

Zscaler Business Update

05. März 2024



What is Zscaler doing & where are we heading?

Kevin Schwarz

CTO EMEA & APJ

March 2024

Safe harbor forward-looking statements

This presentation has been prepared by Zscaler, Inc. ("Zscaler") for informational purposes only and not for any other purpose. Nothing contained in this presentation is, or should be construed as, a recommendation, promise or representation by the presenter or Zscaler or any officer, director, employee, agent or advisor of Zscaler. This presentation does not purport to be all-inclusive or to contain all of the information you may desire.

This presentation contains forward-looking statements. All statements other than statements of historical fact, including statements regarding our planned products and upgrades, business strategy and plans and objectives of management for future operations of Zscaler are forward-looking statements. These statements involve known and a significant number of unknown risks, uncertainties, assumptions and other factors that could cause results to differ materially from statements made in this message, including any performance or achievements expressed or implied by the forward-looking statements. Moreover, we operate in a very competitive and rapidly changing environment, and new risks may emerge from time to time. It is not possible for us to predict all risks, nor can we assess the impact of all factors on our business or the extent to which any factor, or combination of factors, may cause actual results or outcomes to differ materially from those contained in any forward-looking statements we may make. Additional risks and uncertainties that could affect our financial and operating results are included in our most recent filings with the Securities and Exchange Commission. You can locate these reports through our website at <http://ir.zscaler.com> or on the SEC website at www.sec.gov.

In some cases, you can identify forward-looking statements by terms such as "anticipate," "believe," "continue," "contemplate," "could," "estimate," "expect," "explore," "intend," "likely," "may," "plan," "potential," "predict," "project," "should," "target," "will" or "would" or the negative of these terms or other similar words. Zscaler based these forward-looking statements largely on its current expectations and projections about future events that it believes may affect its business. Actual outcomes and results may differ materially from those contemplated by these forward-looking statements. All forward-looking statements in this message are based on information available to us as of the date hereof, and we do not assume any obligation to update the forward-looking statements provided to reflect events that occur or circumstances that exist after the date on which they were made.



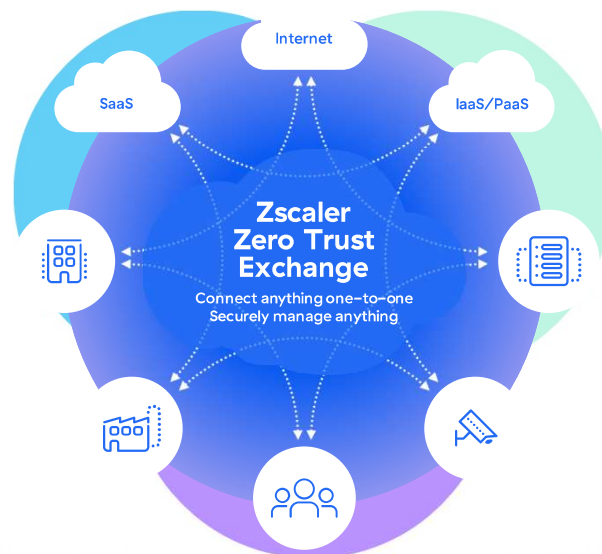
Zscaler Business Update

05. März 2024



Empowering your business to be more
secure, **simple**, and **productive**.

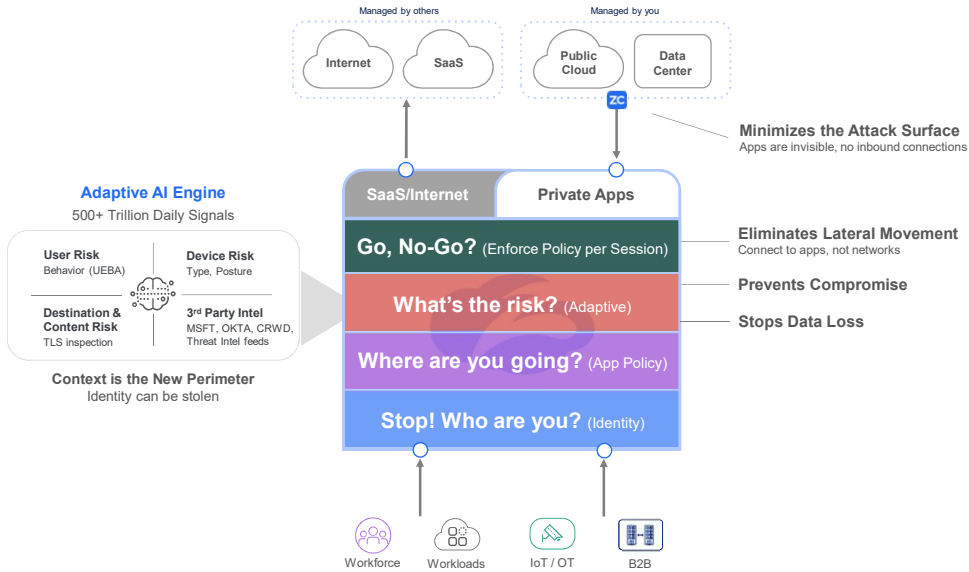
Zero Trust Exchange



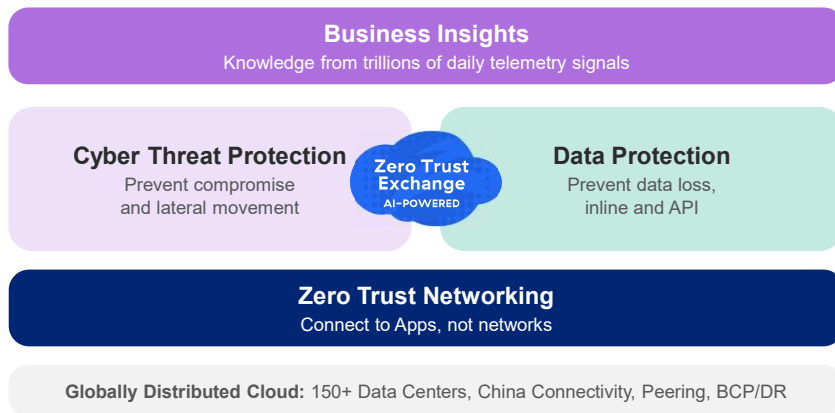
Zscaler Business Update

05. März 2024

A New Architecture is the Answer: Zero Trust Exchange



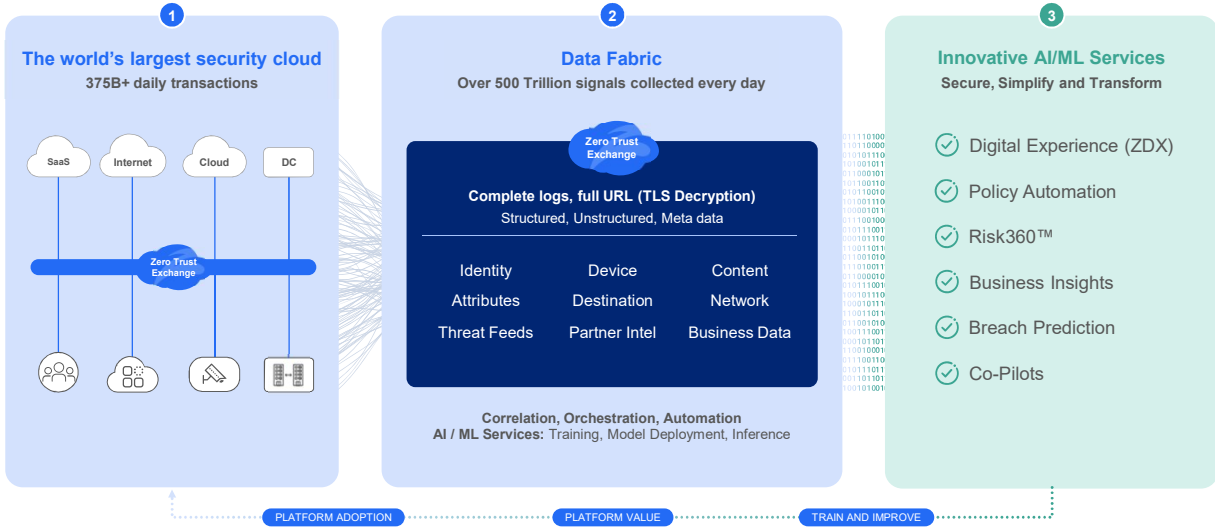
Comprehensive Solutions Across Four Key Areas



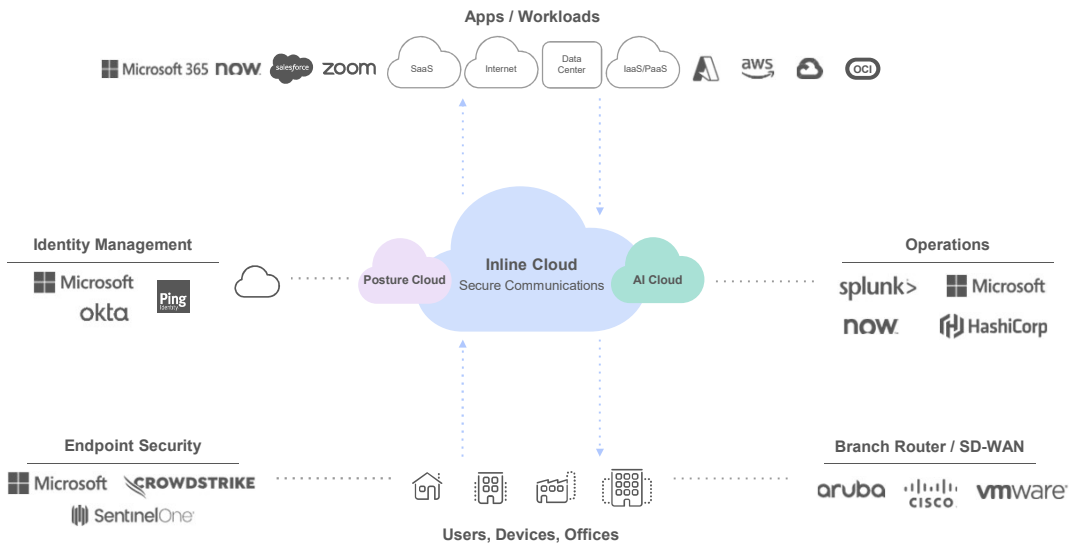
Zscaler Business Update

05. März 2024

Zscaler Leadership and Advantage in AI

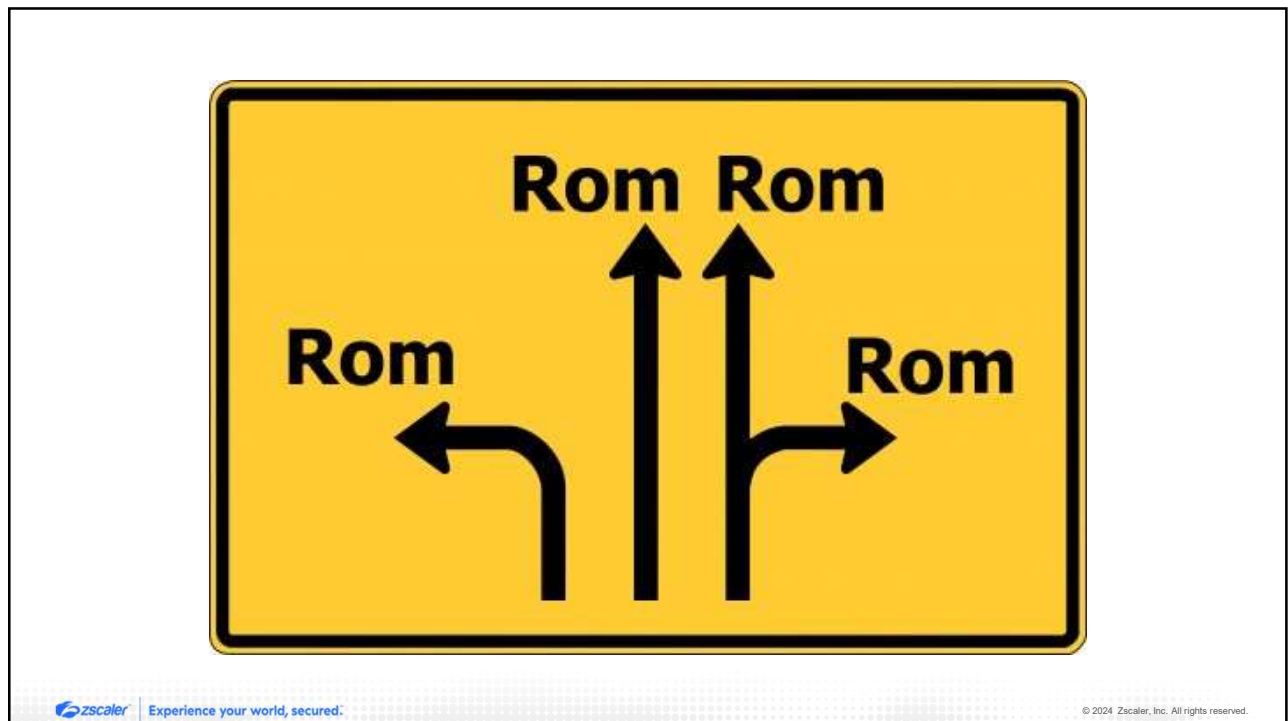
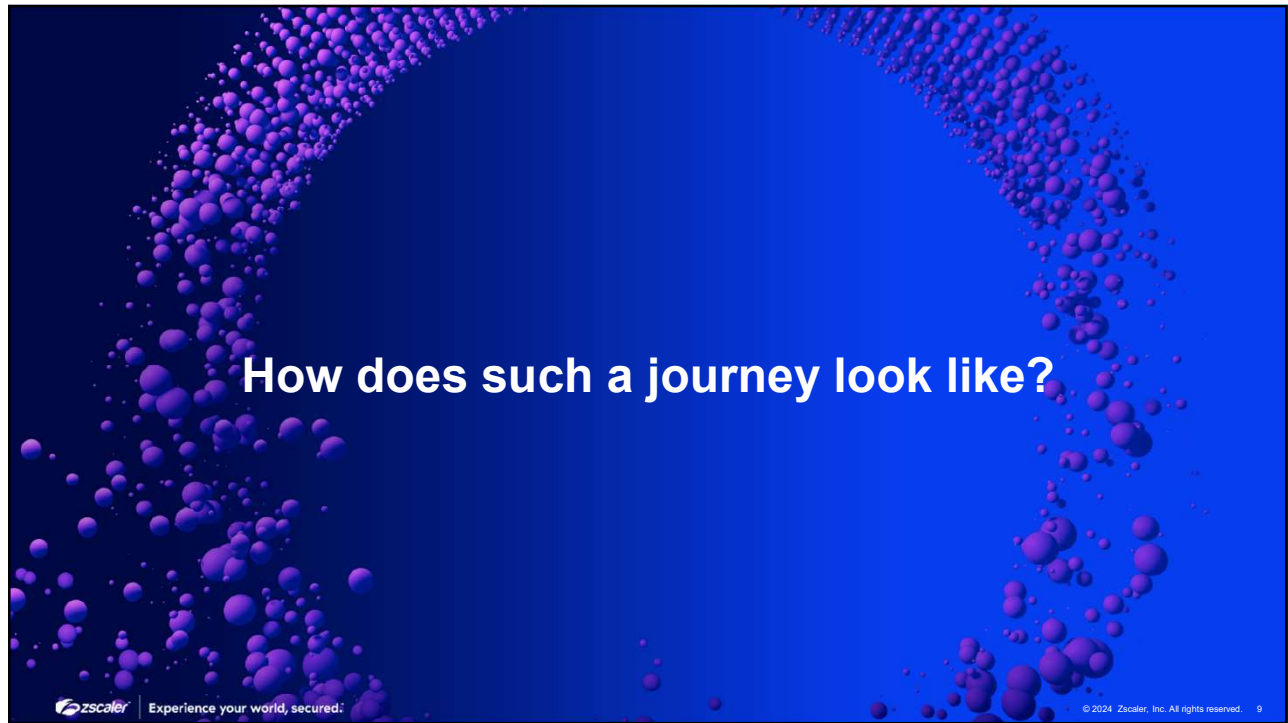


Best of Breed Platforms to Implement Zero Trust



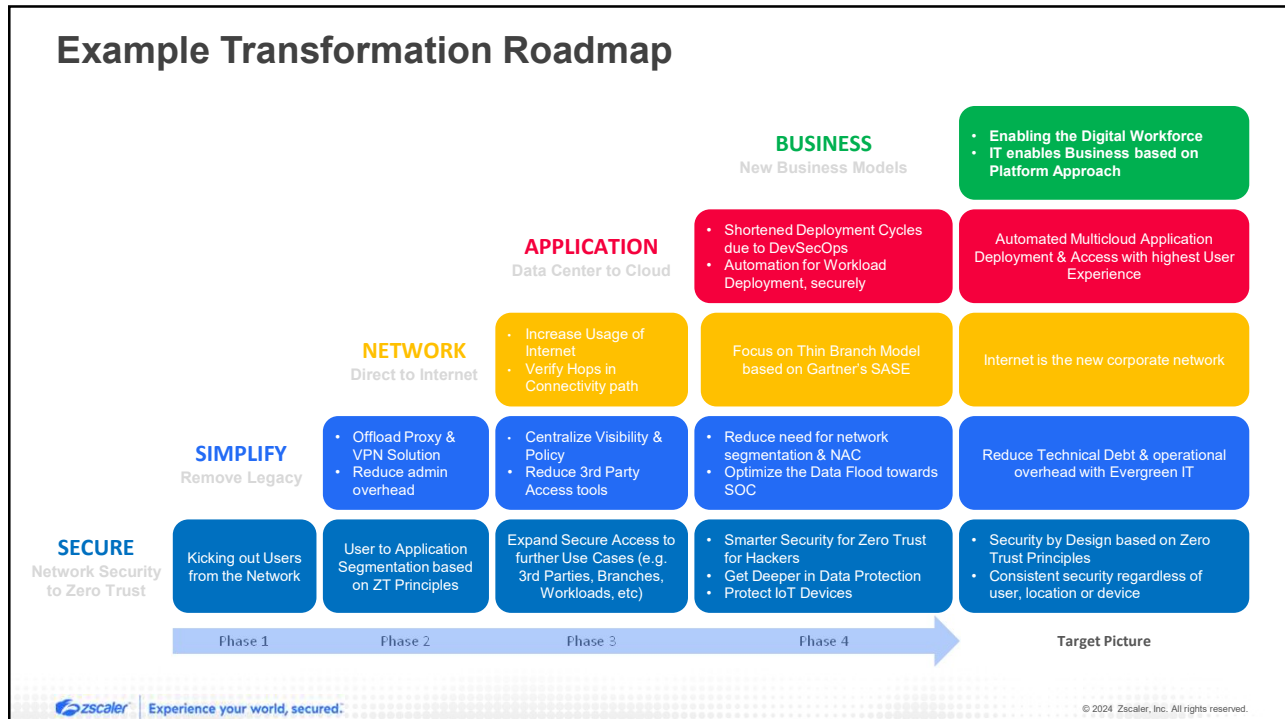
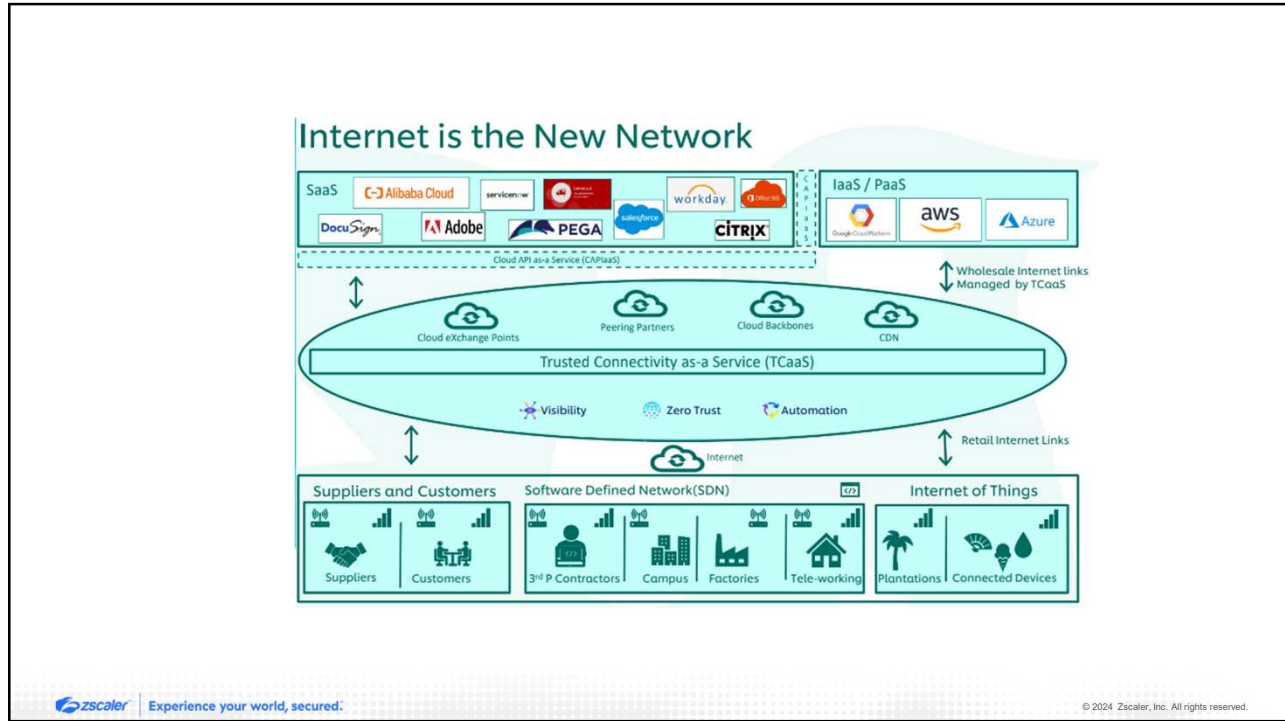
Zscaler Business Update

05. März 2024



Zscaler Business Update

05. März 2024



Zscaler Business Update

05. März 2024

Secure Communications

Business Analytics
Knowledge from trillions of daily telemetry signals


Cyber Threat Protection
Prevent compromise and lateral movement

Zero Trust Exchange


Data Protection
Prevent data loss, inline and API

Zero Trust Connectivity
Workforce, Third Parties, Customers, Branches, Factories, Public Clouds, Data Centers


Globally Distributed Cloud: 150+ Data Centers, China Connectivity, Peering, BCP/DR




Zscaler for Users




Zscaler for Workloads



Zscaler for B2B



Zscaler for IoT / OT

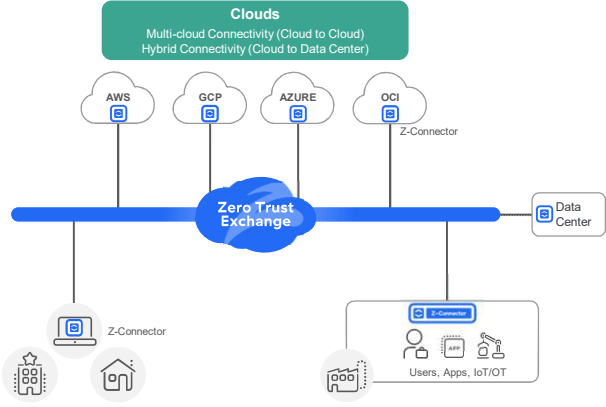


Experience your world, secured.

© 2024 Zscaler, Inc. All rights reserved.

Zero Trust Connectivity for Users, Cloud, and Branches

Clouds
Multi-cloud Connectivity (Cloud to Cloud)
Hybrid Connectivity (Cloud to Data Center)




Users
Workforce / B2B Customers & Suppliers
Remote Access to Cloud and DC Apps

Locations
Branches, Factories
Branch to DC, Branch to Cloud Connectivity

Zero Trust Connectivity

- Eliminates Lateral Movement**
 - Connectivity is a non-routable network overlay
- Reduces Operational Complexity and Cost**
 - Eliminates DC / Cloud DMZs, site-to-site VPNs
- Secures all Communications**
 - AI-powered cyber threat and data protection
- Delivers a Great Experience**
 - Device to app digital experience, users today



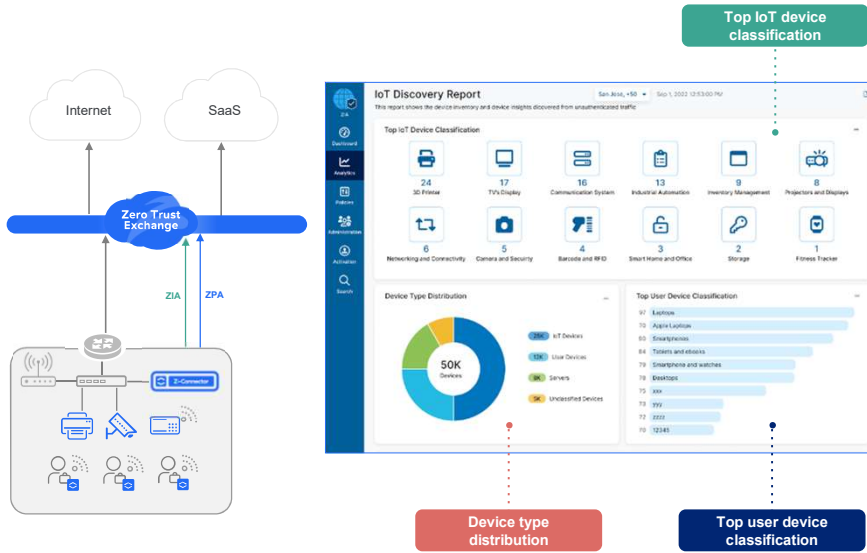
Experience your world, secured.

© 2024 Zscaler, Inc. All rights reserved.

Zscaler Business Update

05. März 2024

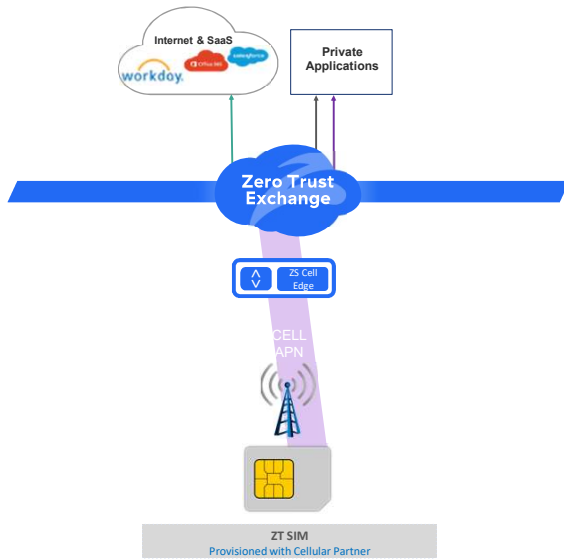
Use Cases: IoT device discovery and classification



Benefits

- ✓ Agentless visibility and insights into IoT devices at branch
- ✓ Automatic device classification based on traffic profiles
- ✓ Policy controls for IoT traffic* (roadmap)

We thought a bit different about IoT Security...



Business risk - decreased by

- Having granular control & visibility on SIM Card level independent of location
- Leverage the power of the Zero Trust Exchange for protection against data loss, security threats, etc.

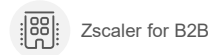
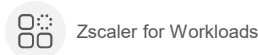
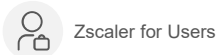
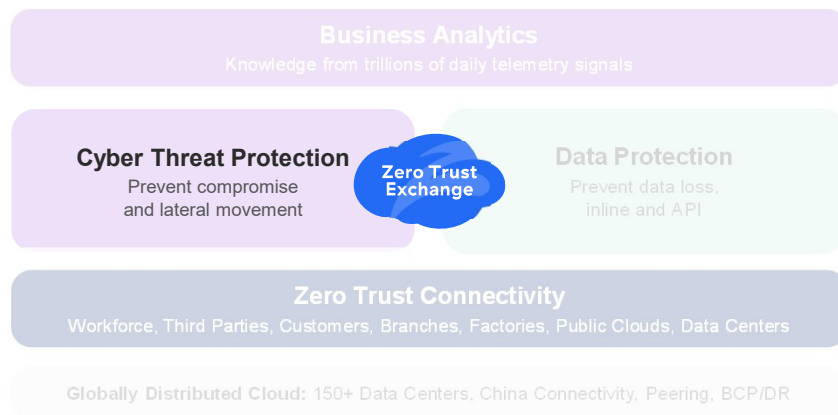
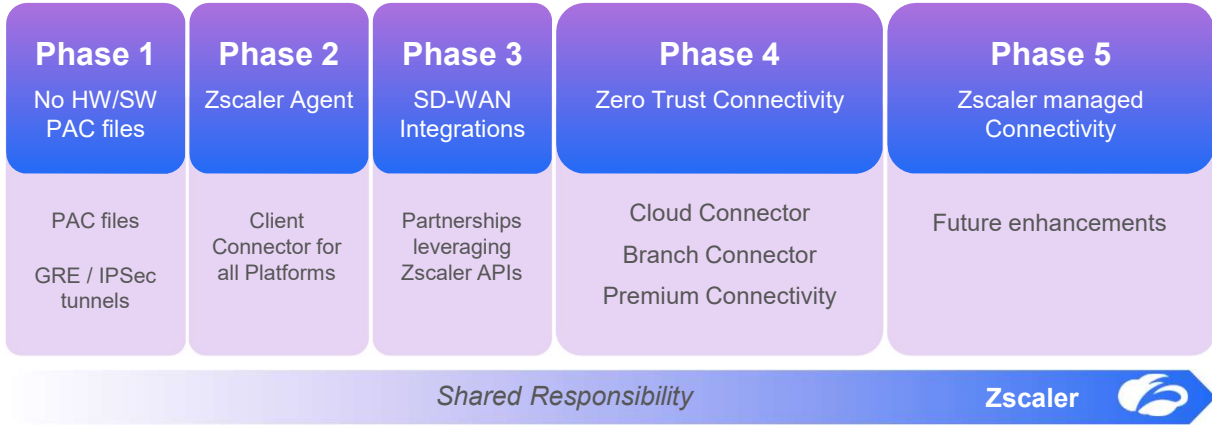
Cost & complexity - decreased by

- Instant deployment possibility
- No additional hardware required
- Utilizing existing Security environment to avoid split between OT & IT departments
- Having possibility to access Devices remotely for maintenance scenarios
- Avoiding unnecessary dispatching of Remote Engineers

Zscaler Business Update

05. März 2024

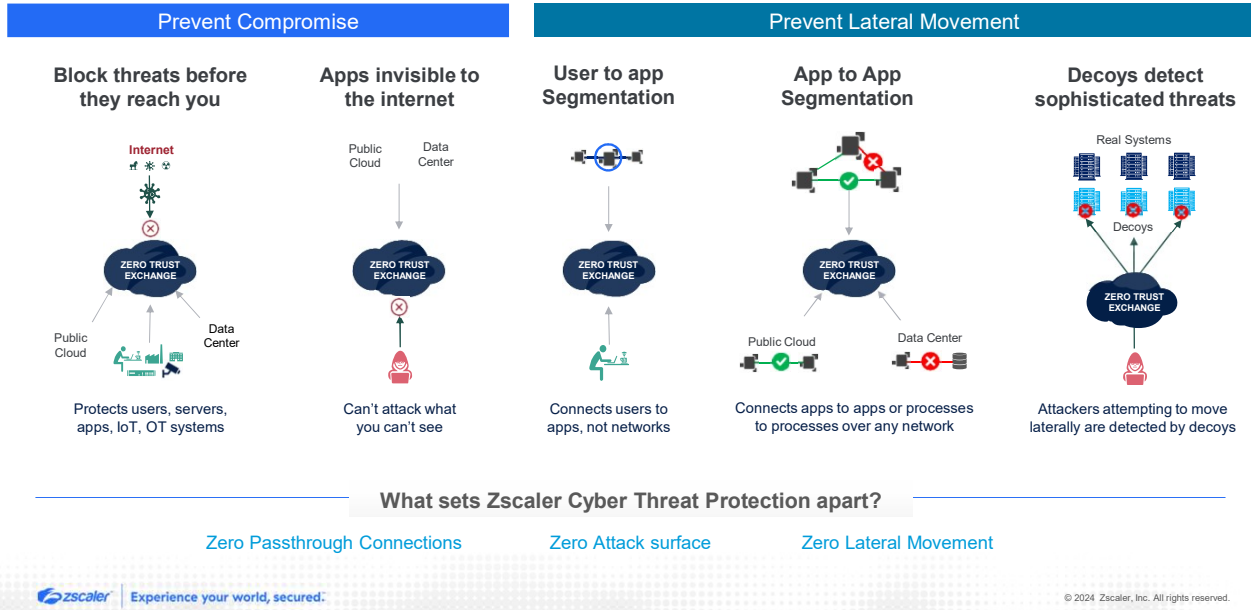
The Evolution of Zscaler's Connectivity Stack



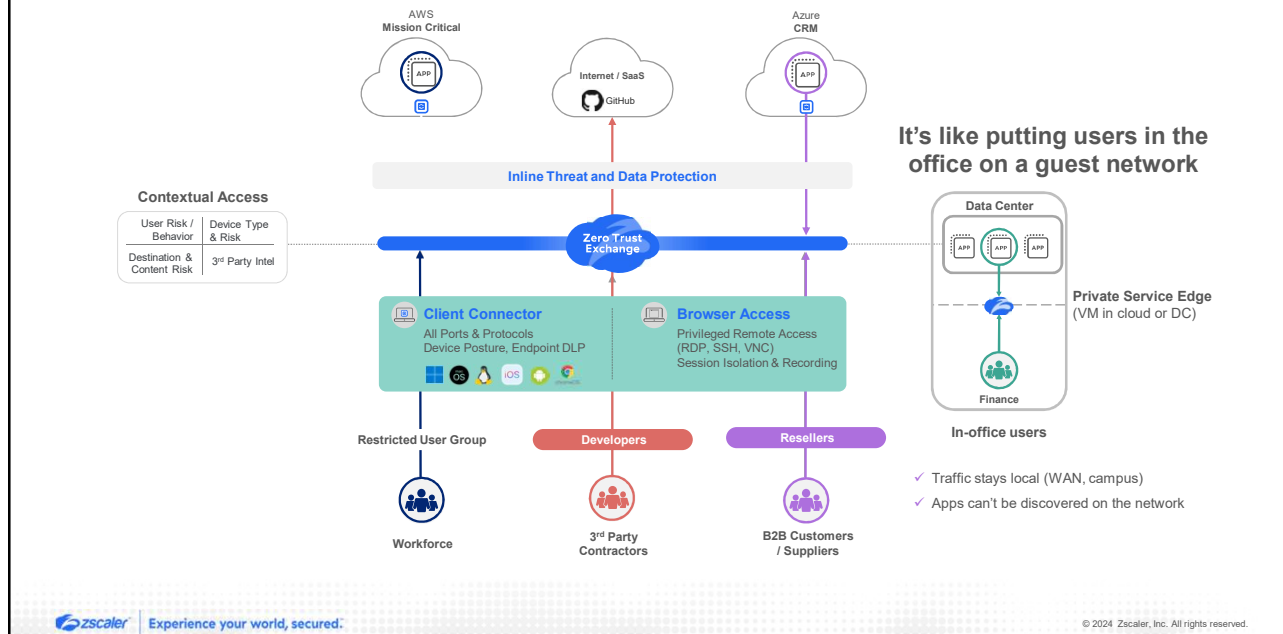
Zscaler Business Update

05. März 2024

Zero Trust Security: Cyber Threat Protection



Zero Trust Connectivity for Users



Zscaler Business Update

05. März 2024

Most organizations face one or more of these challenges...

Don't have comprehensive application inventory

Don't know all the application owners

Don't know who needs access to what

Hard to maintain granular policy

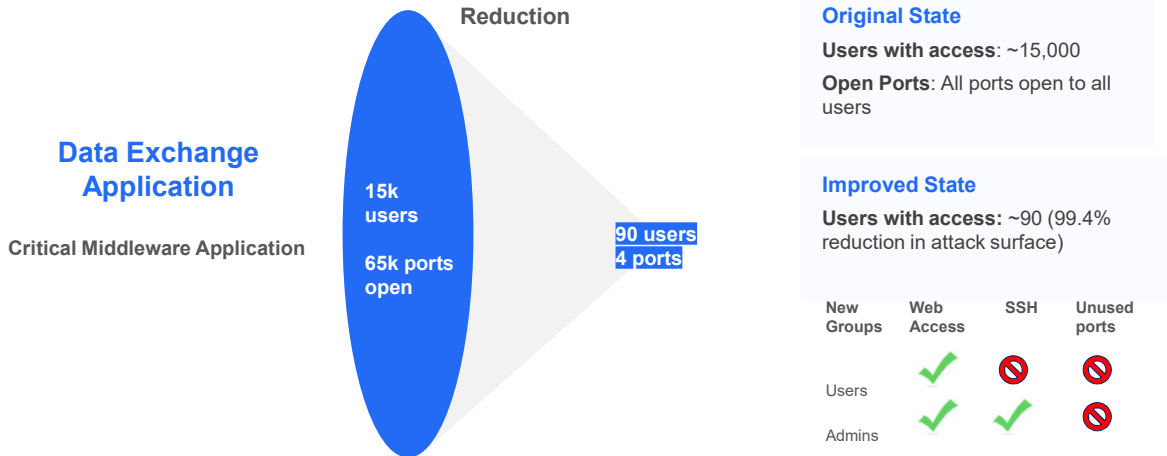
I need an Army!



Intelligent Policy reduced attack surface by 99%

Reduced over-privileged access from 15,000 users → ~90 users

99.4% Attack Surface Reduction

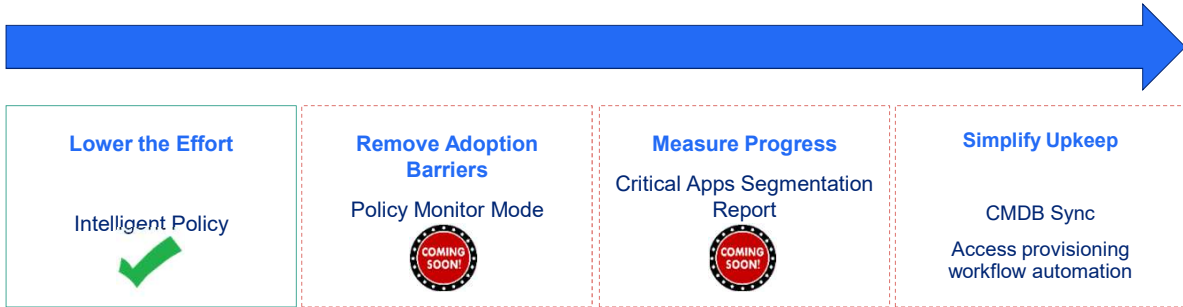


Zscaler Business Update

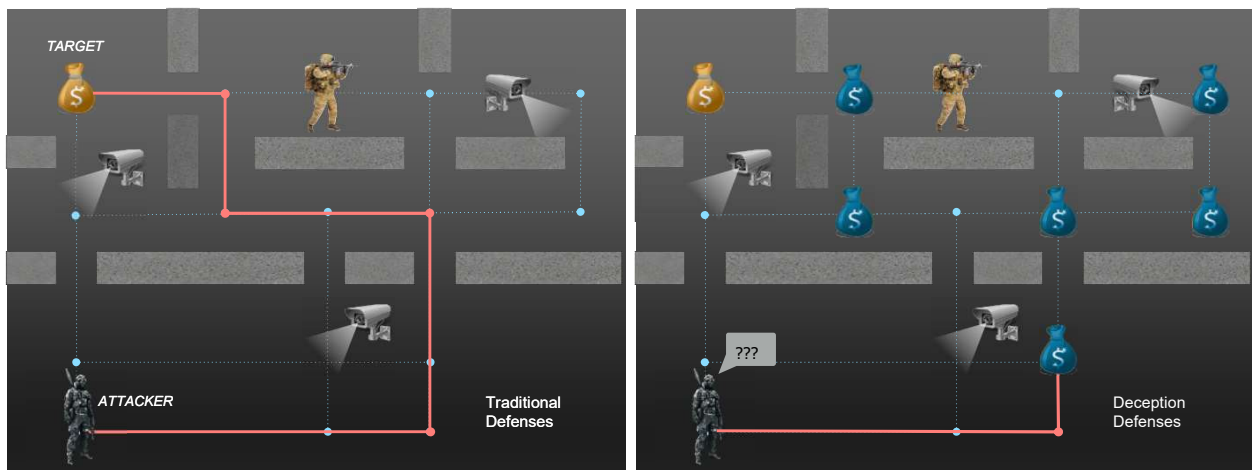
05. März 2024

Continuing to simplify segmentation with ZPA

Four-phased approach to simplifying Segmentation



Deception disrupts advanced attacks

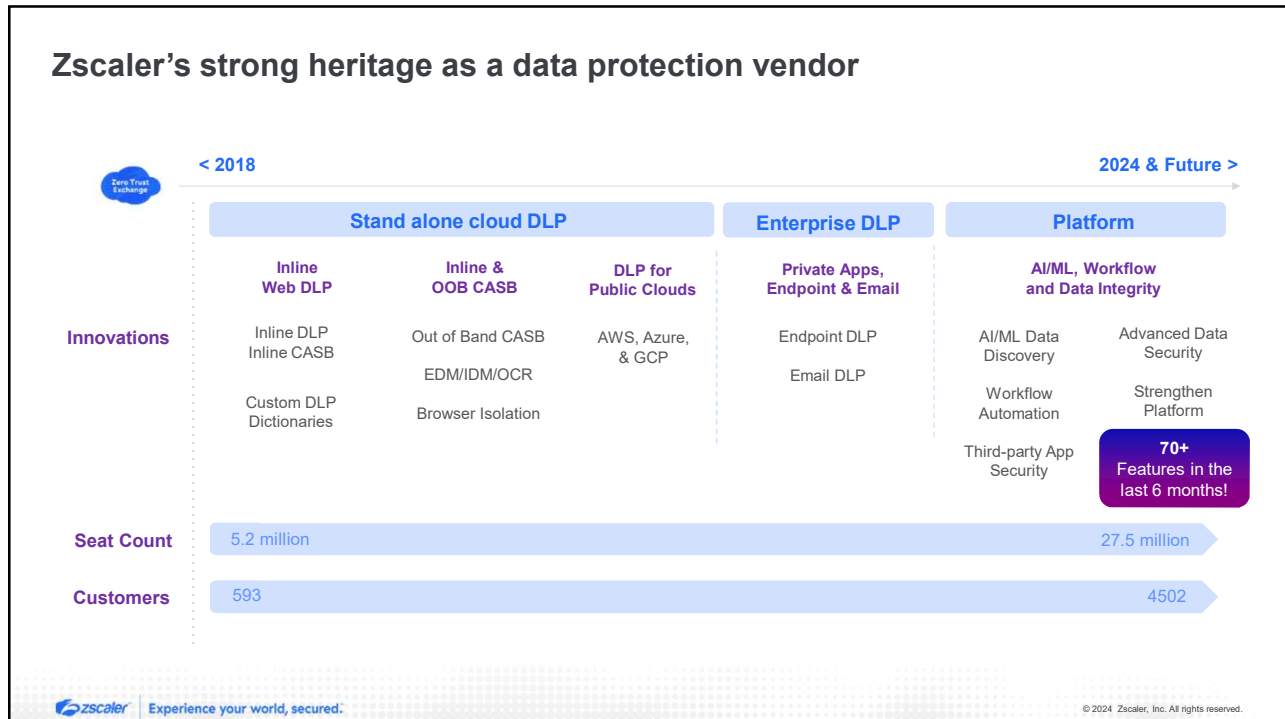
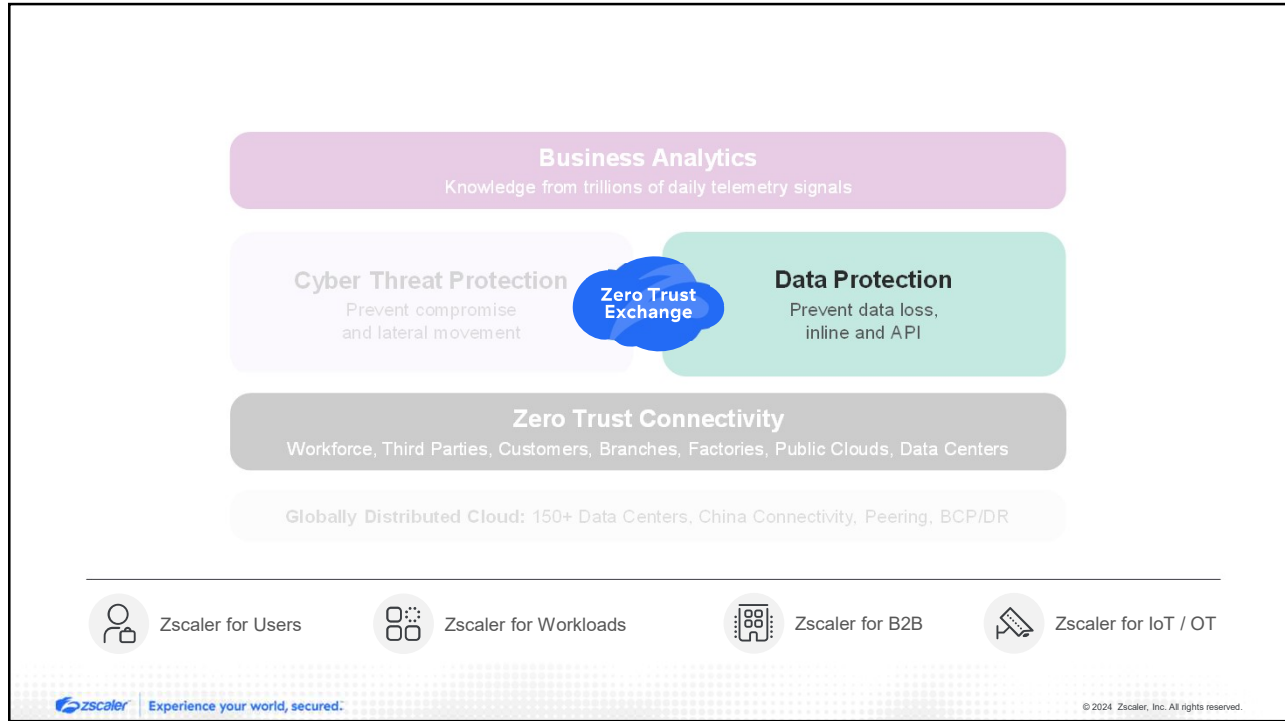


Attackers know your strategy. Predictable defenses are easily bypassed

Decoys and traps make your environment unpredictable, disrupt attacker playbooks

Zscaler Business Update

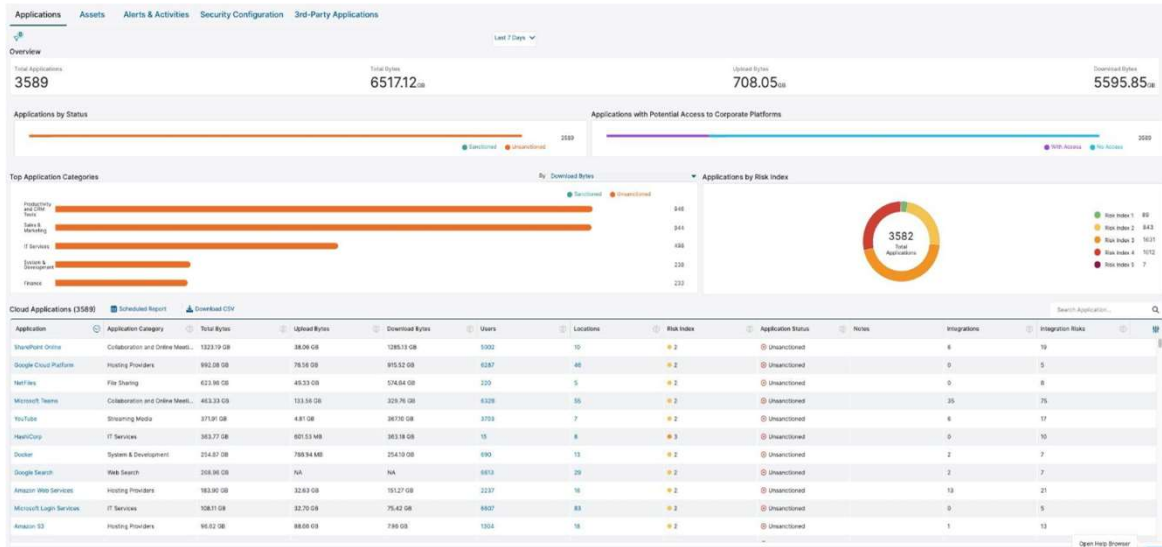
05. März 2024



Zscaler Business Update

05. März 2024

SaaS Security Report



Auto classification & data discovery powered by AI/ML

Problem

Help IT staff who aren't experts

- No Rules, regex or complicated policies
- No end user markup or classification

Solution

Find and secure sensitive content

- Deep learning engine
- Over 90 Thematic Data Categories
- Customer defined categories
- Supervised learning model
- NLP, TF/ITF, document clustering
- Vector learning



Zscaler Business Update

05. März 2024

Business Analytics

Knowledge from trillions of daily telemetry signals

Cyber Threat Protection

Prevent compromise and lateral movement

Zero Trust Exchange


Data Protection

Prevent data loss, inline and API


Zero Trust Connectivity

Workforce, Third Parties, Customers, Branches, Factories, Public Clouds, Data Centers


Globally Distributed Cloud: 150+ Data Centers, China Connectivity, Peering, BCP/DR




Zscaler for Users




Zscaler for Workloads



Zscaler for B2B



Zscaler for IoT / OT



Experience your world, secured.

© 2024 Zscaler, Inc. All rights reserved.

Business Analytics


Digital Experience

End-to-end visibility

Apps
Performance, availability, and uptime

Network
Hop-by-hop performance

Endpoint
Device and Connectivity Health



Experience Score

25 BAD

75 OKAY

100 GOOD

Proactively resolve performance issues

Business Insights

App Insights
Visibility into app landscape, usage, & spend

Salesforce

Save **\$150,000/year** by removing 150 inactive users (last 90 days)

Location Insights
Visibility into where employees are working for office space optimization

San Jose, CA 2873 employees

- In Office 875
- Remote 1,123
- Hybrid 345

[View Details](#)

Workforce Insights
Discover how employees and departments are collaborating. Process optimization.


HR Finance

- Messaging 1394 messages
- Meetings 98minutes
- Email 42 emails s

[View Details](#)

Risk360

Holistic view of company-wide risk



Critical

External Attack Surface

Low Medium High Critical

Compromise

Low Medium High Critical


Lateral Propagation

Low Medium High Critical

Data Loss

Low Medium High Critical

Discover ways to remediate risk
Peer Comparisons



Experience your world, secured.

© 2024 Zscaler, Inc. All rights reserved. 30

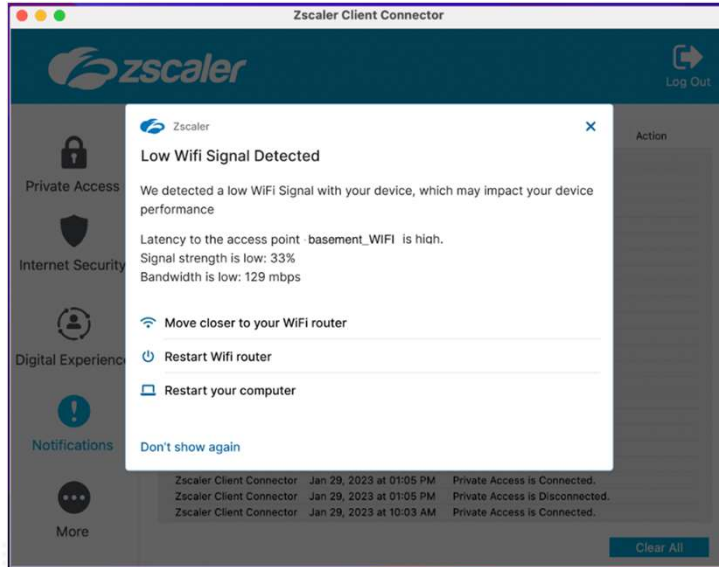
Zscaler Business Update

05. März 2024

Self Service IT

Helping user remediate on the fly

Detect exactly when problems happen



Last but not least, some cool
Events coming up!

Zscaler Business Update

05. März 2024



CXO
EXCHANGE

26-27 MARCH 2024

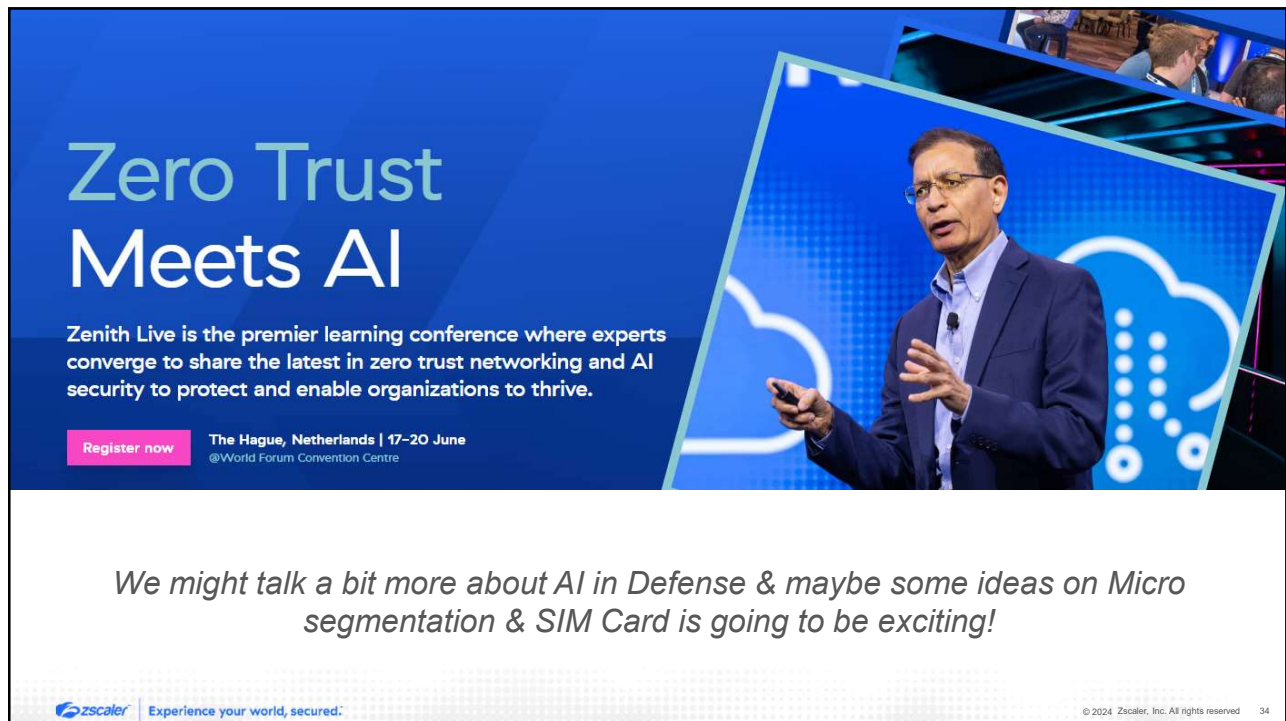
🌐 EMEA | AMSTERDAM
THE NETHERLANDS

CXO REvolutionaries

SPONSORED BY: 

 Experience your world, secured.

© 2024 Zscaler, Inc. All rights reserved 33




Zero Trust Meets AI

Zenith Live is the premier learning conference where experts converge to share the latest in zero trust networking and AI security to protect and enable organizations to thrive.

[Register now](#) The Hague, Netherlands | 17-20 June
@World Forum Convention Centre

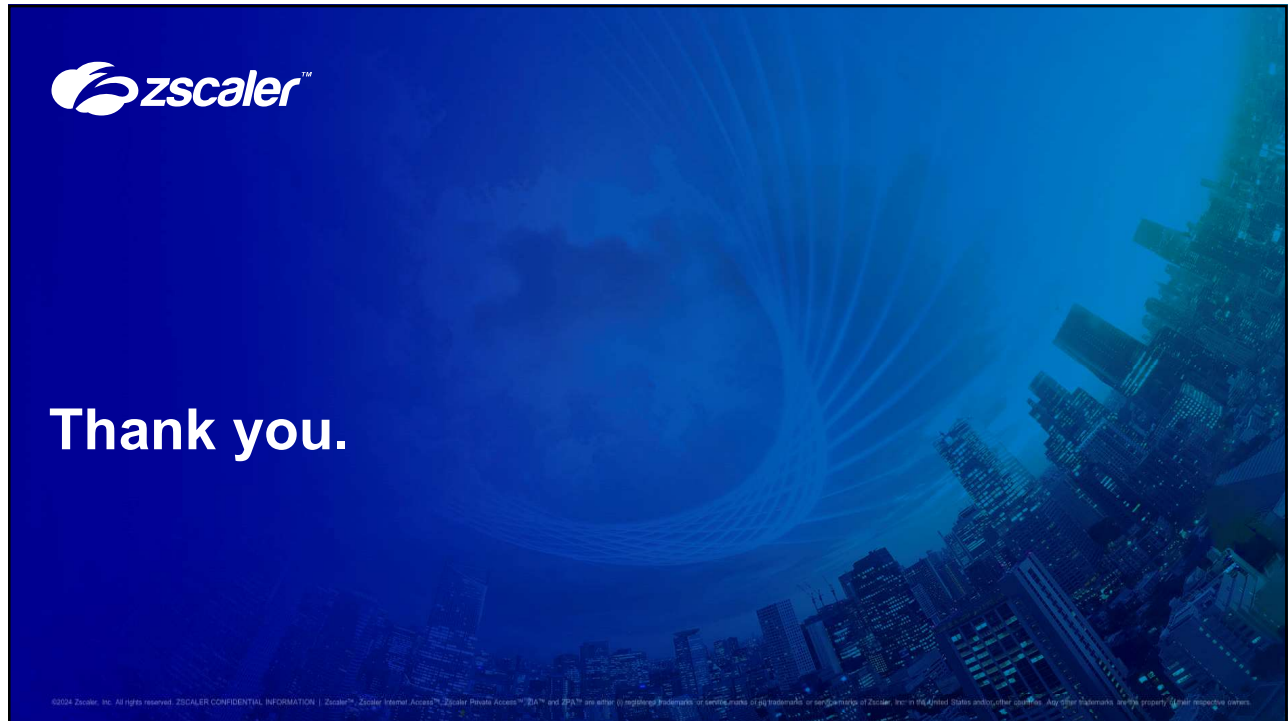
We might talk a bit more about AI in Defense & maybe some ideas on Micro segmentation & SIM Card is going to be exciting!

 Experience your world, secured.

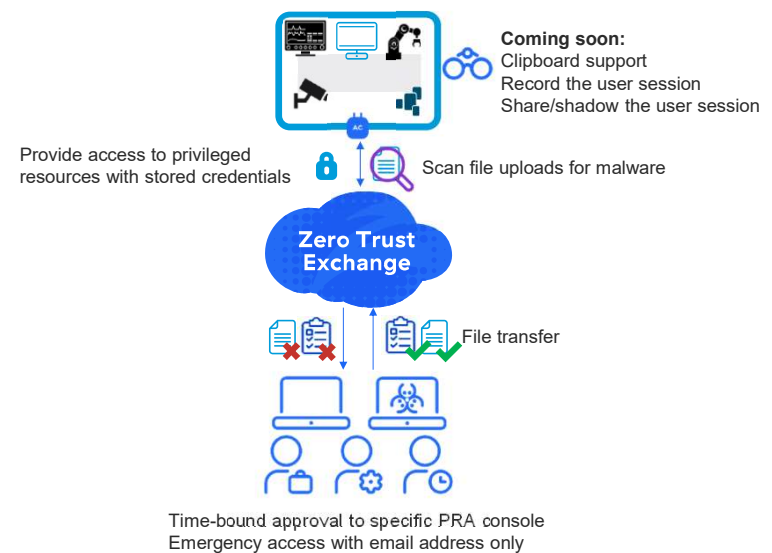
© 2024 Zscaler, Inc. All rights reserved 34

Zscaler Business Update

05. März 2024



Eliminate lateral movement risk from 3rd party users with privileged remote access



Zscaler Business Update

05. März 2024

Session Recording & Playback

Problem	Risks from privileged users are constant especially in business-critical systems like OT. Audit logs provide information about who is accessing which assets and when, but not information about what is being done in the session. It is difficult to undo or recover without the session details.
Solution	Privileged Remote Access allows organizations to monitor, record and playback the activities of users within critical systems.
Benefits	<ul style="list-style-type: none"> • Improved Incident Response - Capture forensics data to troubleshoot issues related to user activity, and utilize data to investigate and respond to incidents. • Compliance - Comply with regulatory requirements by providing a record of user activity that can be used for auditing and compliance reporting purposes. • Reduced Risk - provide visibility into actions of privileged users and suspicious activity.

The screenshot shows the 'PRIVILEGED CAPABILITIES' settings interface. The 'Record Sessions' option is highlighted with a red box and is currently set to 'Enable'. Below this, there is a 'Recordings' section with a summary card showing 'Total 31' recordings. A table lists individual recordings with columns for Connection, Recording Duration, Policy, User, Console, Console Type, and Actions. One recording entry is highlighted with a red box in the Actions column.

Connection	Recording Duration	Policy	User	Console	Console Type	Actions
Jun 2nd, 2023, 14:4...	9 minutes 13 seconds	Privileged Policy	manesh@shahu.haus	engg-workstation	RDP	▶ ⬇
Jun 2nd, 2023, 14:3...	1 minute 3 seconds	Privileged Policy	manesh@shahu.haus	engg-workstation	RDP	▶ ⬇
Jun 2nd, 2023, 14:2...	8 seconds	Privileged Policy	manesh@shahu.haus	engg-workstation	RDP	▶ ⬇
Jun 2nd, 2023, 14:2...	1 minute 5 seconds	Privileged Policy	manesh@shahu.haus	engg-workstation	RDP	▶ ⬇
May 30th, 2023, 14...	23 seconds	Privileged Policy	manesh@shahu.haus	ot-hmi	VNC	▶ ⬇

Experience your world, secured.

© 2024 Zscaler, Inc. All rights reserved.

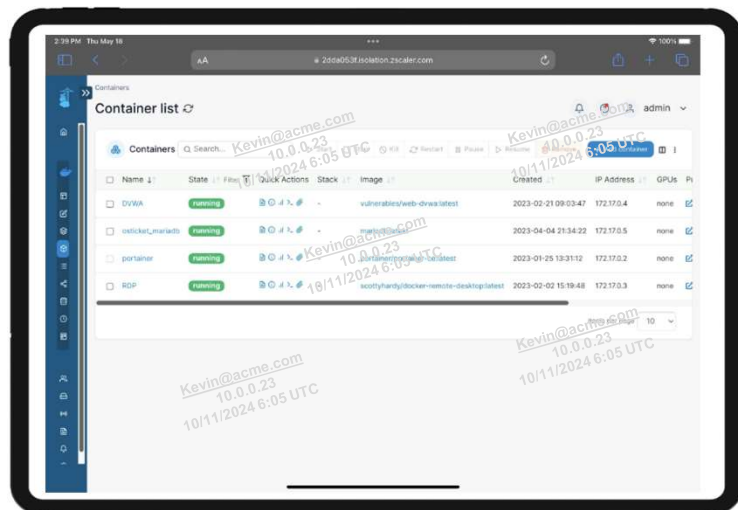
Browser isolation for private apps

Watermarking for security

Prevent and trace data theft with a watermark
Adds username and timestamp to the screen

Mobile device support

Support mobile form factors
Enable touchscreens & on-screen keyboards



Zscaler Business Update

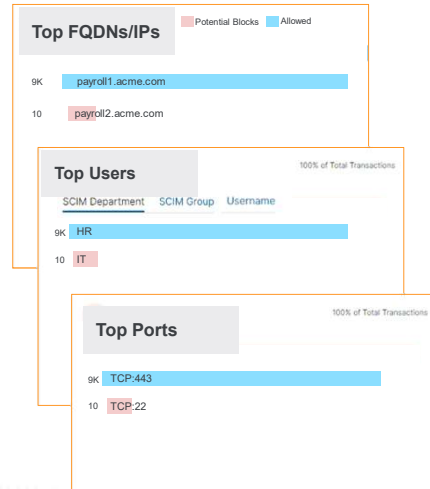
05. März 2024

Policy Monitoring: Eliminate Operational Risk

Test new policies before implementation

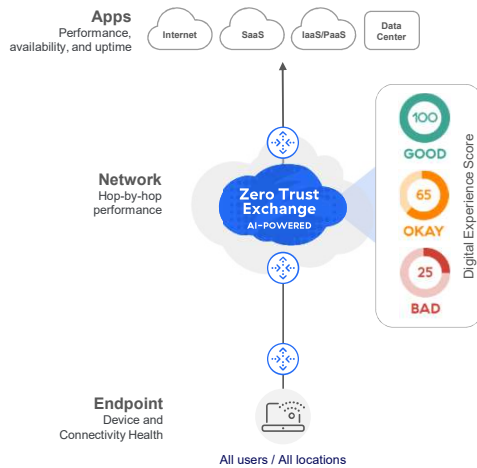
Execute Policy Test

Rule Order	Name
> 1	badr530
> 2	badr28
> 3	badr243
> 4	badr246
> 5	badr249
> 6	badr258



Proactively identify and resolve performance issues (ZDX)

Visibility from Endpoint to App
Troubleshoot and resolve device, network and apps issues



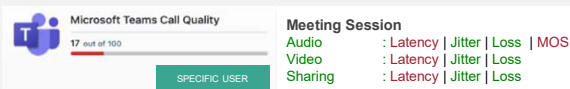
Full view of every step of the traffic path



Device Health
CPU | Memory | Disk I/O
N/W I/O | Bandwidth | Processes

High latency between
Hotel gateway and ISP

Quickly identify Zoom and Teams performance issues



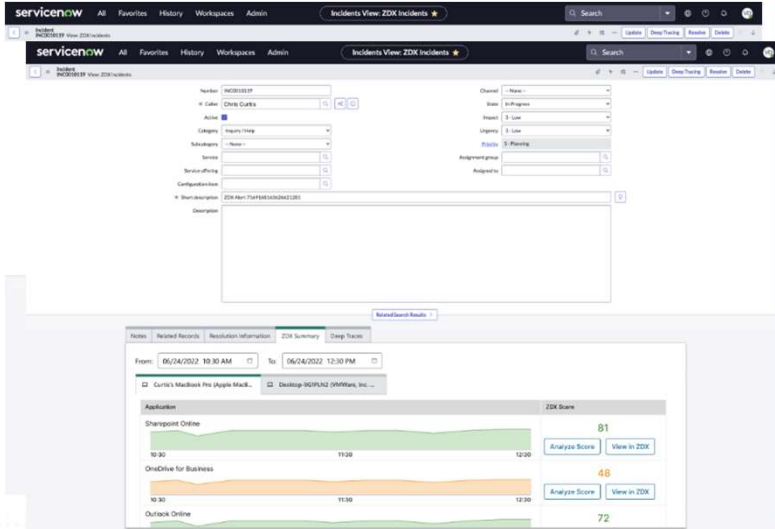
Unify monitoring silos for great visibility to quickly troubleshoot performance issues

Zscaler Business Update

05. März 2024

ServiceNow Integration using ZDX API

Access User's application performance for contextual information



Deeper integration using ZDX API to give contextual information:

- Applications specific contextual data for individual users incident to help troubleshoot.
- Ability to run Automated Root Cause Analysis to identify issues.
- Ability to pull contextual data on Alerts once an incident is created in ServiceNow using Alert webhooks.

Zscaler Risk360™: Company-wide Risk Quantification and Visualization

- 1 Understand your Security Control Posture
- 2 Assess reconnaissance activity in your environment and on the Internet
- 3 Leverage ThreatLabz threat intelligence
- 4 Gain insights from real data in your environment + external feeds



Understand the top cyber risk drivers

Actionable insights with guided workflows

Risk events by location & user

Risk score trend & peer comparison

Board-ready CISO slides

Zscaler Business Update

05. März 2024

Visualize and report: Risk by breach stages

Risk visualized across four stages of a breach



Risk also broken down via four key entities:



© reserved 483

Protect sensitive data from Generative AI

Problem

- Control the use of Generative AI like ChatGPT
- Allow granular access controls as opposed to just blocking

Solution

- Full DLP inspection across Generative AI platforms like ChatGPT
- Granular access controls including the use of Browser Isolation

Benefits

- Improved user productivity without incurring additional data loss risks

CRITERIA

- DLP Engines: Source Code
- Cloud Applications: ChatGPT
- ZPA Application Segment: Any
- Minimum Data Size (KB): 0
- URL Categories: Any
- Cloud Application Instances: None
- File Type: Any
- Users: Include
- Groups: Include
- User Risk Profile: Any
- Location Groups: Any
- Protocols: HTTP, HTTPS, Native FTP
- OCR: Enable
- Inspect Downloads: Enable

ACTION

- Application Access: Allow
- Daily Bandwidth Quota (MB): Enter Text
- Daily Time Quota (min): Enter Text
- Cascade to URL Filtering: [X]

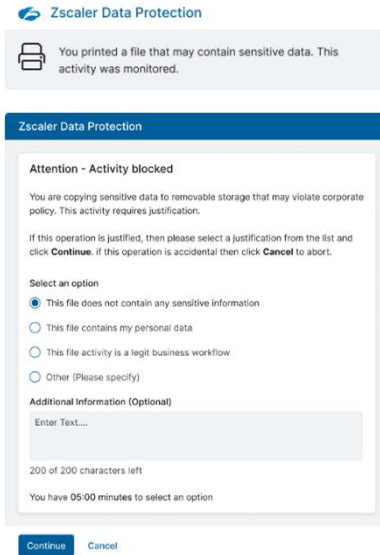
Zscaler Business Update

05. März 2024

Endpoint DLP - End User Experience

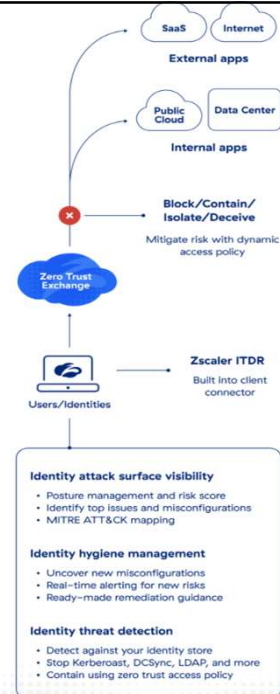
- Windows & macOS support
- Rule actions: Allow, Confirm, Block
- End-user interaction
 - Notification dialog
 - Confirmation dialog - user coaching
 - Request bypass

Flexible - from stealth mode to user education to full policy enforcement



ITDR – Mitigate the risk of identity attacks

Problem	Traditional threat detection and identity management approaches are ineffective against identity attacks because they are prone to false positives and rely on users to make smart decisions. Attacks like DCSync, DCShadow, 2FA MiTM, 2FA spamming, SIM cloning, session token hijacking/cookie stealing, etc. start by using valid credentials to compromise identities and then fly under the radar circumventing existing defenses and identity preventive controls.
Solution	Zscaler ITDR is a new identity security capability comprising identity posture, hygiene management, and threat detection. It provides continuous security assessment of Active Directory, change detection to flag risky configuration and permission changes in real-time, and identity threat detection to mitigate the risk of attacks stemming from misconfigurations and issues that cannot be remediated for business reasons.
Benefits	<ul style="list-style-type: none"> • Identity Attack Surface Visibility: Continuous visibility into misconfigurations, excessive permissions, and vulnerabilities in the Active Directory that can aid adversaries in escalating privileges and moving laterally • Identity Hygiene Management: Resources and content to build strong identity hygiene with step-by-step remediation guidance in the form of video tutorials, scripts, and commands. • Identity Threat Detection and Response: Detect and stop attacks like DCSync, DCShadow, kerberoasting, and more in the event of an identity compromise. Contain and respond using native integrations with ZPA and ZIA and tech integrations with leading EDRs and SIEMs.



Zscaler Business Update

05. März 2024

Target Picture – Simplified but still enforcing Zero Trust Access Principles

