eBook

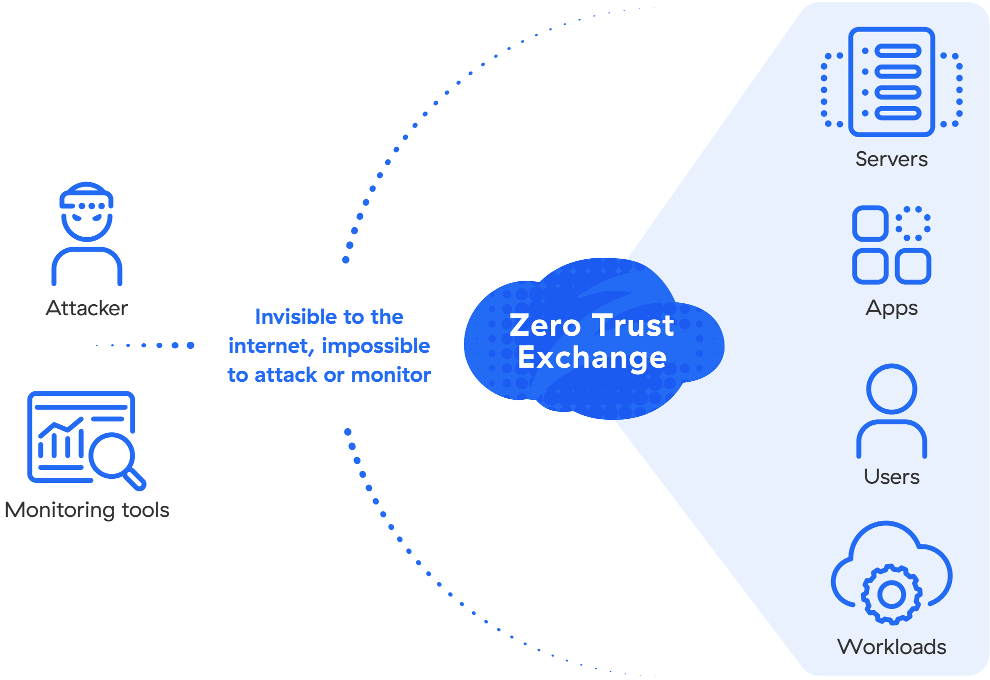
Why Network Monitoring Tools Fail Within Secure Environments

Contents

Fundamental shift

There is a fundamental shift happening through secure digital transformation, which includes application transformation (data center to SaaS, IaaS, PaaS), network transformation (hub-and-spoke to direct connectivity), and security transformation (castle-and-moat to zero trust).

As these transformations occur, Security Service Edge (SSE) is growing rapidly as a solution to fundamental challenges related to secure edge computing, remote work, and digital transformation. SSE is a convergence of network security services delivered from a unified cloud platform. As organizations adopt infrastructure and software as a service (IaaS, SaaS) offerings and cloud apps, their data becomes more distributed outside their on-premises data centers. In addition, many organizations' users are increasingly mobile and remote, connecting to apps and data from everywhere, over any connection.



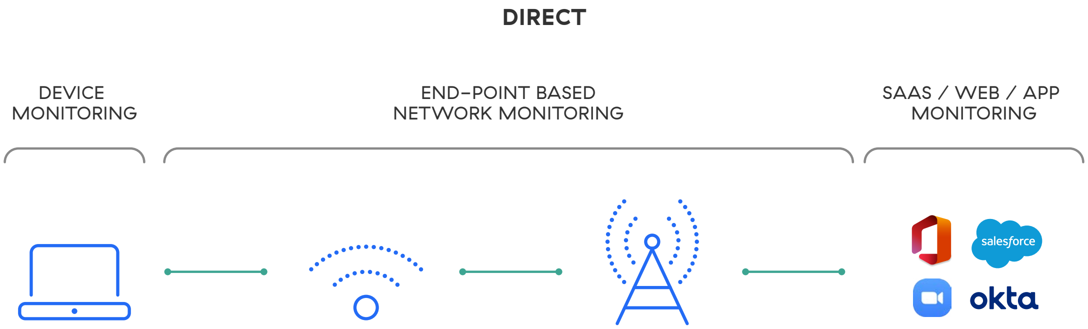
Limiting the attack surface breaks traditional monitoring tools

As enterprises move toward secure digital transformation and work-from-anywhere initiatives, they must be aware that traditional monitoring tools are insufficient for determining the source of any issues that may arise. Gaining visibility into devices, networks, and applications that don't reside within the data center is difficult, as they are out of the IT team's control. Achieving the ideal balance between restricting the attack surface and monitoring visibility is an ongoing challenge.

In order to understand why network monitoring tools fail within a secure environment, we must first look at how users connect. As employees continue to operate in a hybrid model, there are three common scenarios end users experience, all of which pose challenges for network operations teams.

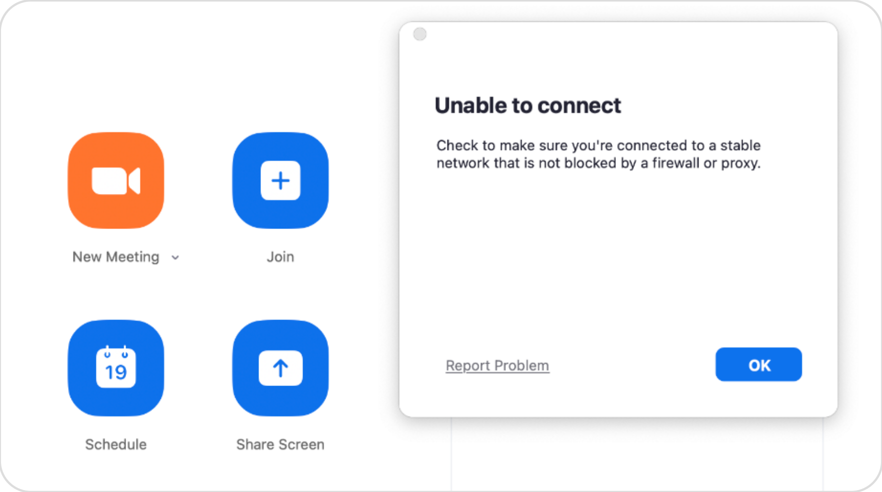
Scenario 1: Direct connect to SaaS applications

The most basic scenario is when an end user connects directly to SaaS applications from a remote location (home/hotel). The traffic routes to a home wireless router which forwards packets to an Internet Service Provider (ISP) and connects to the SaaS application. In this scenario, traffic is not secured, which leaves the end user vulnerable to attacks.


DIRECT
DEVICE MONITORING
END-POINT BASED NETWORK MONITORING
SAAS / WEB / APP MONITORING
salesforce
okta

Challenge: Network operations teams don't own the connectivity between the end user's device and SaaS applications, which makes it difficult to troubleshoot. Issues could reside with the Wi-Fi network or ISP, the end user's device, or the application.

For example, when an end user connects directly to SaaS applications (e.g., Zoom) and has issues, they may provide "Zoom is unable to connect" as their problem. The challenge is taking the information and diagnosing the root cause in a meaningful way. Support typically runs through a basic runbook since the issue could reside with the device, network, or application, which increases troubleshooting cycles and disrupts the end user's productivity, creating a poor user experience. When traffic is sent directly to the end application and IT does not have the proper monitoring solution, the end user's productivity and security suffer.



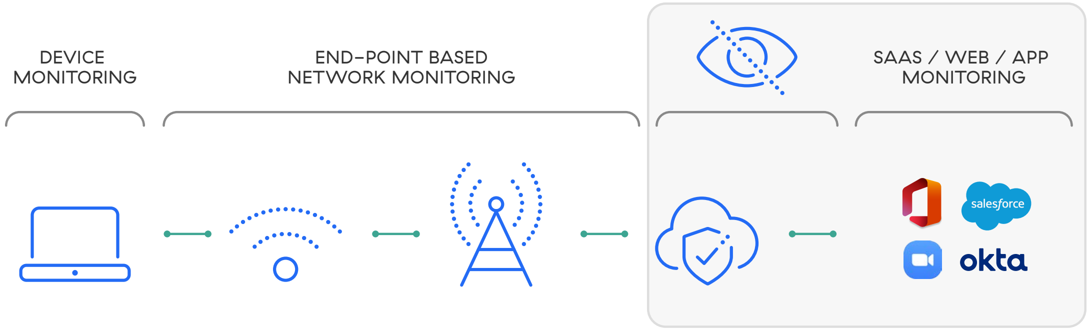
Unable to connect

Check to make sure you're connected to a stable network that is not blocked by a firewall or proxy.

Scenario 2: Secure SaaS applications

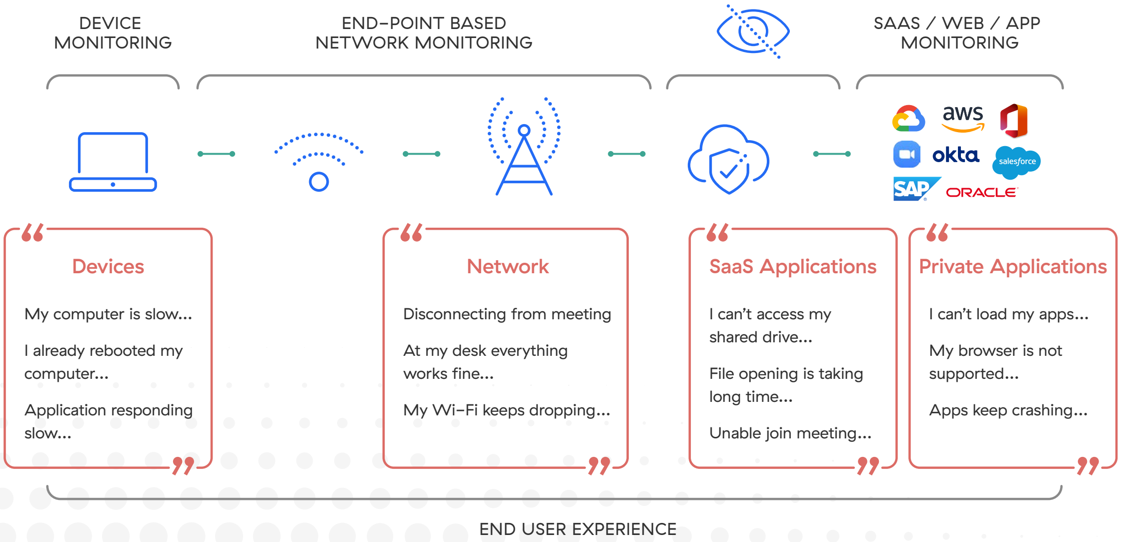
In the second scenario, the end user connects via their remote network (home/hotel), however, traffic is now forwarded to a security solution that inspects the traffic and connects to the SaaS application. As traffic is secured, the attack surface is limited, however, traditional monitoring solutions lack end-to-end visibility.

SECURE SAAS APPS


DEVICE MONITORING
END-POINT BASED NETWORK MONITORING
SAAS / WEB / APP MONITORING
salesforce
okta

Challenge: Network operations teams must utilize multiple tools to gain insights from end user devices, networks, SaaS applications, and security solutions. This lack of end-to-end visibility from a single pane of glass into digital experiences forces IT teams into reactive troubleshooting versus proactively identifying and resolving issues. Additionally, correlating data between monitoring tools is time consuming and increases mean time to resolution (MTTR).

For example, IT tickets are typically spread across devices, networks, and applications. The end user experience is a combination of all three segments working together. The challenge occurs when tickets are created, as there isn't enough data to quickly triage the problem. End users report anything from "my computer is slow" to "everything is working fine at my desk" to "I'm unable to join a meeting." The shift to cloud as the data center, the internet as the network, and securing communications only exacerbates the problem as IT visibility is limited.

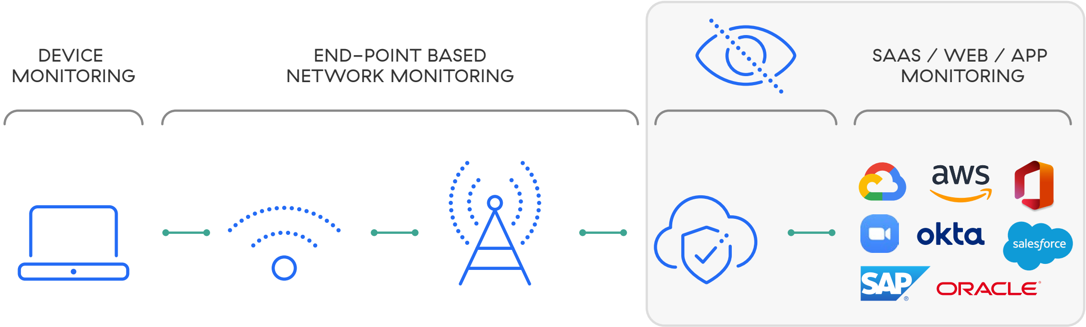

DEVICE MONITORING
END-POINT BASED NETWORK MONITORING
SAAS / WEB / APP MONITORING
aws
okta
salesforce
SAP
ORACLE
Devices
My computer is slow...
I already rebooted my computer...
Application responding slow...
Network
Disconnecting from meeting
At my desk everything works fine...
My Wi-Fi keeps dropping...
SaaS Applications
I can't access my shared drive...
File opening is taking long time...
Unable join meeting...
Private Applications
I can't load my apps...
My browser is not supported...
Apps keep crashing...
END USER EXPERIENCE

Increasing end user complexity causes poor user experience

Scenario 3: Secure SaaS and private applications

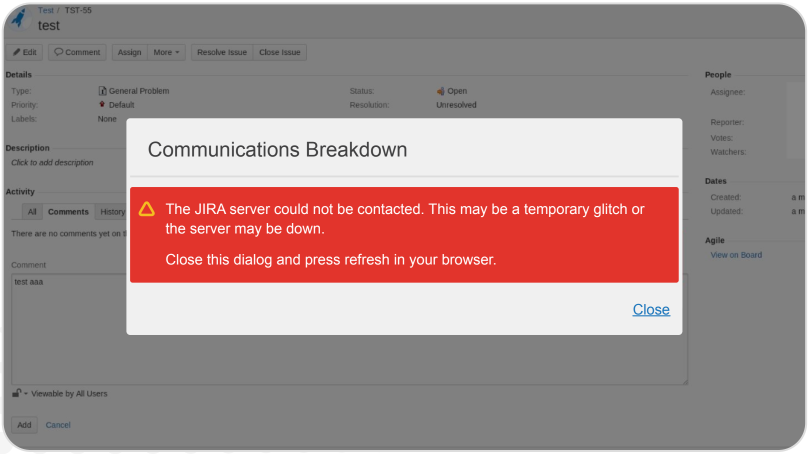
In this scenario, SaaS applications and private applications are both secured. Traffic from the end user device starts the same as the first two scenarios, but adds an additional route for private applications (hosted on-premises or in a public cloud). Again, as traffic is secured, the attack surface further is limited, and traditional monitoring solutions increase visibility gaps.

SECURE SAAS & PRIVATE APPS


DEVICE MONITORING
END-POINT BASED NETWORK MONITORING
SAAS / WEB / APP MONITORING
aws
okta
salesforce
SAP
ORACLE

Challenge: This scenario is complex when troubleshooting as network operations teams must diagnose several fragmented networks to piece together an end user's traffic to an application. This is time consuming, creates cumbersome processes, and requires network expertise to correlate data across multiple monitoring solutions. Additionally, as an end user's traffic is secured—limiting the attack surface—network operations teams tend to lose complete visibility as monitoring tools fail within secure environments, causing major blind spots for these teams. This seems to be the case any time traffic is sent over an encrypted network.

For example, an end user reports the following when trying to connect to a private application; "communication breakdown, Jira server could not be contacted." There are too many variables to diagnose the root cause from the error message. It could be the VPN network, application, or possibly the device. L1 support faces many such tickets, and there is no easy way to quickly diagnose the problem.



test

Details

Type: General Problem

Priority: Default

Labels: None

Status: Open

Resolution: Unresolved

Description

Click to add description

Activity

There are no comments yet on t

Comment

test aaa

Viewable by All Users

People

Assignee:

Reporter:

Votes:

Watchers:

Dates

Created: a m

Updated: a m

Agile

Communications Breakdown

The JIRA server could not be contacted. This may be a temporary glitch or the server may be down.

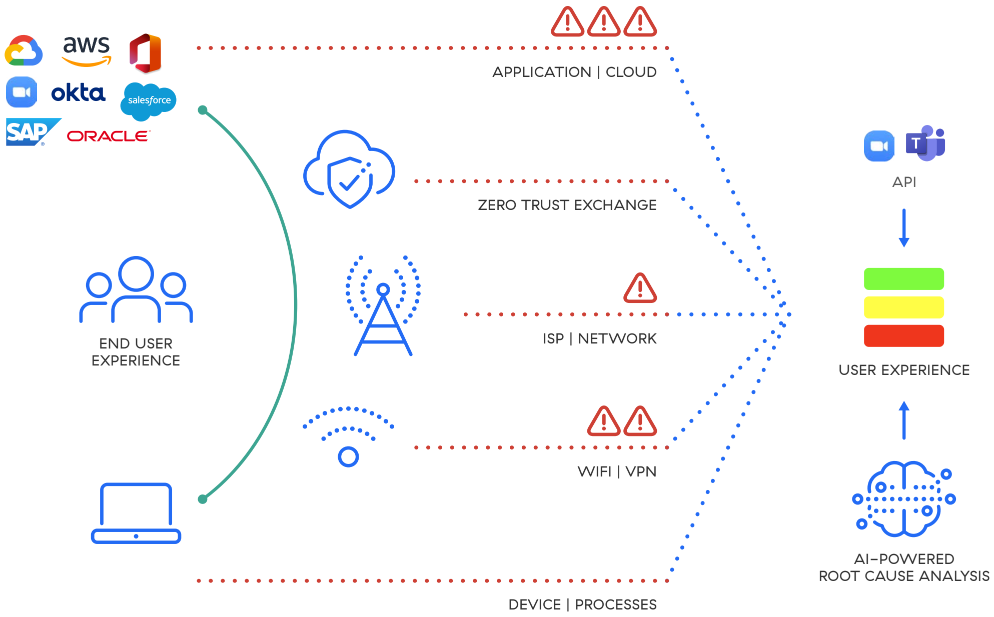
Close this dialog and press refresh in your browser.

End user faces private application (e.g., Jira) connectivity problems

Zscaler's end–to–end digital experience monitoring solution

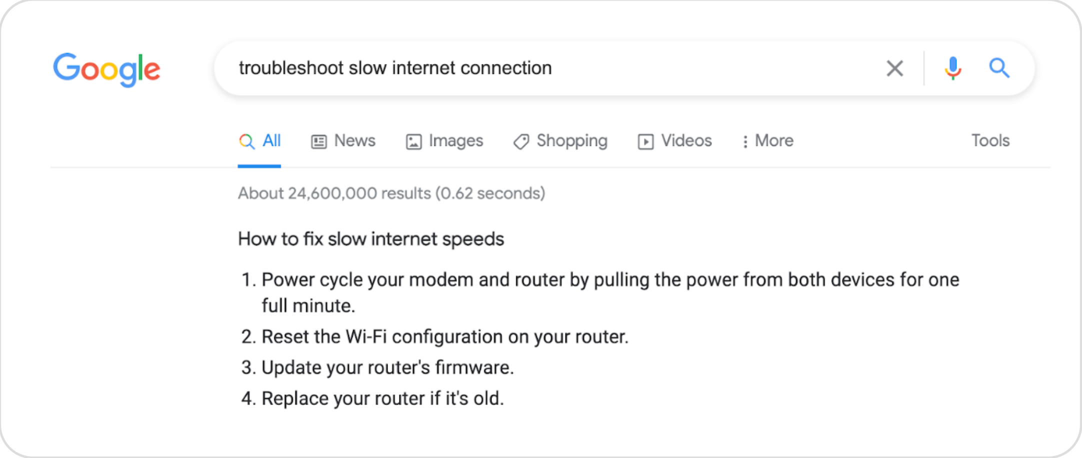
Digital transformation is a journey that requires a focus on end user experience. However, it is a balancing act between end user productivity and providing a secure environment to operate the business. Some monitoring and security solutions will push businesses to choose one or the other. With solutions available today, that should no longer be the case. Businesses should demand keeping their end users productive while providing security.

With Zscaler Digital Experience (ZDX), organizations can now fully monitor the cloud application experience from the end user perspective. ZDX restores visibility across the complete connection and quickly isolates user experience issues. ZDX delivers holistic, end–to–end user experience monitoring across any network, helping network operation teams streamline troubleshooting and improve user productivity across secure environments.



Eliminate monitoring silos with Zscaler's Digital Experience

For example, network operations teams need quick insight into potential areas of focus, so triaging issues is fast and painless. Many times the remote worker's issue tends to be within their local environment, but it doesn't mean it's an issue at their physical location. Have you ever tried to Google "troubleshoot slow internet connection?" The results point to the home router. However, that doesn't provide a holistic view of the situation.



About 24,600,000 results (0.62 seconds)

How to fix slow internet speeds

1. Power cycle your modem and router by pulling the power from both devices for one full minute.
2. Reset the Wi-Fi configuration on your router.
3. Update your router's firmware.
4. Replace your router if it's old.

Not all search responses yield the correct course of action

ZDX not only provides insights into end user environments, it also extends that into the Zscaler Zero Trust Exchange, the platform on which all Zscaler services are built. With ZDX, network operations teams get insights into Zscaler Internet Access (ZIA), which secures traffic to SaaS applications and optimizes network efficiencies. ZDX also supports Zscaler's Private Access (ZPA), which protects private application traffic.

Network operations teams benefit from a centralized dashboard with all relevant telemetry data to troubleshoot and resolve user experience issues with both public and private applications. As you embark on your digital transformation journey to a secure world, consider how you plan to ensure a great end user experience.

Learn more about ZDX here

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.