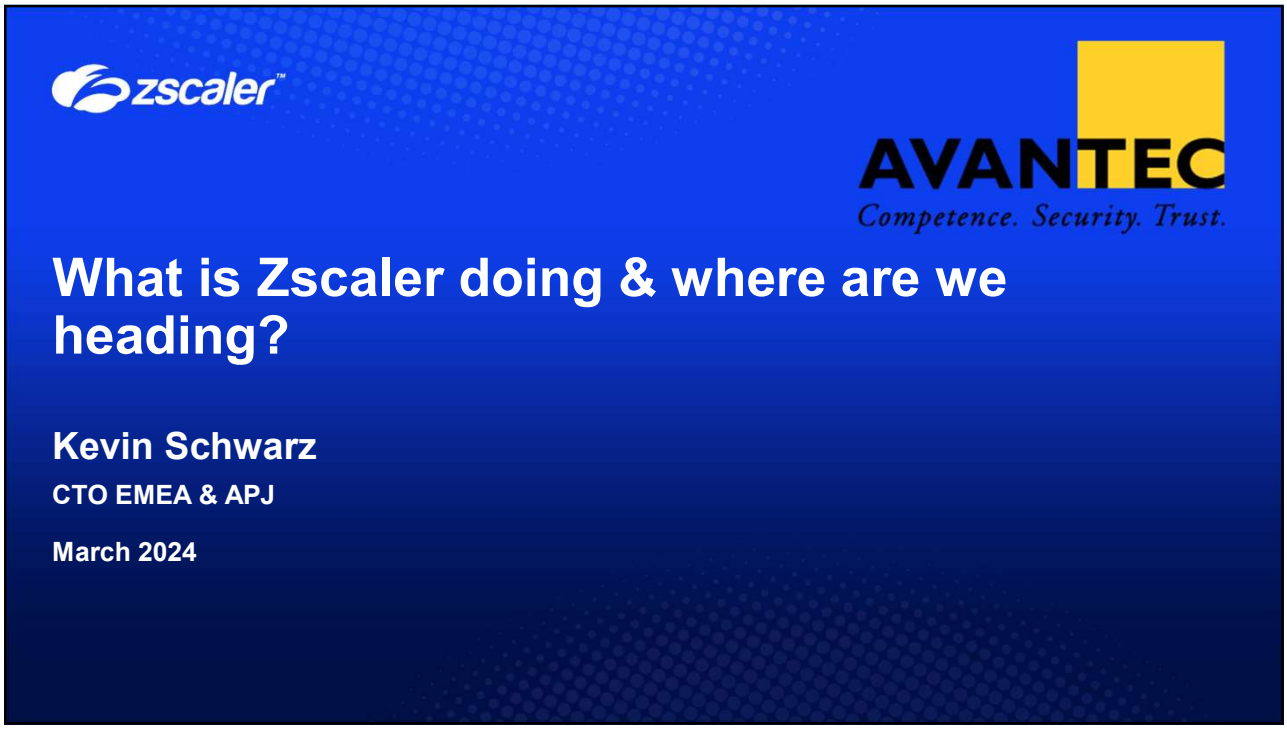
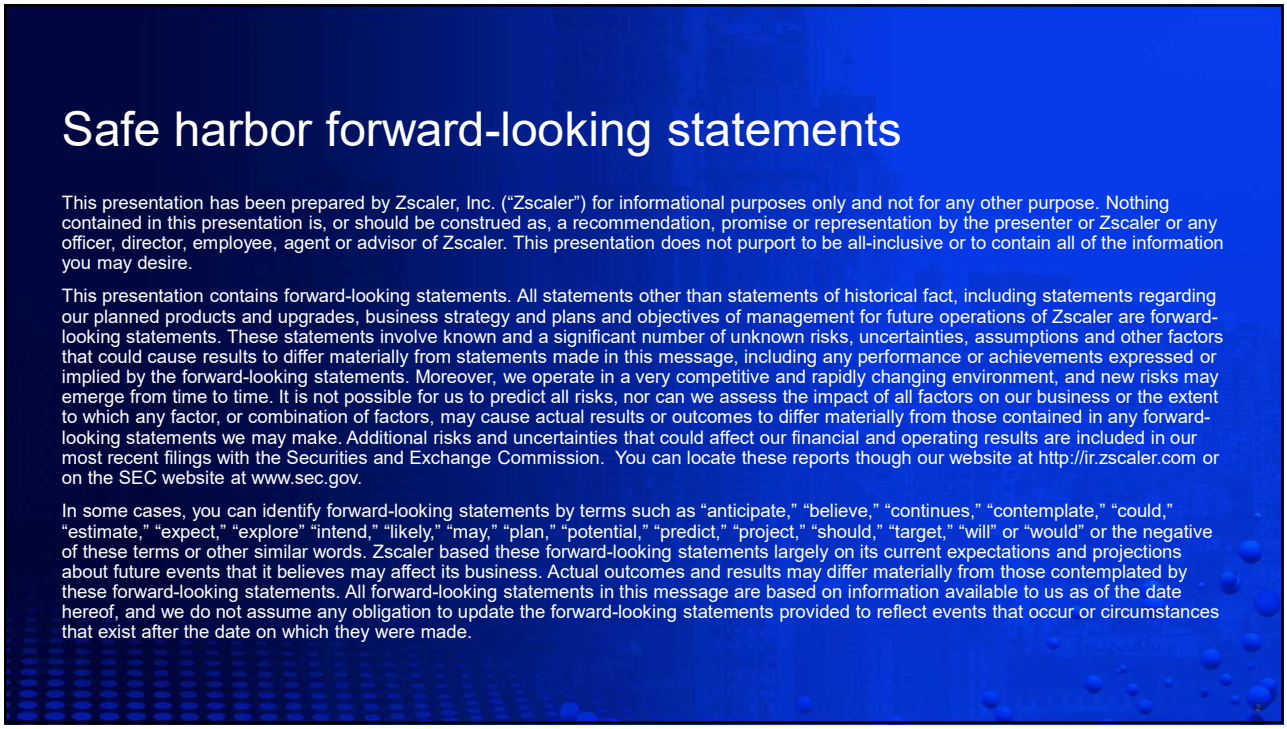
Zscaler Business Update
05. März 2024





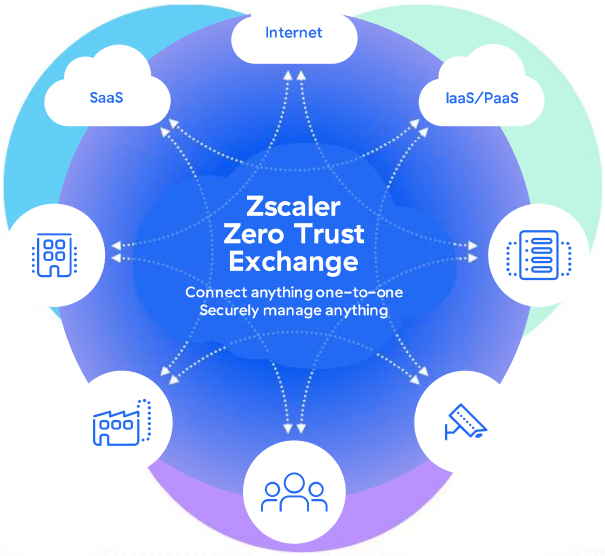
AVANTEC
Competence. Security. Trust.

Zscaler Business Update
05. März 2024

Empowering your business to be more

secure, **simple**, and **productive**.

Zero Trust Exchange



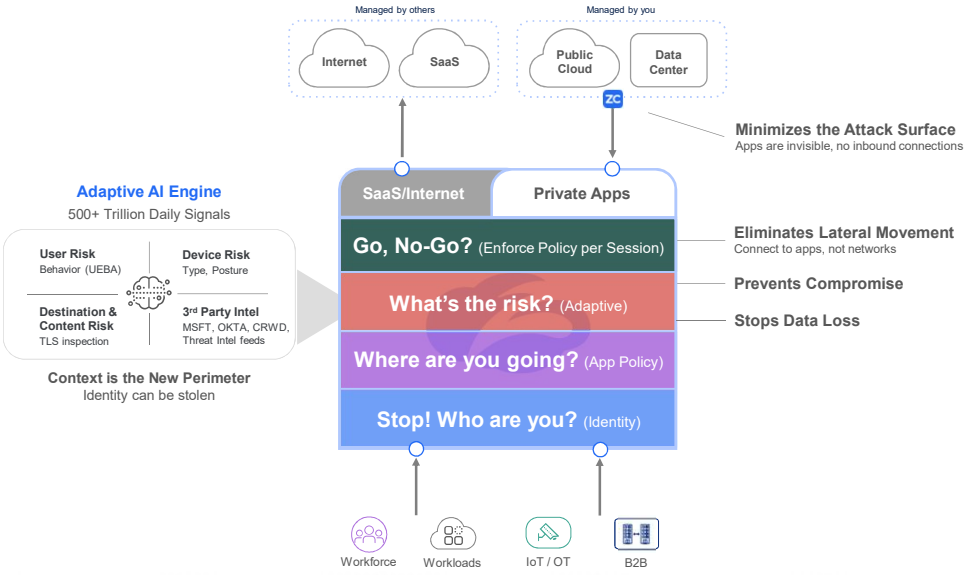
Experience your world, secured.

© 2024 Zscaler, Inc. All rights reserved.

AVANTEC
Competence. Security. Trust.

Zscaler Business Update
05. März 2024

A New Architecture is the Answer: Zero Trust Exchange



zscaler | Experience your world, secured.

© 2024 Zscaler, Inc. All rights reserved. 5

Comprehensive Solutions Across Four Key Areas

Business Insights
Knowledge from trillions of daily telemetry signals

Cyber Threat Protection
Prevent compromise and lateral movement

Zero Trust Exchange
AI-POWERED

Data Protection
Prevent data loss, inline and API

Zero Trust Networking
Connect to Apps, not networks

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

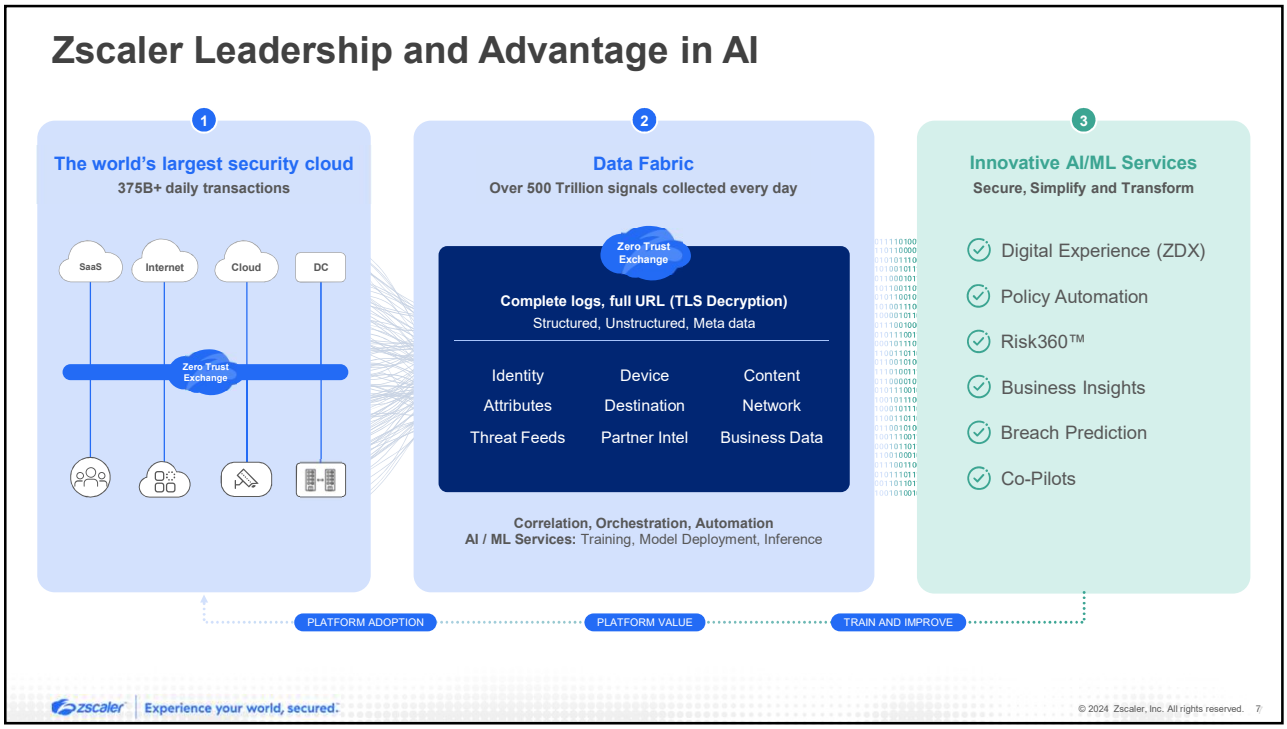
Zscaler for Users | Zscaler for Workloads | Zscaler for B2B | Zscaler for IoT / OT

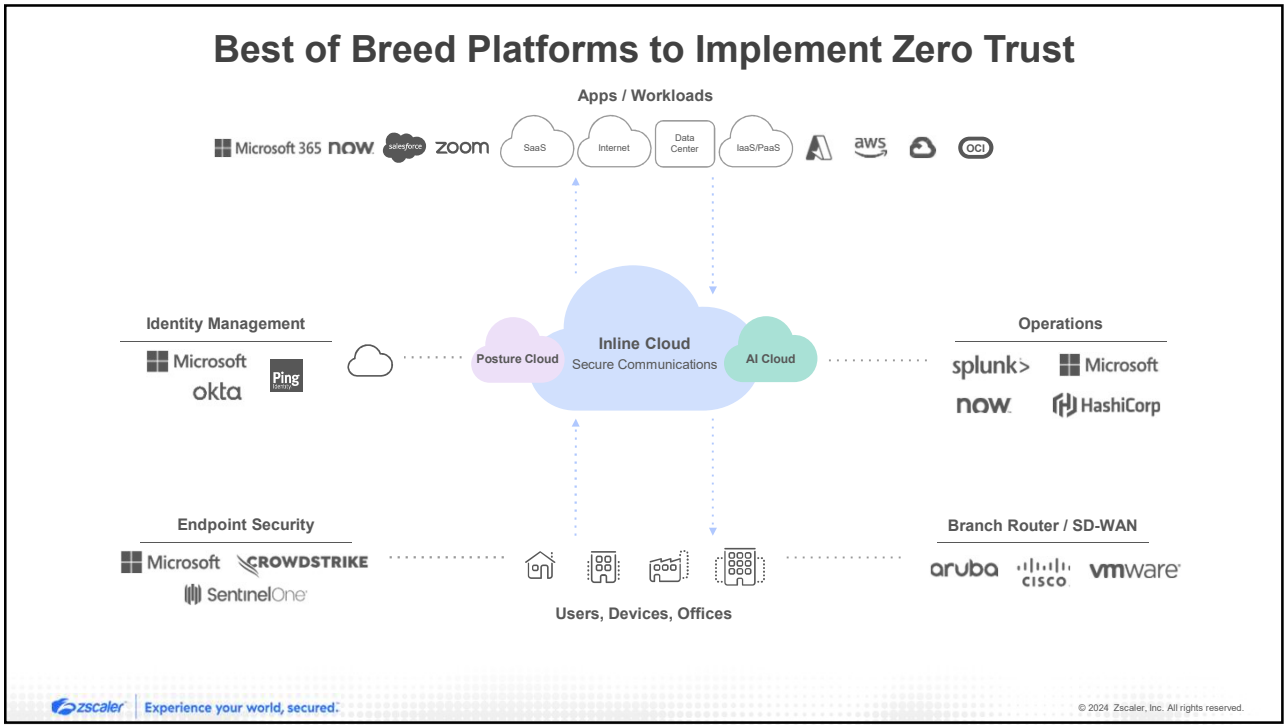
zscaler | Experience your world, secured.

© 2024 Zscaler, Inc. All rights reserved.

AVANTEC
Competence. Security. Trust.

Zscaler Business Update
05. März 2024



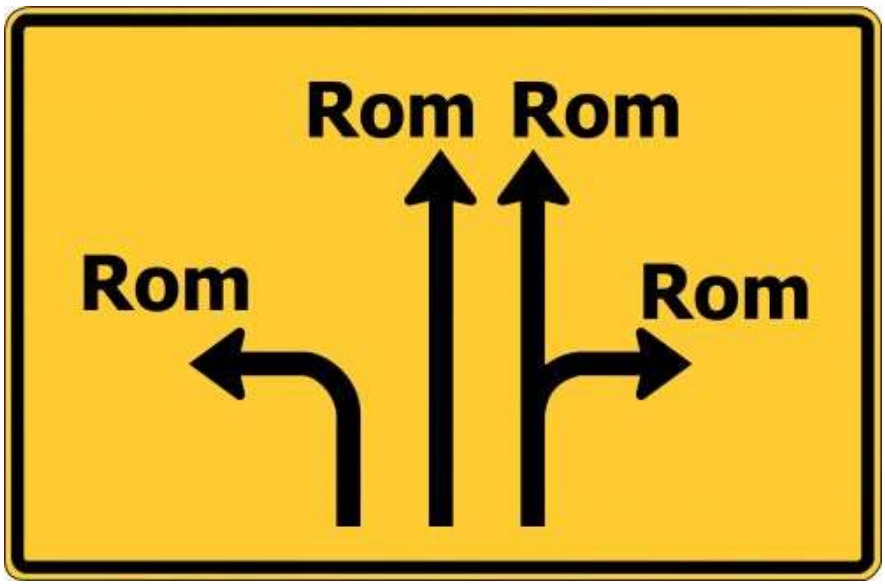


AVANTEC
Competence. Security. Trust.

Zscaler Business Update
05. März 2024

How does such a journey look like?

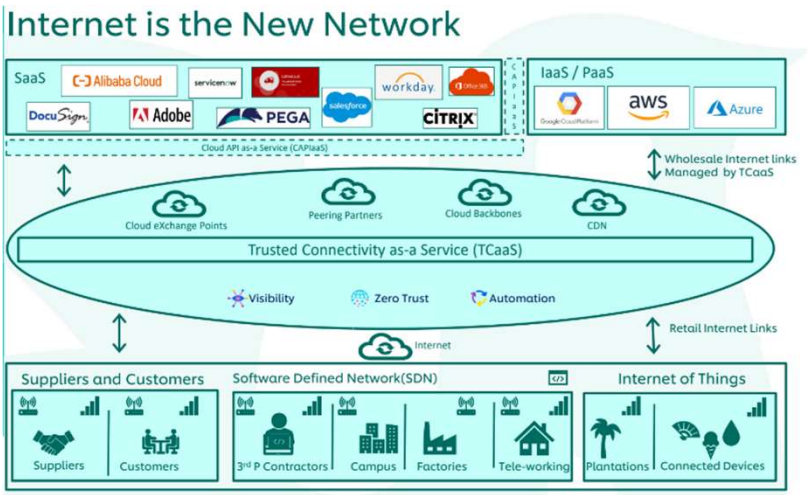
zscaler | Experience your world, secured.
© 2024 Zscaler, Inc. All rights reserved. 9



zscaler | Experience your world, secured.
© 2024 Zscaler, Inc. All rights reserved.

AVANTEC
Competence. Security. Trust.

Zscaler Business Update
05. März 2024



zscaler | Experience your world, secured.

© 2024 Zscaler, Inc. All rights reserved.

Example Transformation Roadmap

	Phase 1	Phase 2	Phase 3	Phase 4	Target Picture
BUSINESS New Business Models					• Enabling the Digital Workforce • IT enables Business based on Platform Approach
APPLICATION Data Center to Cloud				• Shortened Deployment Cycles due to DevSecOps • Automation for Workload Deployment, securely	Automated Multicloud Application Deployment & Access with highest User Experience
NETWORK Direct to Internet			• Increase Usage of Internet • Verify Hops in Connectivity path	Focus on Thin Branch Model based on Gartner's SASE	Internet is the new corporate network
SIMPLIFY Remove Legacy		• Offload Proxy & VPN Solution • Reduce admin overhead	• Centralize Visibility & Policy • Reduce 3rd Party Access tools	• Reduce need for network segmentation & NAC • Optimize the Data Flood towards SOC	Reduce Technical Debt & operational overhead with Evergreen IT
SECURE Network Security to Zero Trust	Kicking out Users from the Network	User to Application Segmentation based on ZT Principles	Expand Secure Access to further Use Cases (e.g. 3rd Parties, Branches, Workloads, etc)	• Smarter Security for Zero Trust for Hackers • Get Deeper in Data Protection • Protect IoT Devices	• Security by Design based on Zero Trust Principles • Consistent security regardless of user, location or device

zscaler | Experience your world, secured.

© 2024 Zscaler, Inc. All rights reserved.

AVANTEC
Competence. Security. Trust.

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

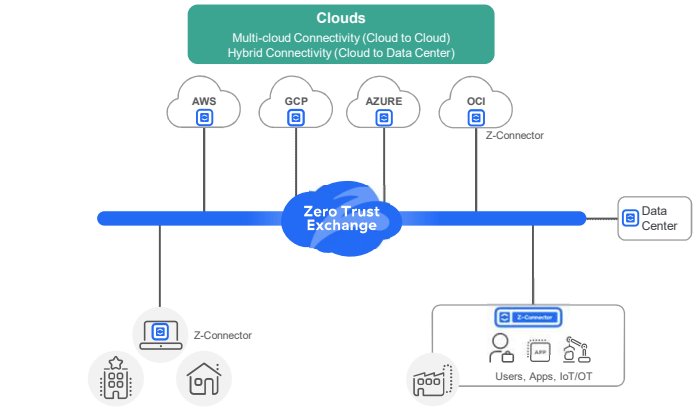
Globally Distributed Cloud: 150+ Data Centers, China Connectivity, Peering, BCP/DR

Zscaler for Users | Zscaler for Workloads | Zscaler for B2B | Zscaler for IoT / OT

zscaler | Experience your world, secured.

© 2024 Zscaler, Inc. All rights reserved.

Zero Trust Connectivity for Users, Cloud, and Branches



Z-Connectors: Send and receive traffic to and from the Zero Trust Exchange

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

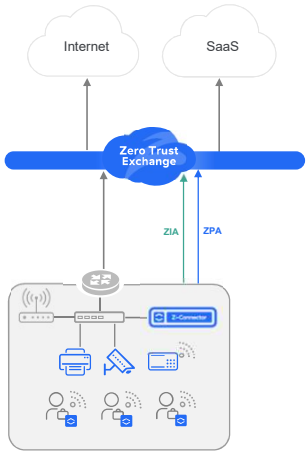
zscaler | Experience your world, secured.

© 2024 Zscaler, Inc. All rights reserved.

AVANTEC
Competence. Security. Trust.

Zscaler Business Update
05. März 2024

Use Cases: IoT device discovery and classification



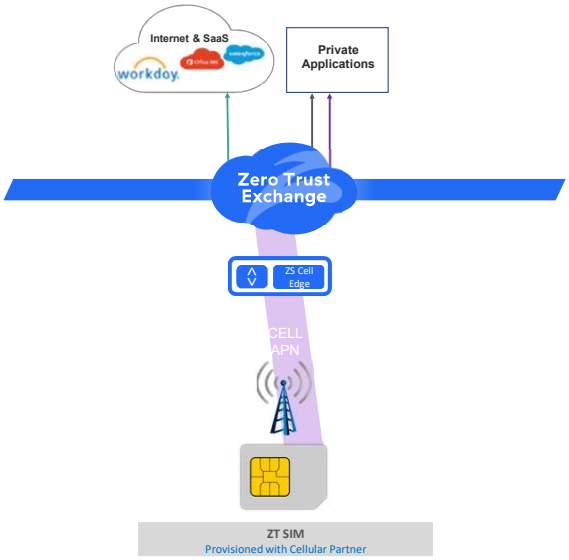
Benefits

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

zscaler | Experience your world, secured.

© 2024 Zscaler, Inc. All rights reserved.

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

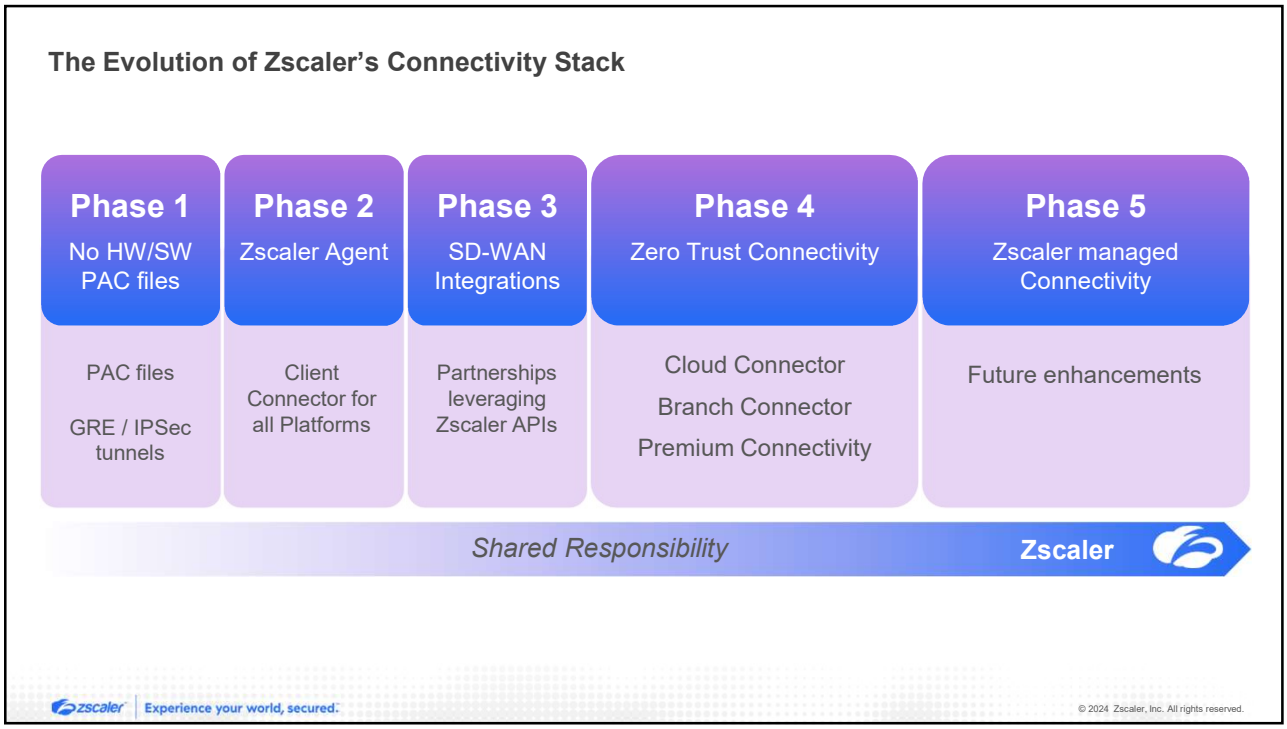
- Instant deployment possibility
- No additional hardware required
- Utilizing existing Security environment to avoid split between OT & IT departments
- Having possibility to access Devices remotely for maintenance scenarios
- Avoiding unnecessary dispatching of Remote Engineers

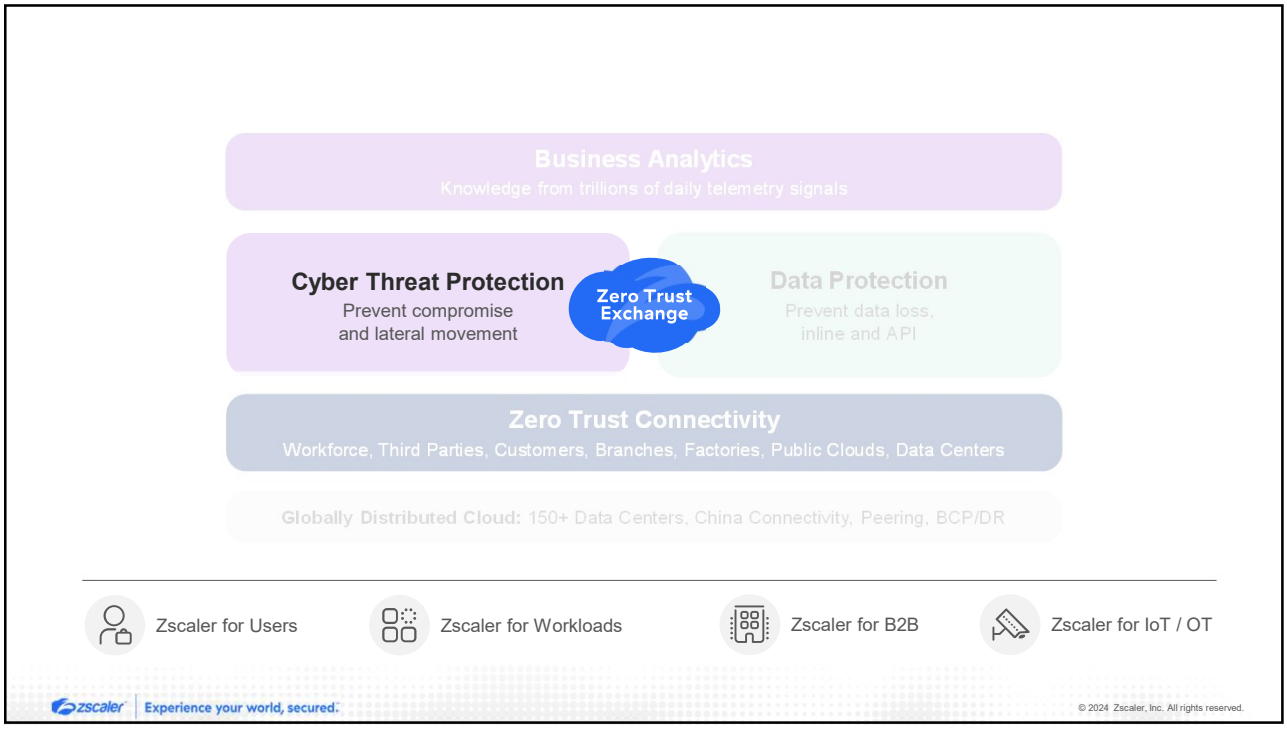
zscaler | Experience your world, secured.

© 2024 Zscaler, Inc. All rights reserved.

AVANTEC
Competence. Security. Trust.

Zscaler Business Update
05. März 2024





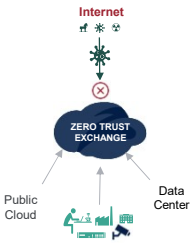
AVANTEC
Competence. Security. Trust.

Zscaler Business Update
05. März 2024

Zero Trust Security: Cyber Threat Protection

Prevent Compromise

Block threats before they reach you



Protects users, servers, apps, IoT, OT systems

Apps invisible to the internet

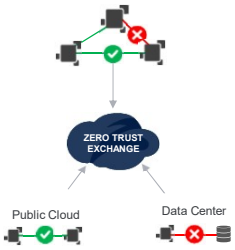
Can't attack what you can't see

Prevent Lateral Movement

User to app Segmentation

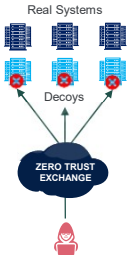
Connects users to apps, not networks

App to App Segmentation



Connects apps to apps or processes to processes over any network

Decoys detect sophisticated threats



Attackers attempting to move laterally are detected by decoys

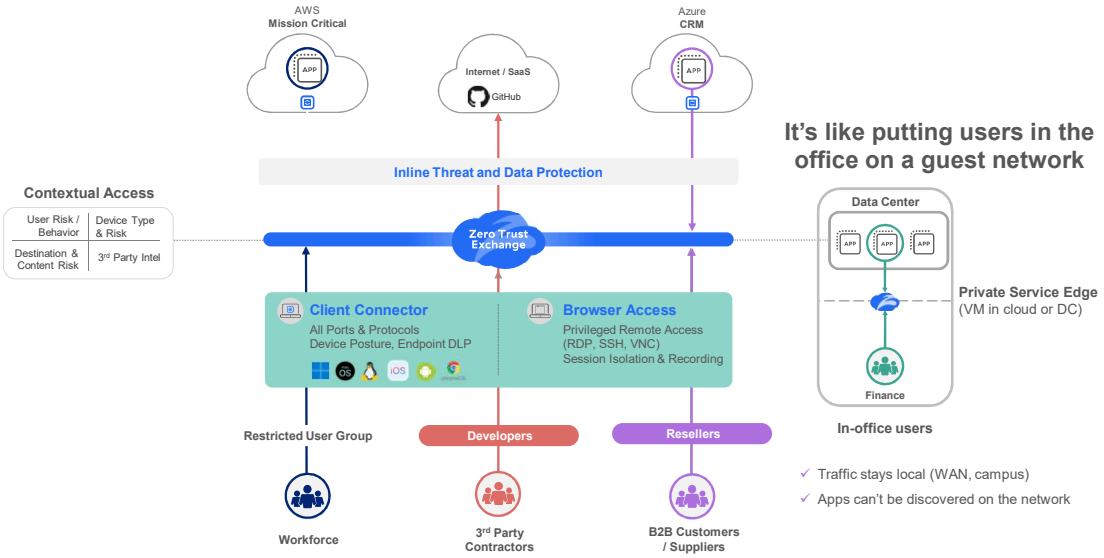
What sets Zscaler Cyber Threat Protection apart?

Zero Passthrough Connections | Zero Attack surface | Zero Lateral Movement

zscaler | Experience your world, secured.

© 2024 Zscaler, Inc. All rights reserved.

Zero Trust Connectivity for Users



It's like putting users in the office on a guest network

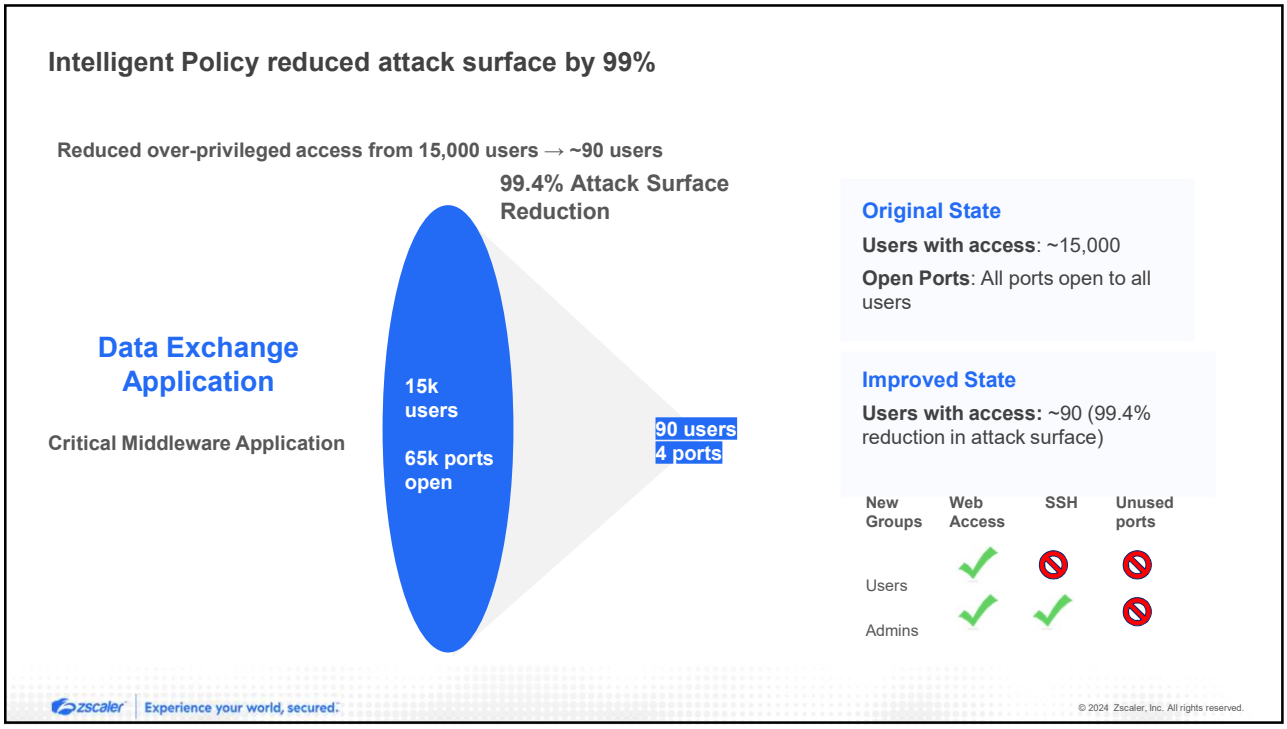
- ✓ Traffic stays local (WAN, campus)
- ✓ Apps can't be discovered on the network

zscaler | Experience your world, secured.

© 2024 Zscaler, Inc. All rights reserved.

AVANTEC
Competence. Security. Trust.

Zscaler Business Update
05. März 2024



AVANTEC
Competence. Security. Trust.

Zscaler Business Update
05. März 2024

Continuing to simplify segmentation with ZPA

Four-phased approach to simplifying Segmentation

Lower the Effort

Intelligent Policy

Remove Adoption Barriers

Policy Monitor Mode

COMING SOON!

Measure Progress

Critical Apps Segmentation Report

COMING SOON!

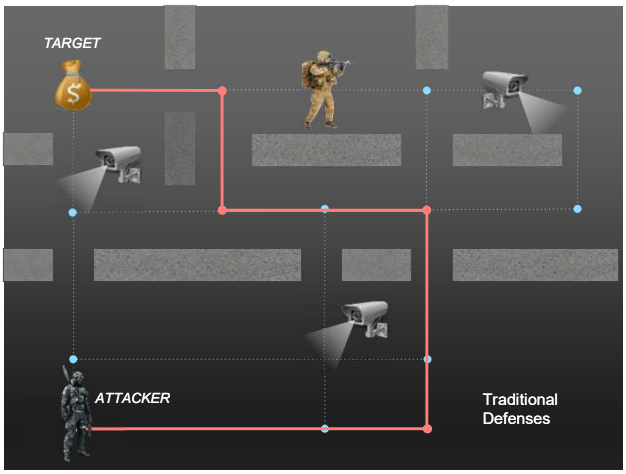
Simplify Upkeep

CMDB Sync

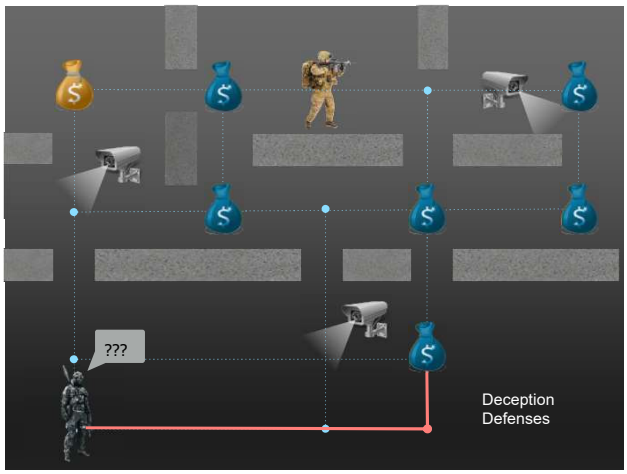
Access provisioning workflow automation

zscaler | Experience your world, secured.
© 2024 Zscaler, Inc. All rights reserved.

Deception disrupts advanced attacks



Attackers know your strategy. Predictable defenses are easily bypassed

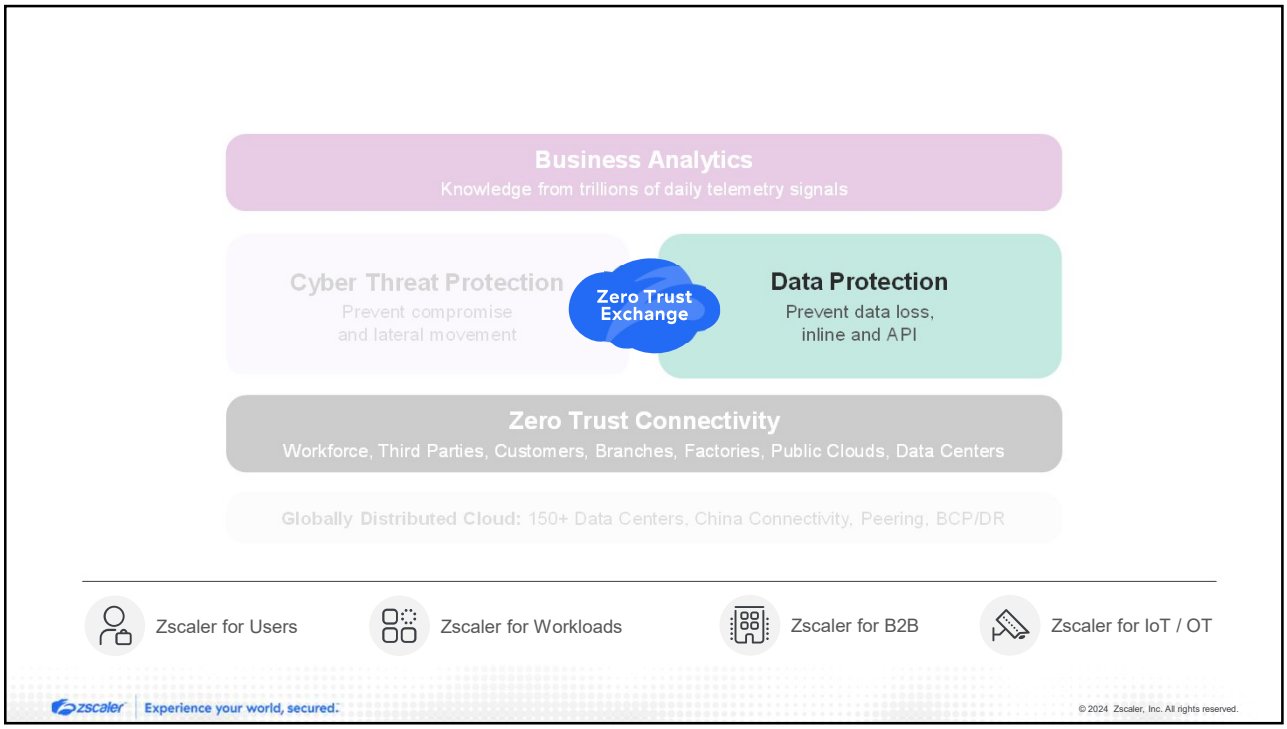


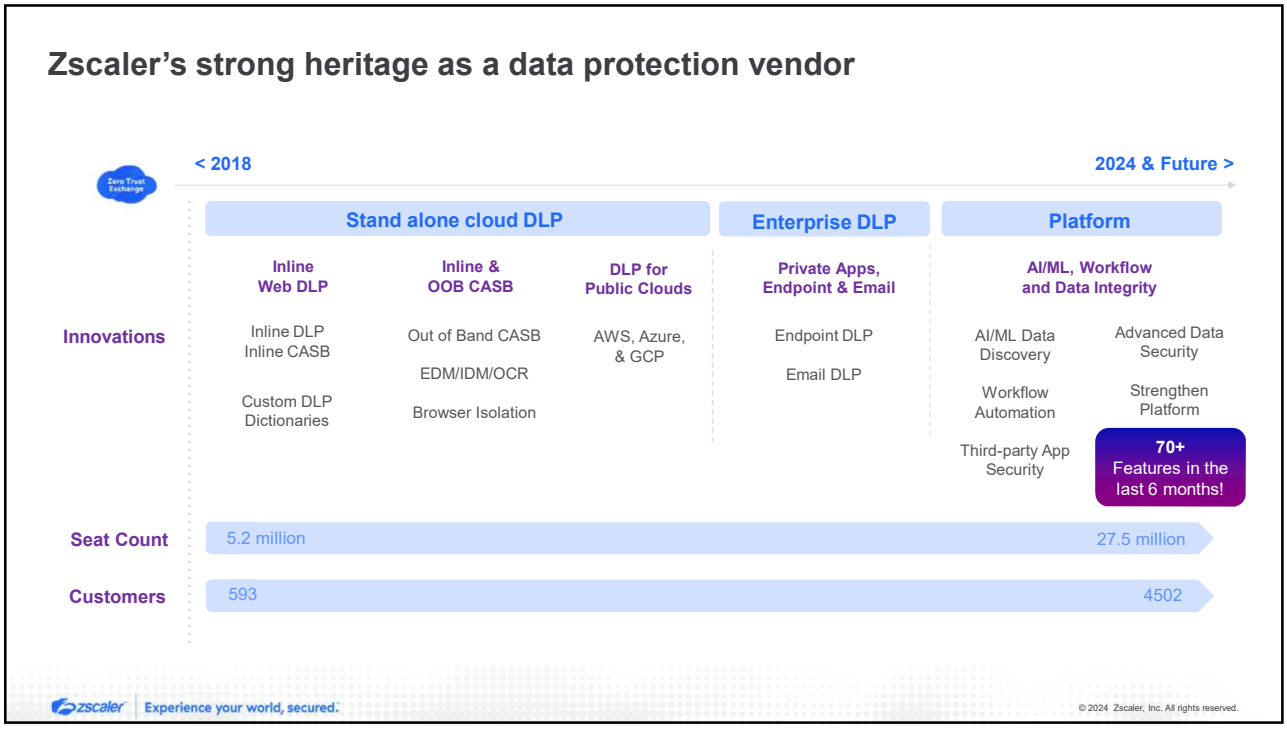
Decoys and traps make your environment unpredictable, disrupt attacker playbooks

zscaler | Experience your world, secured.
© 2024 Zscaler, Inc. All rights reserved.

AVANTEC
Competence. Security. Trust.

Zscaler Business Update
05. März 2024

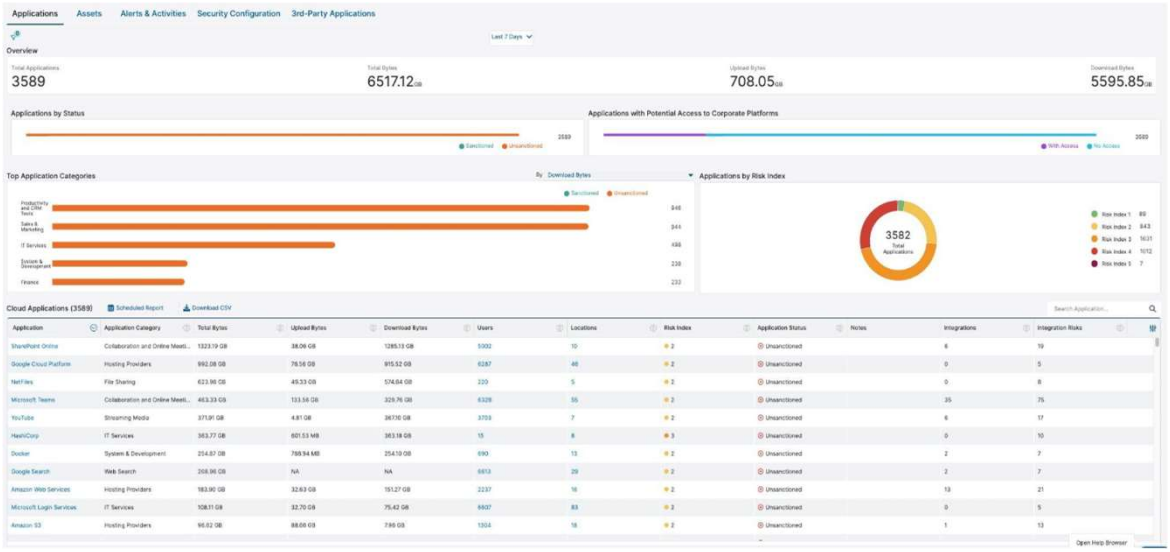




AVANTEC
Competence. Security. Trust.

Zscaler Business Update
05. März 2024

SaaS Security Report



© 2024 Zscaler, Inc. All rights reserved.

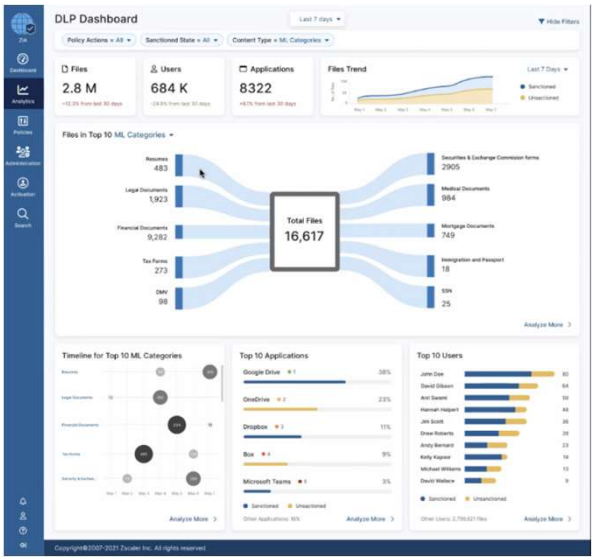
Auto classification & data discovery powered by AI/ML

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

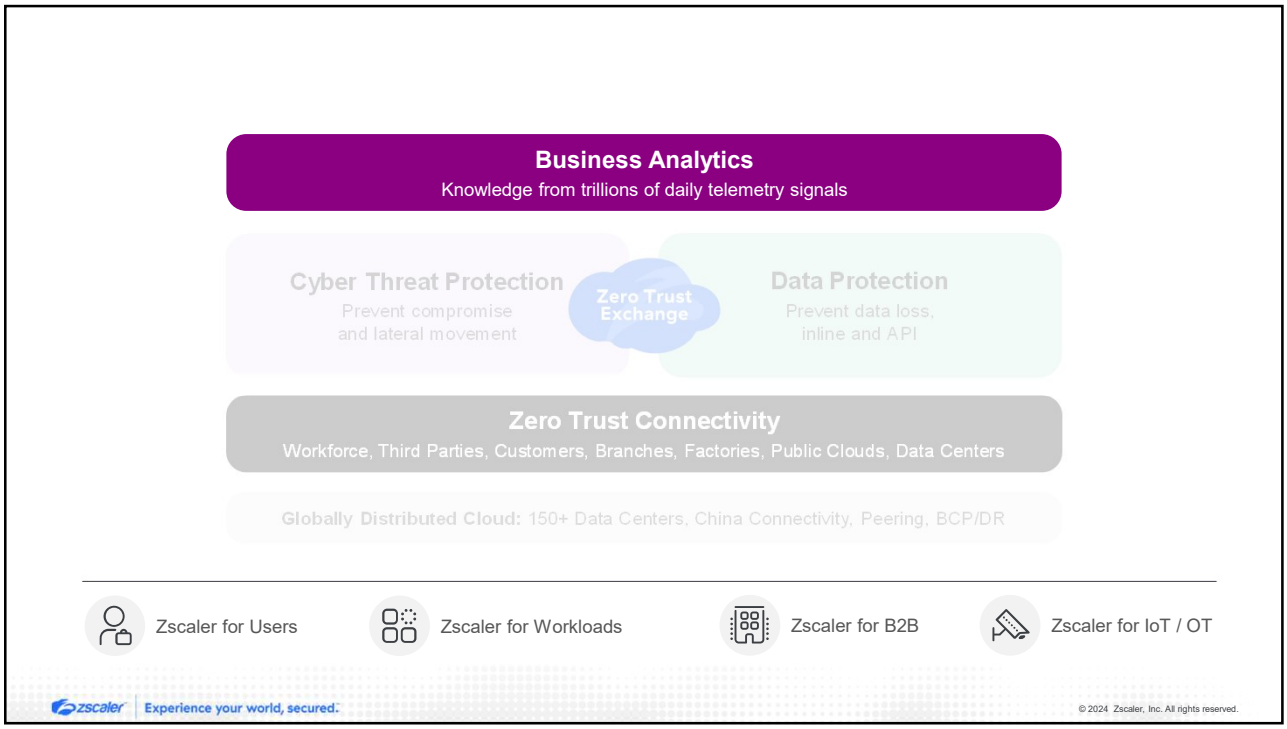
- Deep learning engine
- Over 90 Thematic Data Categories
- Customer defined categories
- Supervised learning model
- NLP, TF/ITF, document clustering
- Vector learning

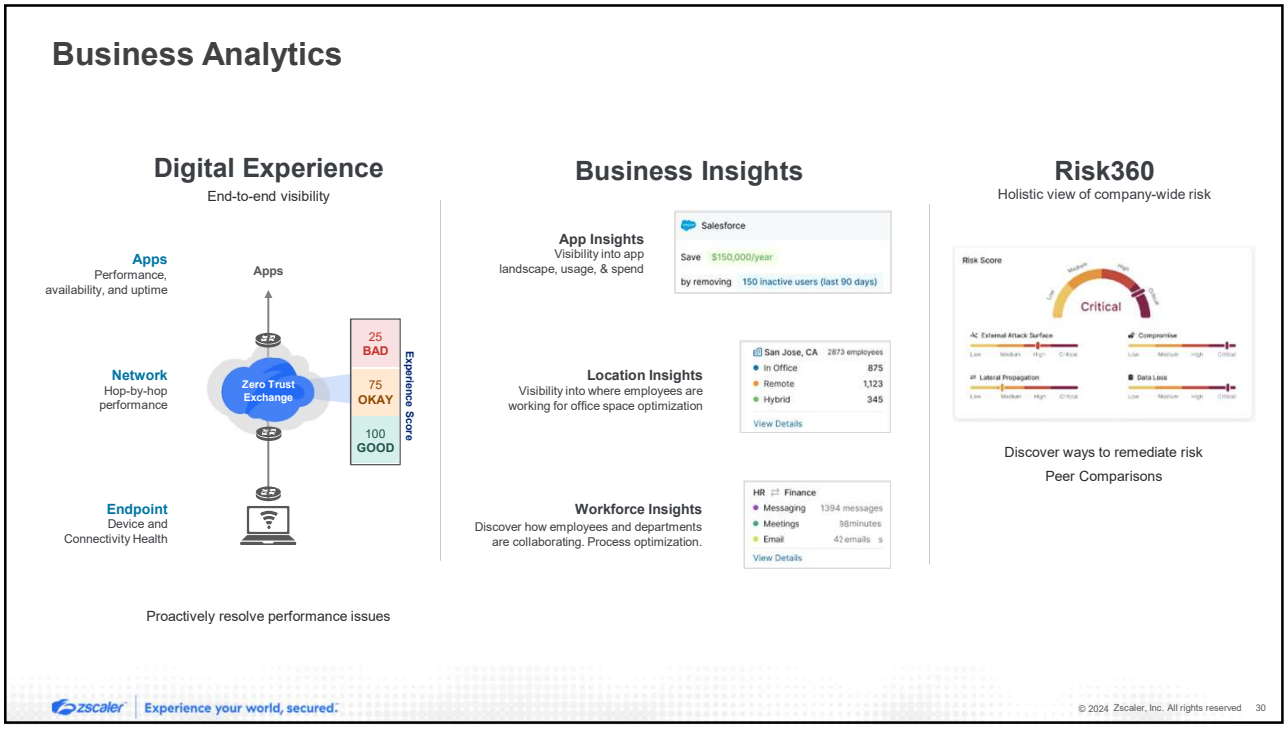


© 2024 Zscaler, Inc. All rights reserved.

AVANTEC
Competence. Security. Trust.

Zscaler Business Update
05. März 2024





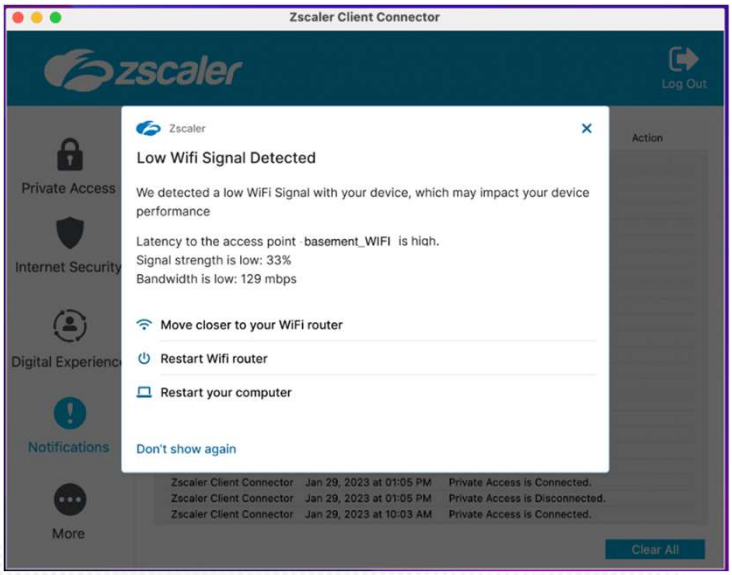
AVANTEC
Competence. Security. Trust.

Zscaler Business Update
05. März 2024

Self Service IT

Helping user remediate on the fly

Detect exactly when problems happen



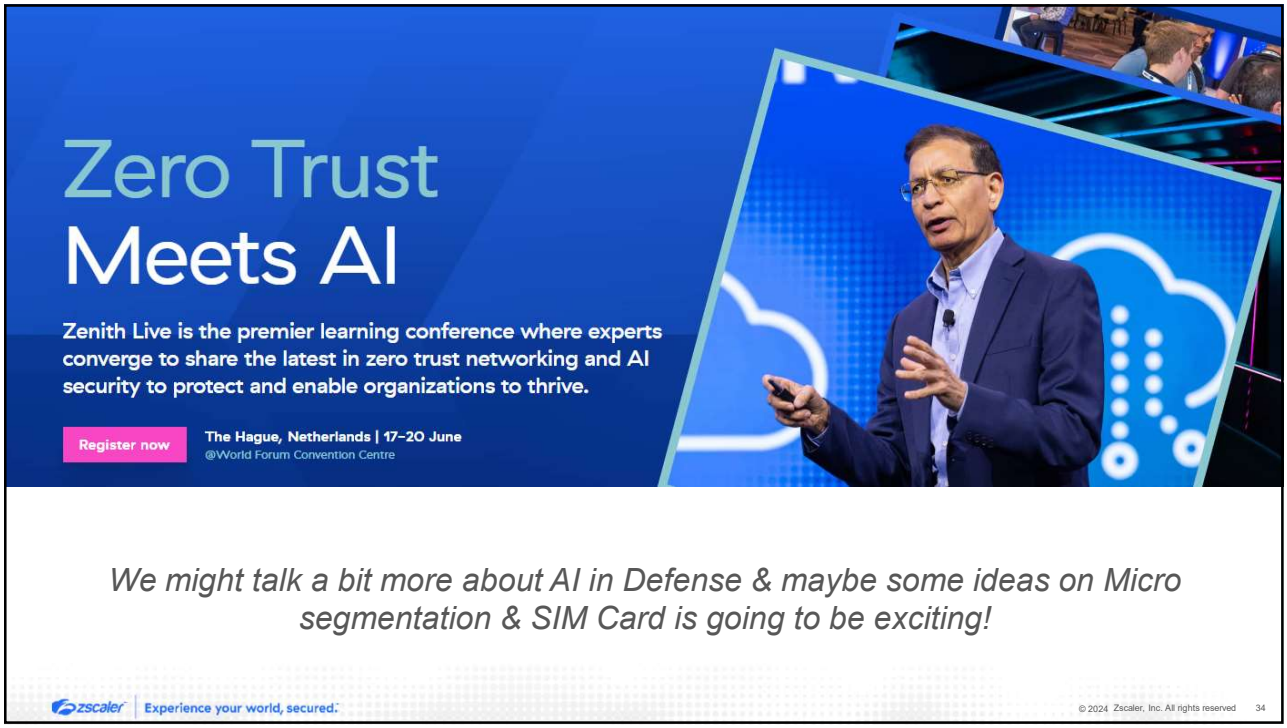
© 2024 Zscaler, Inc. All rights reserved

Last but not least, some cool Events coming up!

© 2024 Zscaler, Inc. All rights reserved.

AVANTEC
Competence. Security. Trust.

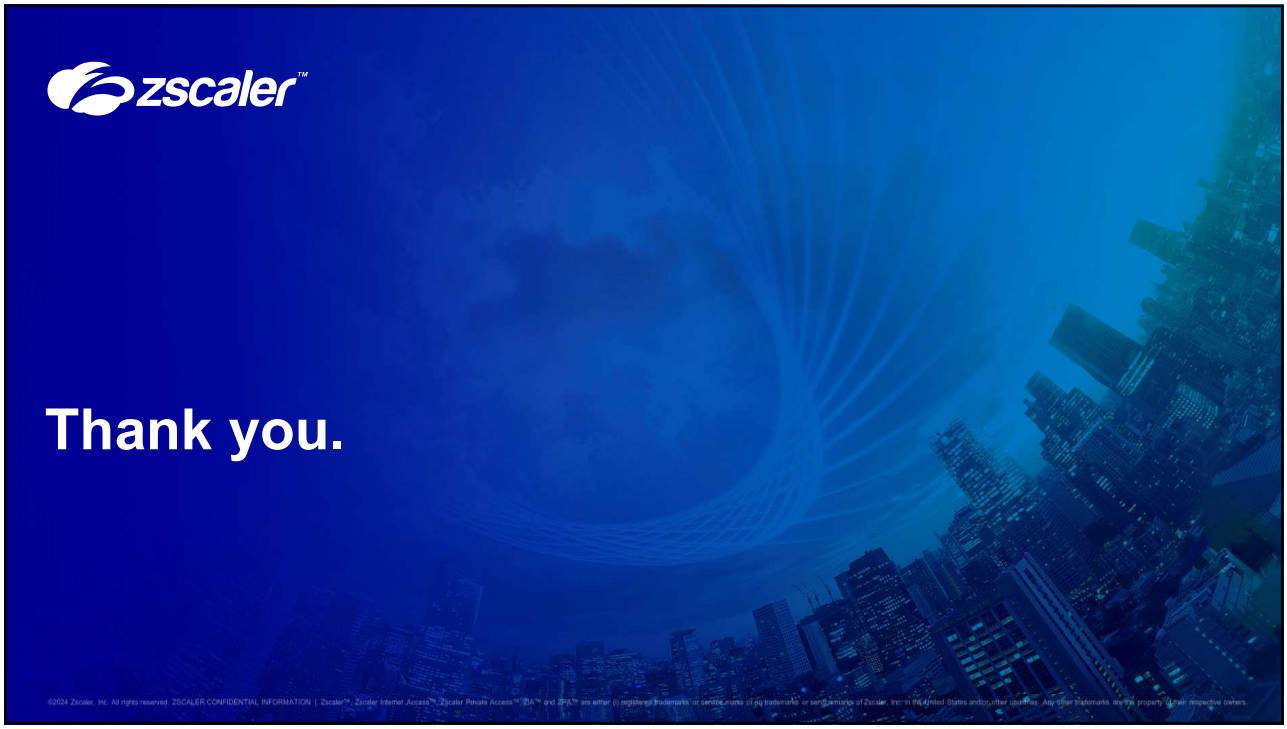
Zscaler Business Update
05. März 2024

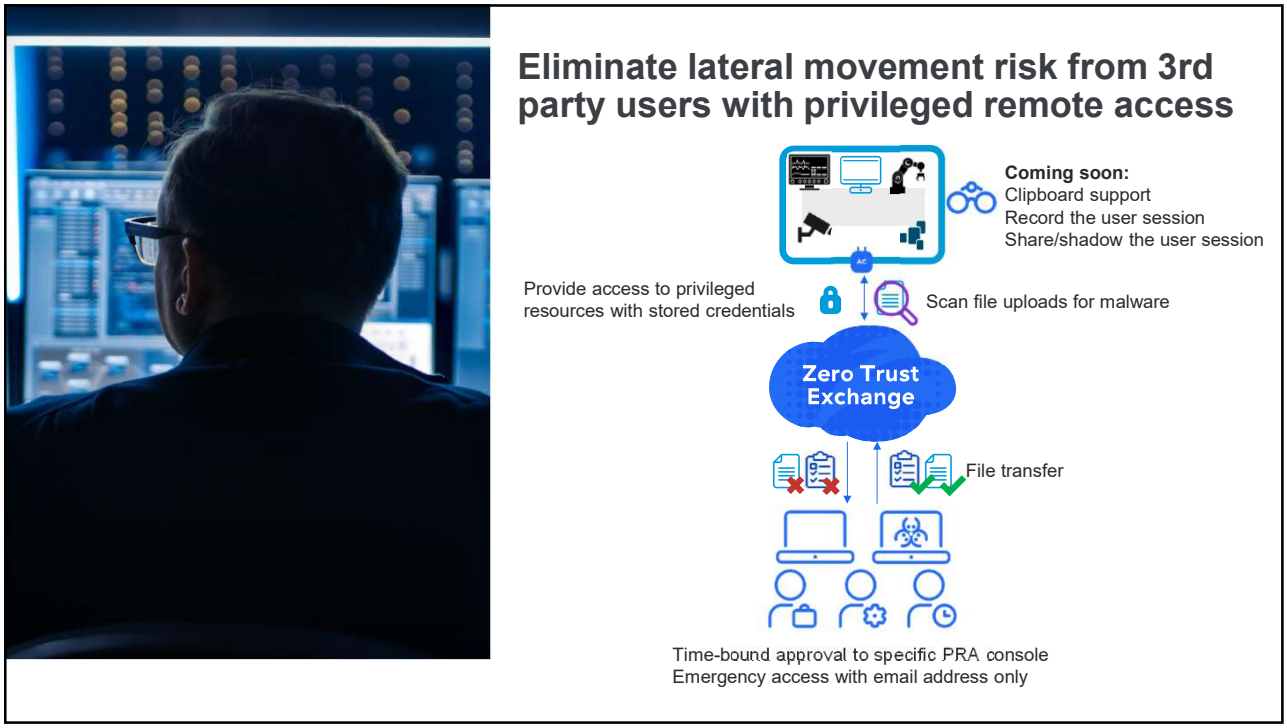


We might talk a bit more about AI in Defense & maybe some ideas on Micro segmentation & SIM Card is going to be exciting!

AVANTEC
Competence. Security. Trust.

Zscaler Business Update
05. März 2024



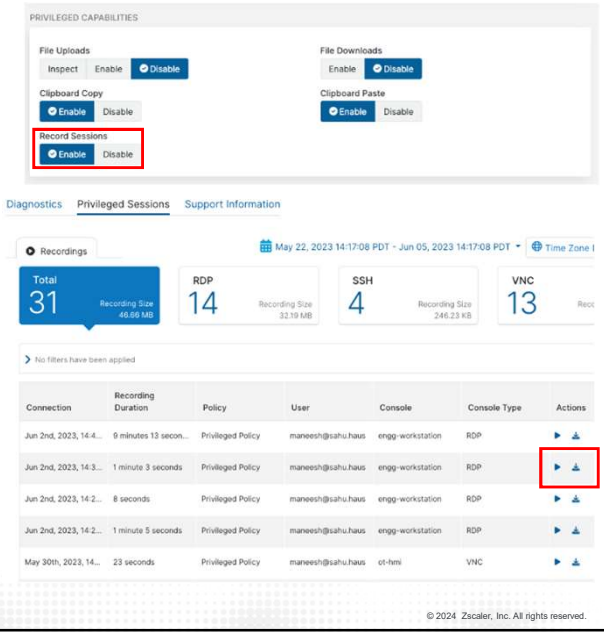


AVANTEC
Competence. Security. Trust.

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	• **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.



zscaler | Experience your world, secured.
© 2024 Zscaler, Inc. All rights reserved.

Browser isolation for private apps

Watermarking for security

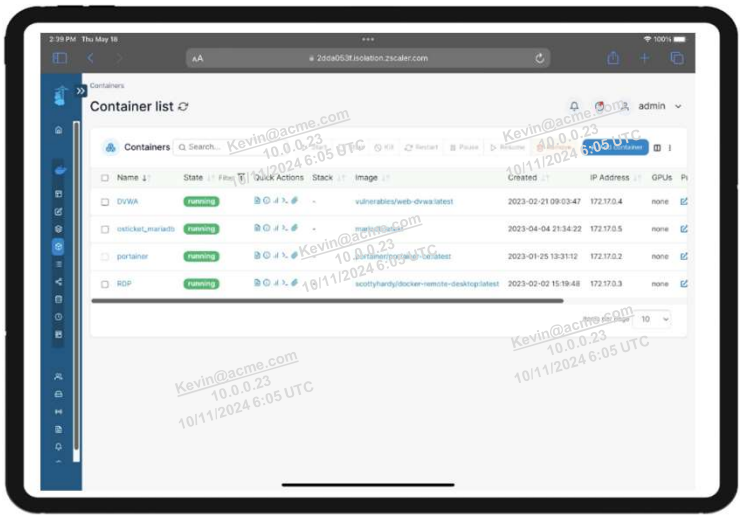
Prevent and trace data theft with a watermark

Adds username and timestamp to the screen

Mobile device support

Support mobile form factors

Enable touchscreens & on-screen keyboards



AVANTEC
Competence. Security. Trust.

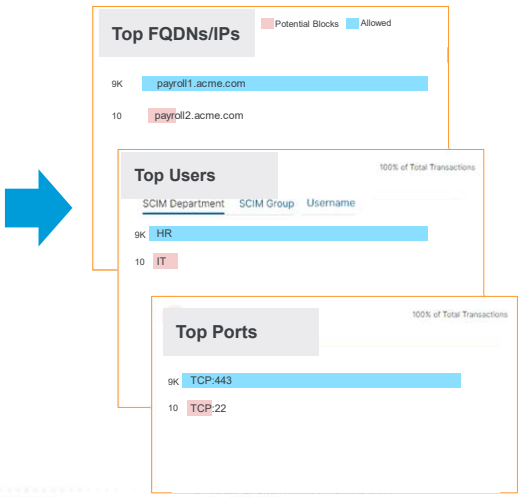
Zscaler Business Update
05. März 2024

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

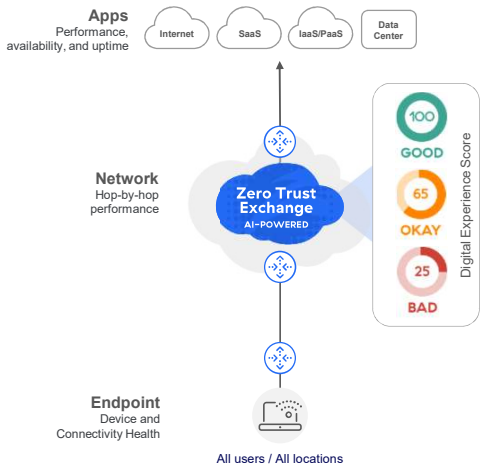


zscaler | Experience your world, secured.

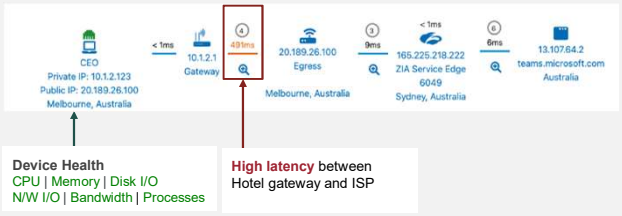
© 2024 Zscaler, Inc. All rights reserved 39

Proactively identify and resolve performance issues (ZDX)

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



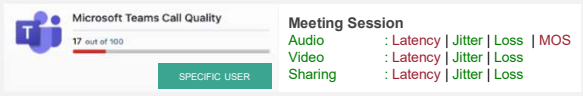
Full view of every step of the traffic path



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



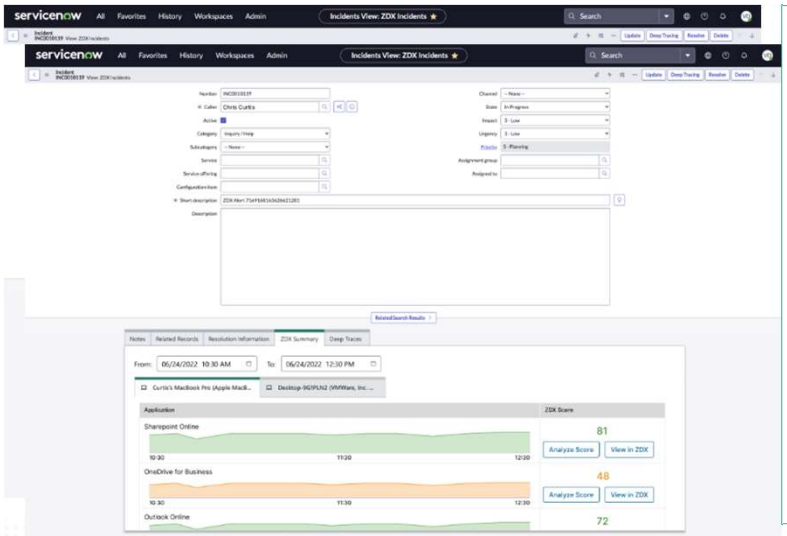
Unify monitoring silos for great visibility to quickly troubleshoot performance issues

AVANTEC
Competence. Security. Trust.

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.

© 2024 Zscaler, Inc. All rights reserved

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

© 2024 Zscaler, Inc. All rights reserved

AVANTEC
Competence. Security. Trust.

Zscaler Business Update
05. März 2024

Visualize and report: Risk by breach stages

Risk visualized across four stages of a breach

External Attack Surface	Prevent Compromise	Lateral Propagation	Data Loss
Looks for exposed servers and ASNs.	Analyzes events, security configs and traffic flows	Assesses private access settings and metrics	Assesses data protection exposures and configurations

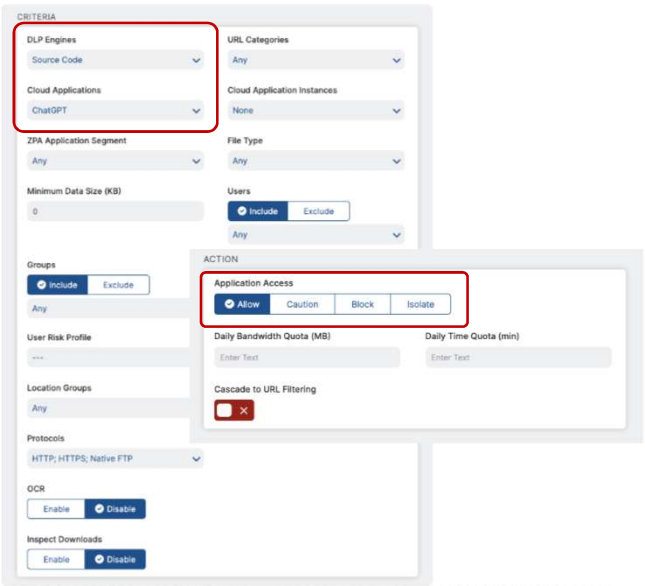
Risk also broken down via four key entities:

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



zscaler | Experience your world, secured.

© 2024 Zscaler, Inc. All rights reserved.

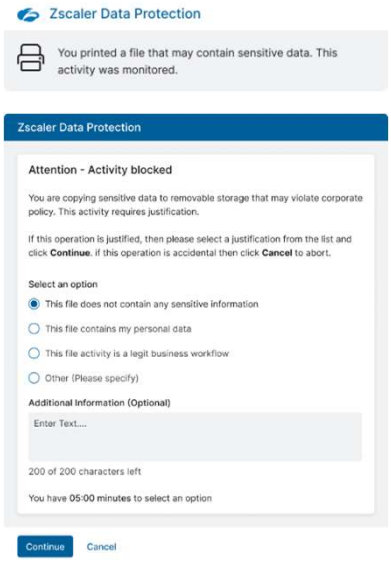
AVANTEC
Competence. Security. Trust.

Zscaler Business Update
05. März 2024

Endpoint DLP - End User Experience

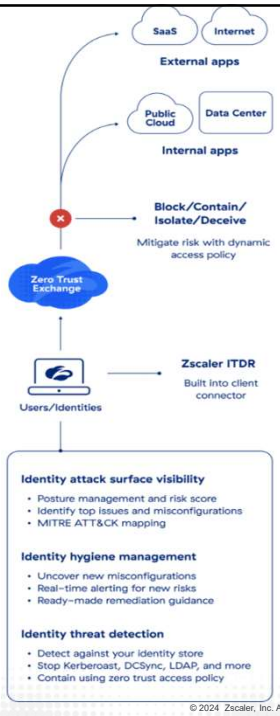
- Windows & macOS support
- Rule actions: Allow, Confirm, Block
- End-user interaction
  - Notification dialog
  - Confirmation dialog - user coaching
  - Request bypass

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. If 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	• **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.



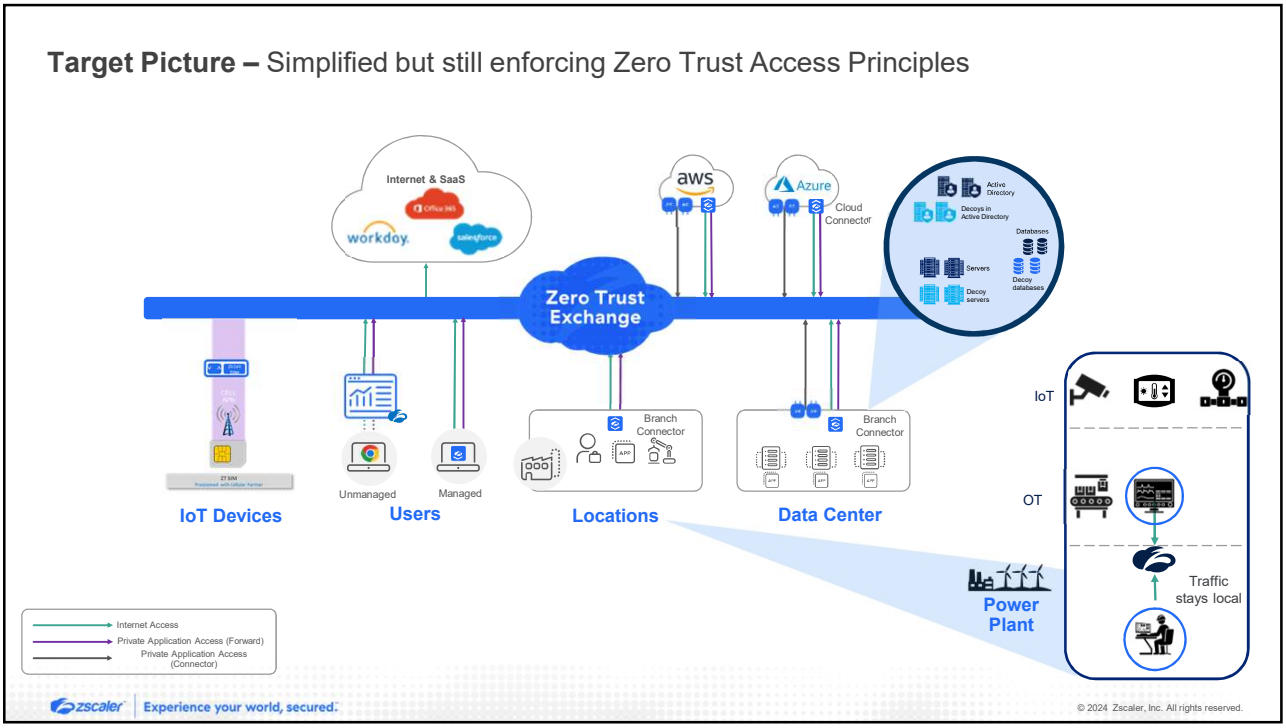
zscaler | Experience your world, secured.

© 2024 Zscaler, Inc. All rights reserved.

AVANTEC
Competence. Security. Trust.

Zscaler Business Update
05. März 2024

Target Picture – Simplified but still enforcing Zero Trust Access Principles



AVANTEC
Competence. Security. Trust.