcomes

4% — Secure Access To All Applications
- Increased security posture
- Increased business agility
- Lower TCO
- Improved Productivity & Mobility

7% — Inspect Devices for Trust & Control
- Reduce Risk from
- Unknown & unmanaged devices
- Raise user security awareness

10% — Enforce Contextual Access Policies
- Reduce Risk from BYOD
- Close security gaps without disrupting workflow
- Redirect Budget

12% — Gain Visibility into Devices & Activity
- Accurate view of device security posture
- Reduce Risk from vulnerable devices
- Rapid Inventory of users, devices and application access scenarios

35% — Confirm User Identities & Verify for Trust
- Increase Compliance
- Reduce Risk from Phishing & Credential Loss
- Identify & Protect High Risk Applications
- Improved User Experience (SSO)

Zero Trust Access

User requests access to an app

Monitor for Anomalies

Enable Secure Connection to App

Enforce Access Policies for User-Device Combination

Evaluate Trustworthiness of User Device & Security Posture

Establish Trust in User Identity via Strong Authentication (MFA)

DUO

Duo Solution Architecture

Policy Engine: Building Trusted Access

Factors

Trusted Users
Strong user authentication for all types of users.

New User
Group Access
User Location

Trusted Authenticators
Enforce security

Trusted Devices
Establish device trust without agents

Trusted Endpoints
Remembered Devices
Operating systems
Browsers
Plugins

Tampered Devices
Screen Lock
Full-Disk Encryption
Mobile Device Biometrics

Trusted Network
Establish network trust

Authorised Networks
Anonymous Networks

DUO

Use Case - Assess Mobile Device Posture **without MDM**

- Check if mobile devices are up-to-date

- Verify encryption and passcode lock

- Check if devices are jailbroken or tampered

- Works for managed and unmanaged mobile devices
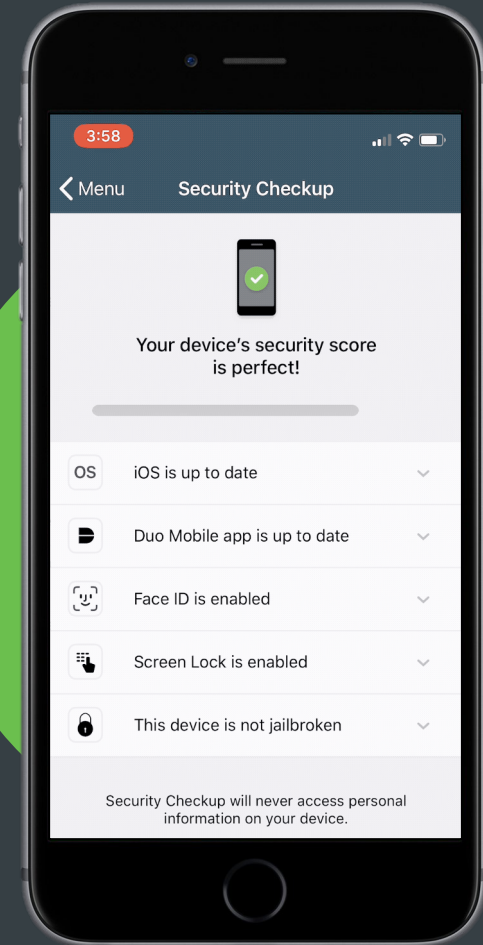
# Use Case – Windows & RDP

Requirements

Users required to utilise MFA to access local and remote Windows workstations

Solution

Duo integrates with Microsoft Windows client and server operating systems to add two-factor authentication to Remote Desktop and local logons.

Solution Components

Duo MFA/Access/Beyond Edition
Duo Authentication for Windows Logon
Duo Mobile
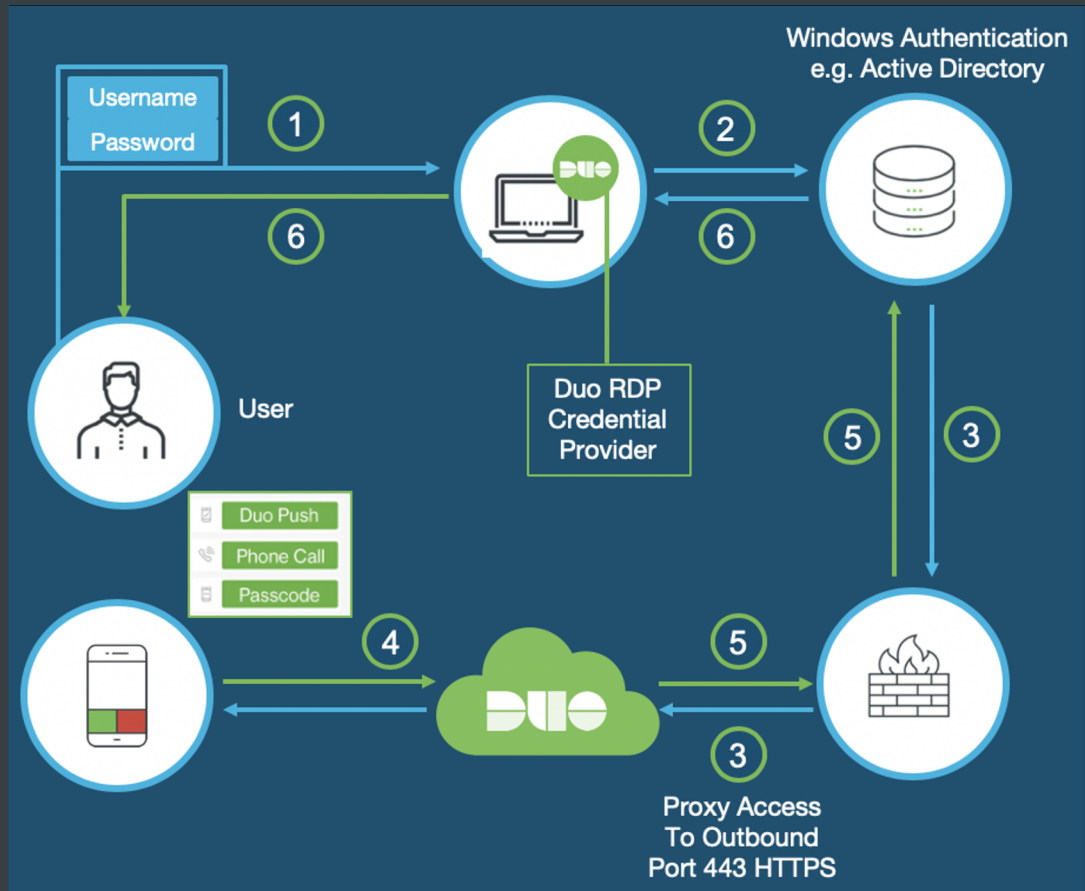
Duo Trust Monitor: User Behavior Analytics

Audience
Security analysts
("Gary")

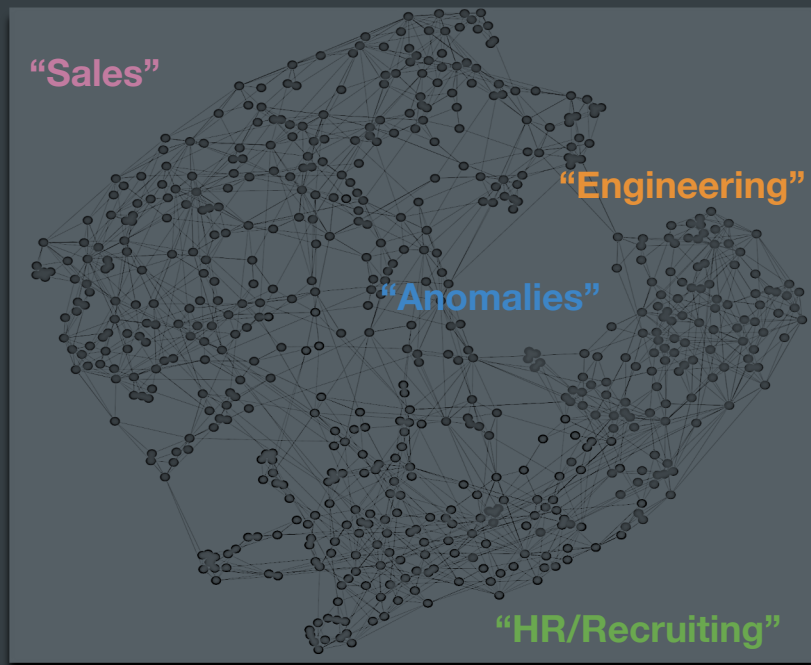**Data**
Properties of incoming
authentications

Goal
Surface *valuable* and
actionable events for
Gary

Method
Build ML models to
analyze authentications
on Gary's behalf

DUO

Duo Trust Monitor: Surfacing Access Anomalies

Duo Trust Monitor creates a tailored baseline of access activity in a corporate environment:

- **who** typically accesses
- which **applications**
- from which **devices**
- at which **times**
- from which **locations**

What is the value to our customers?

| Visibility & Policy Hardening | Risk Detection & Prevention | Security Efficiency | Adaptive Authentication |

- Customer understands what's normal vs. atypical
- Refine access policy based on anomalous logins

- Designate high priority applications
- Gain insight into when these assets are accessed anomalously

- Reduce investigative burden
- Enable junior analysts with a tool that is easy to use and maintain

- Reduce requirements in low-risk authentications
- Step up in suspicious scenarios

DUO

How is Cisco Duo's solution different from other zero-trust vendors?

How Duo Differs

Duo's approach to zero-trust is different from other vendors in 4 ways:

1. **Speed to security:**
   Duo delivers all of the zero-trust building blocks under one solution

2. **Ease of use:**
   Ease of deployment, maintenance and ease of use for your users

3. **Broadest coverage of applications, users, and devices:**
   Accommodating to the different types of applications, users, and devices in your environment

4. **Lower TCO:**
   Operationalizing a solution, from technology to people, from acquisition to deployment to maintenance to retirement

DUO

100 Million+
Annual Recurring Revenue,
EOY 2017

500 Million
Authentication Events Every Month

70+
Net Promoter Score

98%
Of Customers
Recommend Duo

99.99%
Uptime (every year since 2014)

10,000+
Customers Trust Duo

Customers in
100+ Countries

Over 10,000 customers worldwide

- **3000+** Technology
- **500+** Higher Education
- **600+** Healthcare
- **1500+** Financial Services
- **350+** Government
- **80+** Fortune 500

Thank You

Security made easy and effective