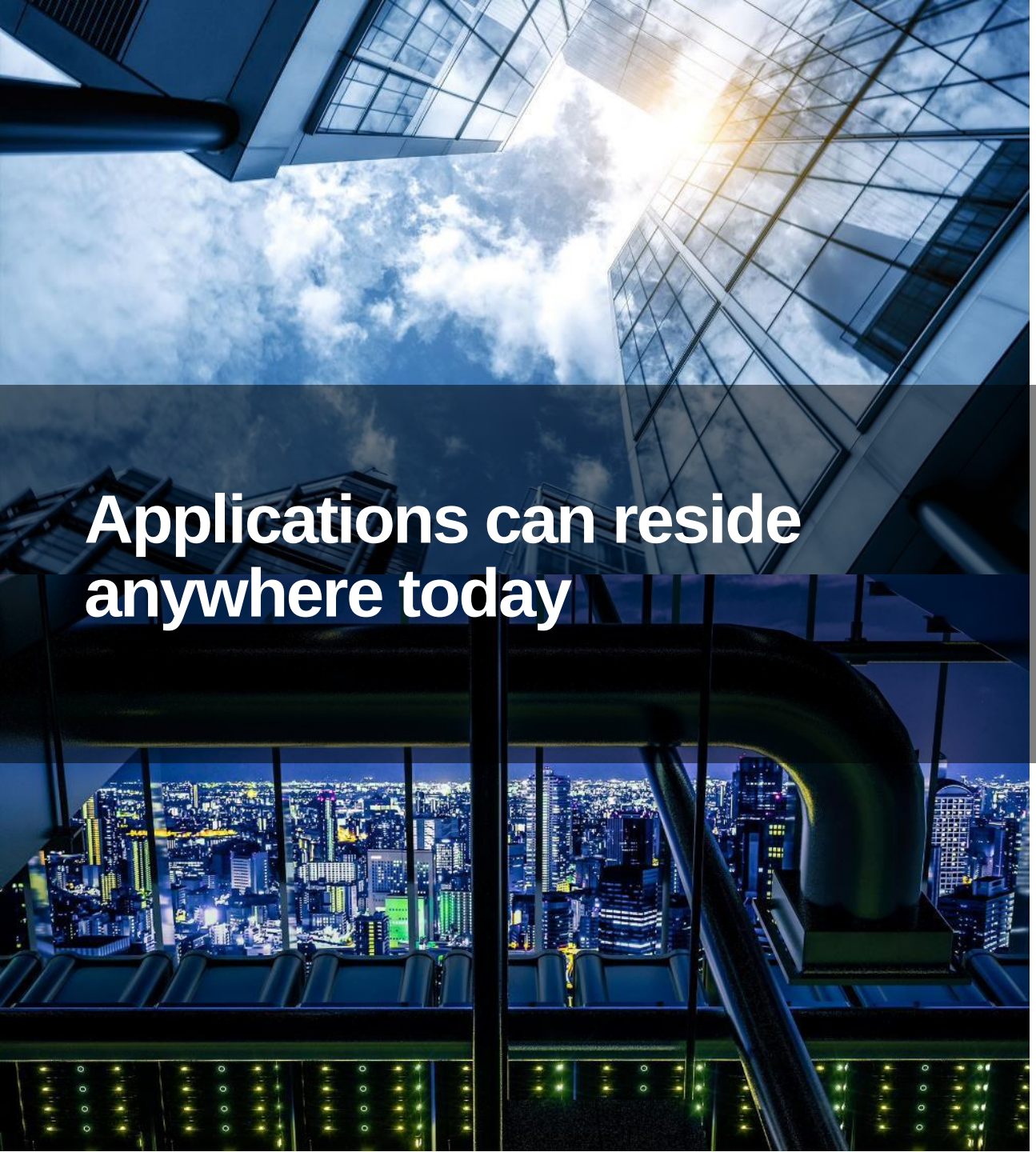
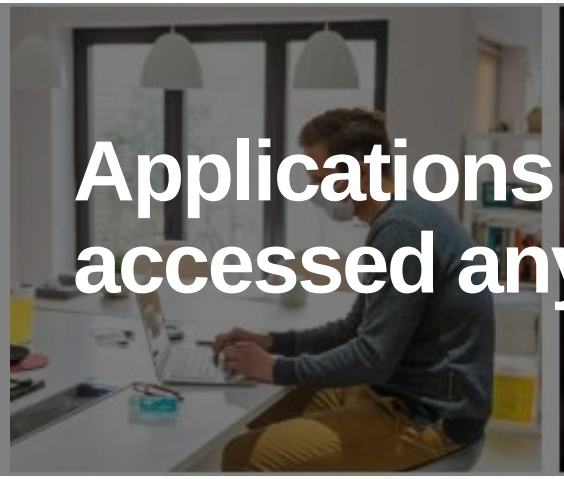
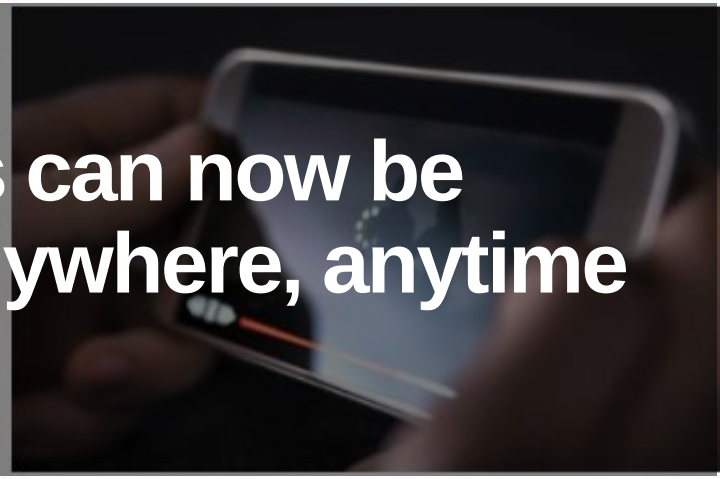
Delivering Zero Trust Application Access

DANIEL VARELA
Solutions Engineer Security



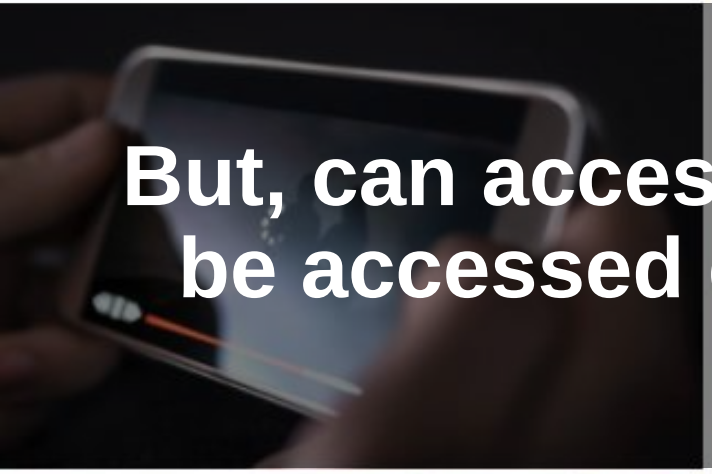
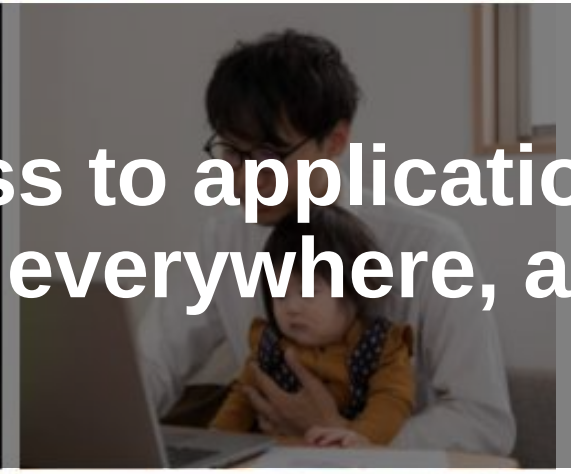
Applications can reside anywhere today





Applications can now be accessed anywhere, anytime



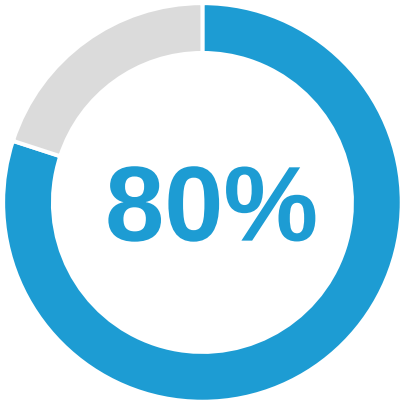




But, can access to applications that reside anywhere and be accessed everywhere, at anytime *really* be trusted?



Apps Today Reside Anywhere and Everywhere

... AND LIKELY WILL FOR THE FORESEEABLE FUTURE



The simplest enterprise workloads are in process of migration to the cloud, but the remaining 80% of workloads remain on-premises

An average of 760 cloud-based (IaaS) apps per organisation

An average employee uses at least 8 SaaS apps and an average organisation of 1,000 employees uses 203 SaaS apps

~60% of IT decision makers believe apps that touch critical data and systems must remain on-premises for security reasons, 42% say they can't migrate off legacy systems because they're mission-critical

Source: McKinsey & Co. for IBM

Application Threats

ORGANISATIONS FACE MANY VARIED, DANGEROUS THREATS TO APPLICATIONS AND THEIR DATA

Unauthorised access

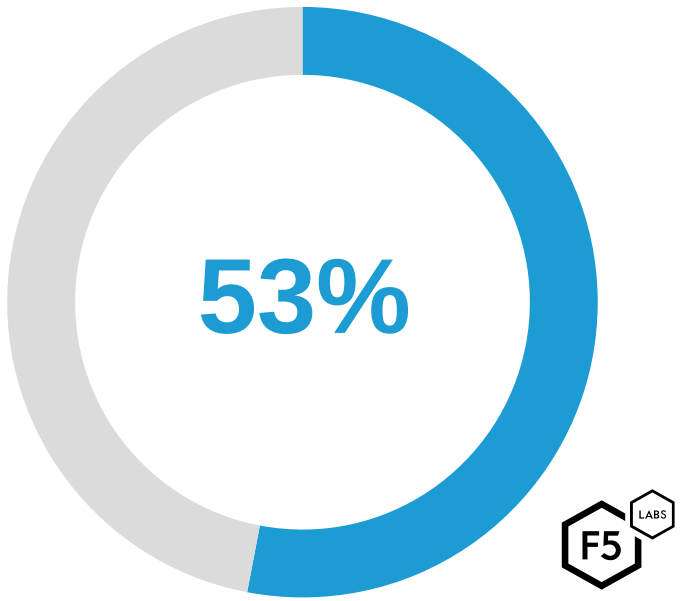
Stolen credentials

Insider threats

Applications and Identities Are Key Attack Targets

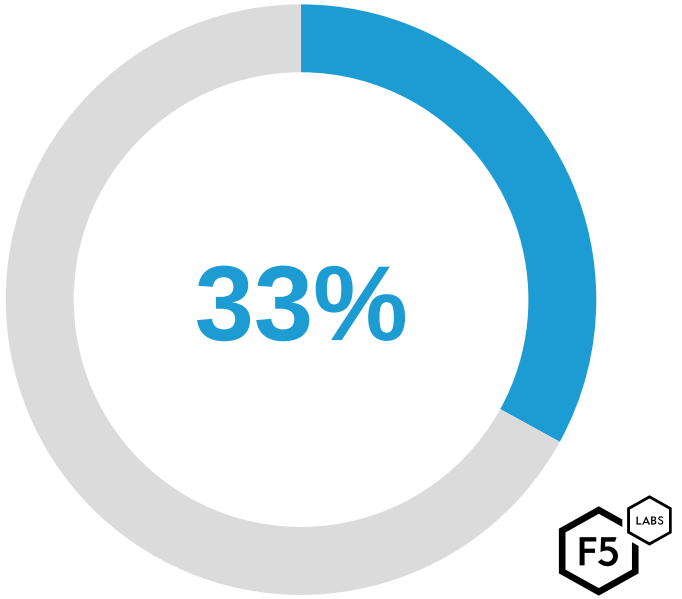
APPLICATIONS

Initial Targets of Breaches
2008 - 2018



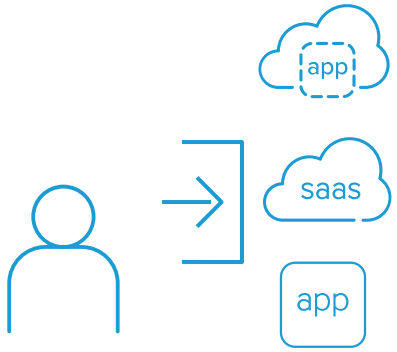
IDENTITIES

Initial Targets of Breaches
2008 - 2018



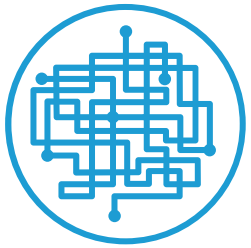
Source: Lessons Learned from a Decade of Data Breaches, F5 Labs

Application Access Challenges



Securing application access, regardless where the app resides or user is located (internal or remote)

Inappropriate and overprivileged user access to applications



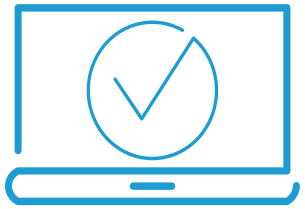
Complicated application access

The Network Perimeter Is No More

"TRUST, BUT VERIFY" IS OUTDATED AND DANGEROUS – IT'S NOW "ZERO TRUST"

NEVER TRUST

ALWAYS VERIFY



CONTINUOUSLY MONITOR

The Zero Trust Approach

ELIMINATES THE IDEA OF A TRUSTED NETWORK INSIDE A DEFINED PERIMETER

*"A way to think about cyberthreats is to **assume you have already been compromised**; you simply don't know it yet. That is the necessary mindset in today's hostile environment.*

*'Trust but verify' leaves you flatfooted and sets you up for crisis management. Zero Trust may seem stark, but it is the **proactive, architectural approach** to align with mission priorities."*

Source: Forrester Research

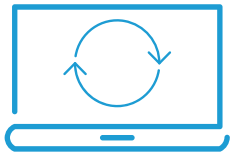
Challenge: Enforcing Zero Trust for App Access

NEVER TRUST

- How should users trust be tested?
- Will users inside the network need to login to apps?
- Will users who have already accessed apps need to re-login?

ALWAYS VERIFY

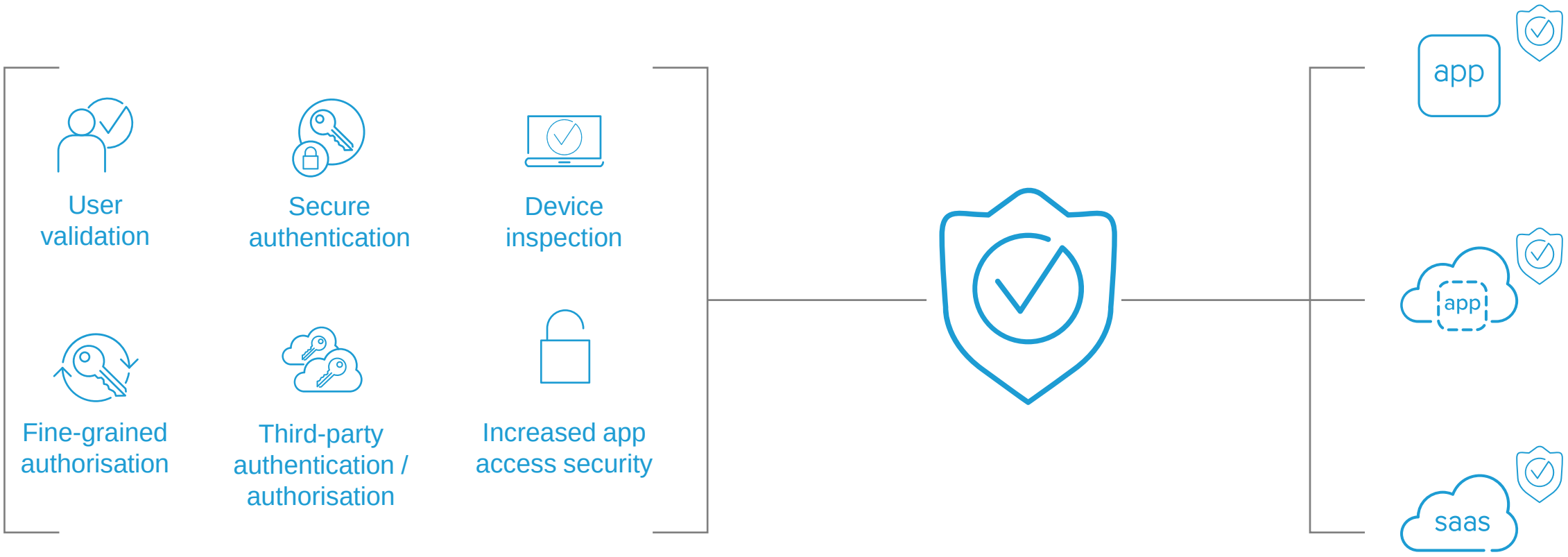
- Will users need to be re-verified when attempting to access any app?
- Will users' devices and their security need to be verified?
- Will users' locations need to be checked?
- Will apps need to be verified for security and access?



CONTINUOUSLY MONITOR

- Will users' devices need to be continuously checked? How, and how often?
- Will users' locations need to be monitored continuously?
- Will users' network access need to be watched for its security?

Needed: Seamless, Secure Application Access



How to Ensure Appropriate Application Access

CREATING AND ENFORCING CONTEXT-AWARE POLICIES

- Is it the ”right” user?
- Is it the “right” device?
- Is the device secure?
- Does it meet and adhere to a security baseline throughout the app session?
- Is the app secure?
- Is the app sensitive?
- Does the user have access rights to the app?
- Is the app time or date sensitive?
- Does the user have rights to access the app at this time?
- Are there locations from which the app may not be accessed?
- Is the network accessing the app secure?
- Are there other access controls or limits on the user, the app, or access to the app?

app

app

saas

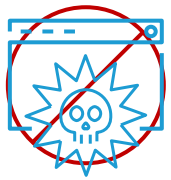
Only the “right” users should be able to access the “right” apps at the “right” time, with the “right” device, with the “right” configuration, from the “right” place

Ensuring User Identity

LEVERAGE A ROOT OF TRUSTED IDENTITY, WHILE INTRODUCING AND ENFORCING MODERN AUTHENTICATION ACROSS ALL APPS

Fewer credentials for users to create and remember

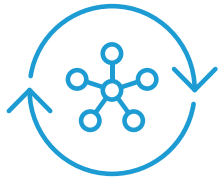
Increased use of multi-factor authentication



Less theft of application credentials

Not a Typical Remote Access Use Case

ZERO TRUST APPLICATION ACCESS / IDENTITY AWARE PROXY IS DIFFERENT

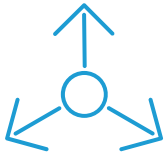


Continuous, increased granular traffic control

Continuous and more granular control of step-up authentication

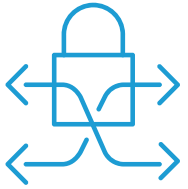
Faster and continuous device posture checking

Third-party risk engine or data source, to make access decisions



Simpler deployment of complex access controls

Simpler integration with third-party identity providers (IDaaS)



Per request-based app access