

Risk Management



Samuel Kölbener
Senior Manager Solution
Consulting, Zscaler



Lots of tools, still lots of questions we can't answer

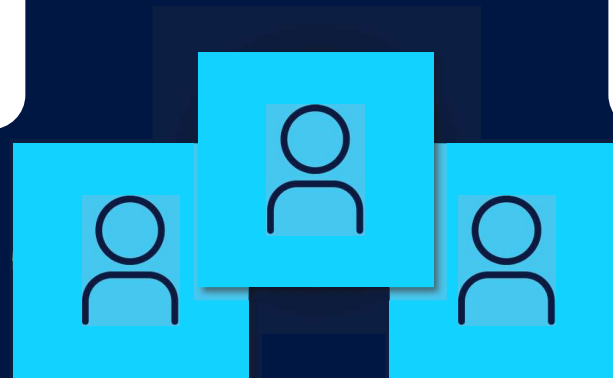


How vulnerable are our most critical apps?

How many assets do we really have?

Are endpoint agents installed everywhere they should be?

How has our risk posture changed since the last board meeting?

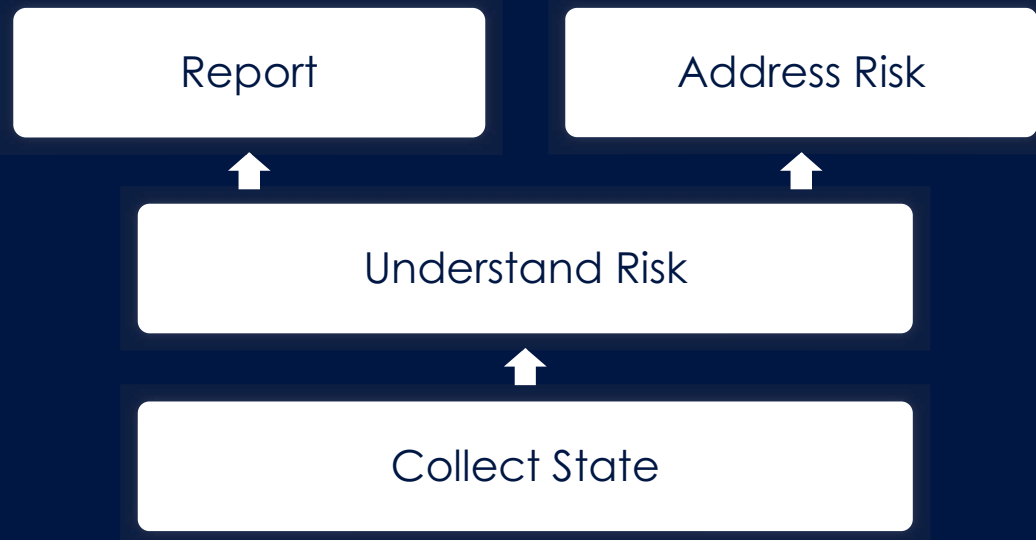


CISOs wonder...

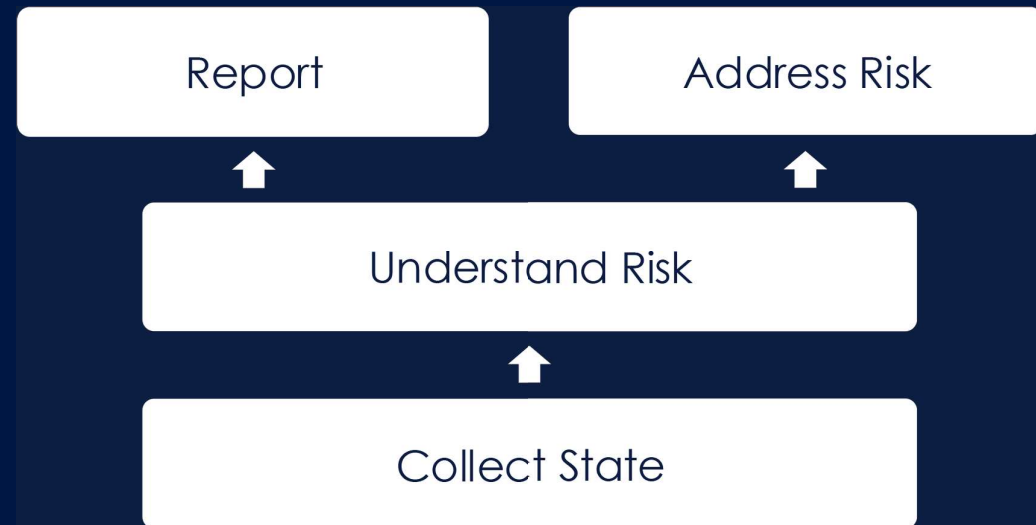
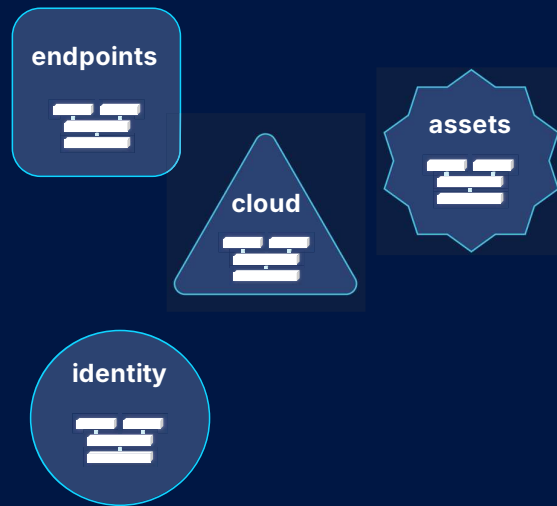
Why is it so hard to understand our threat exposure?



Every security tool provides the same core functions



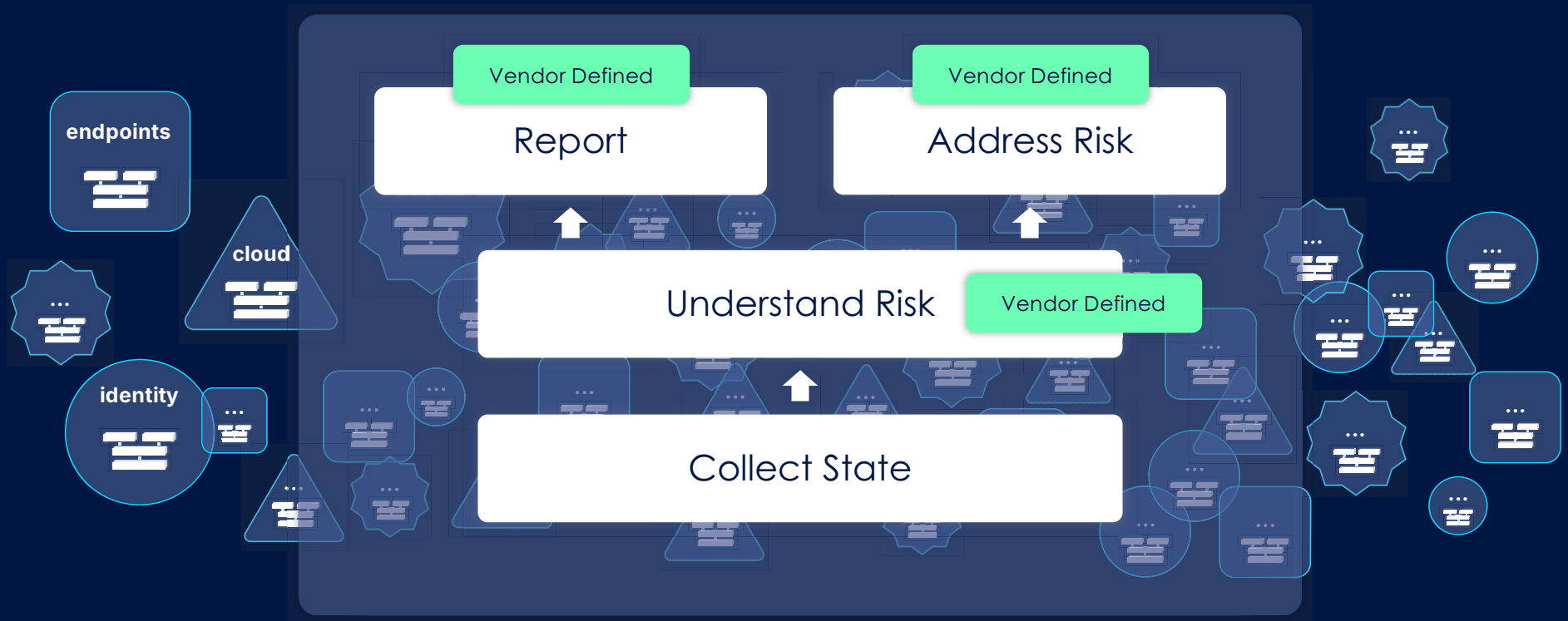
Why is it so hard to understand our threat exposure?



Why is it so hard to understand our threat exposure?



Why is it so hard to understand our threat exposure?



Siloed data lacks context, "intelligence" lives in a black box

What if instead...



Report, Address Risk

Real-time info, from any lens,
with custom workflows

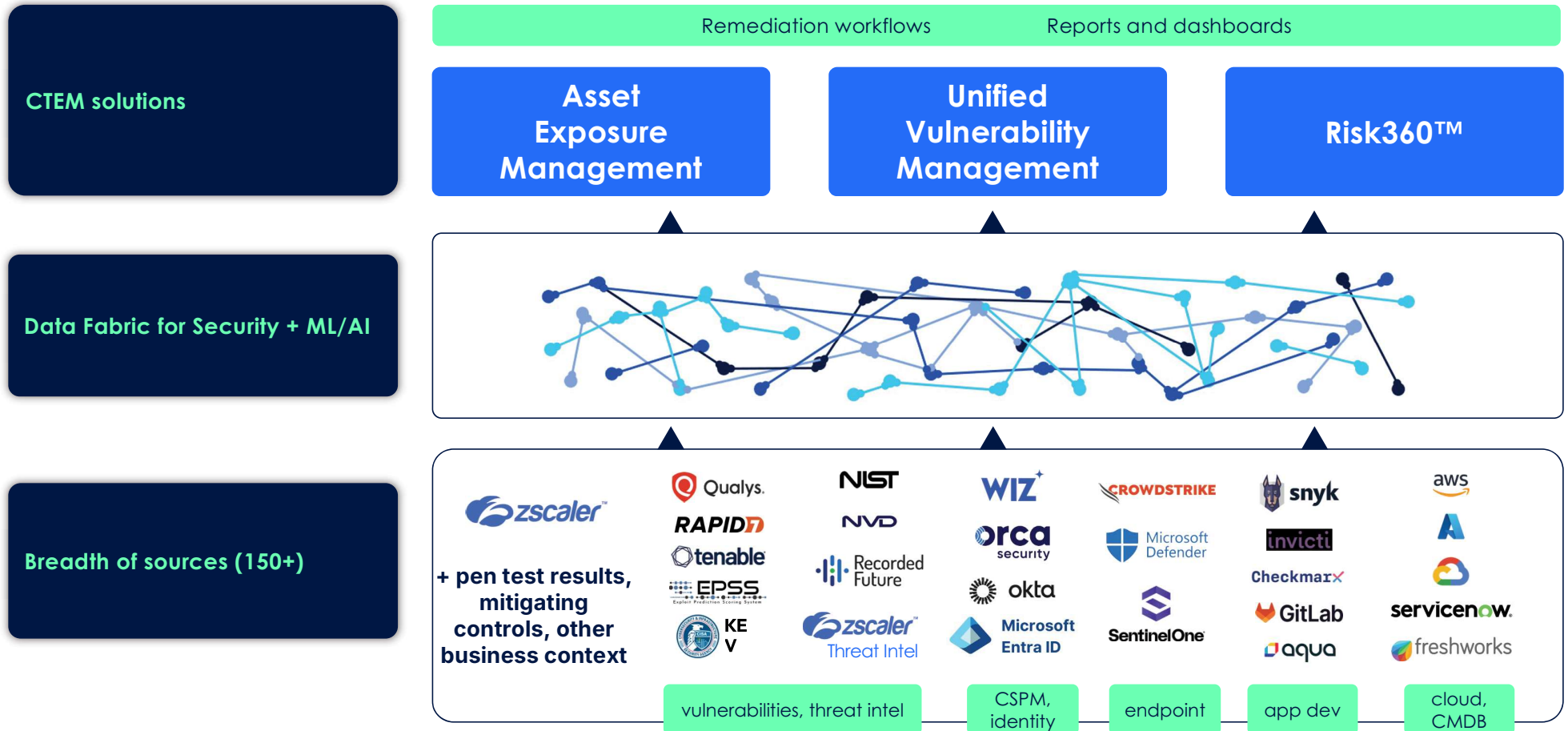
Understand Risk

Enrich and contextualize
full transparency and customization

Collect State

Any input

A deeper dive on data sources and CTEM solutions



Risk360

- Immediate insights into Zscaler misconfigurations and gaps
- Discovery of Internet-facing assets
- Cyber Risk Quantification based on Zscaler and third-party findings
- Compliance framework adherence and guidance



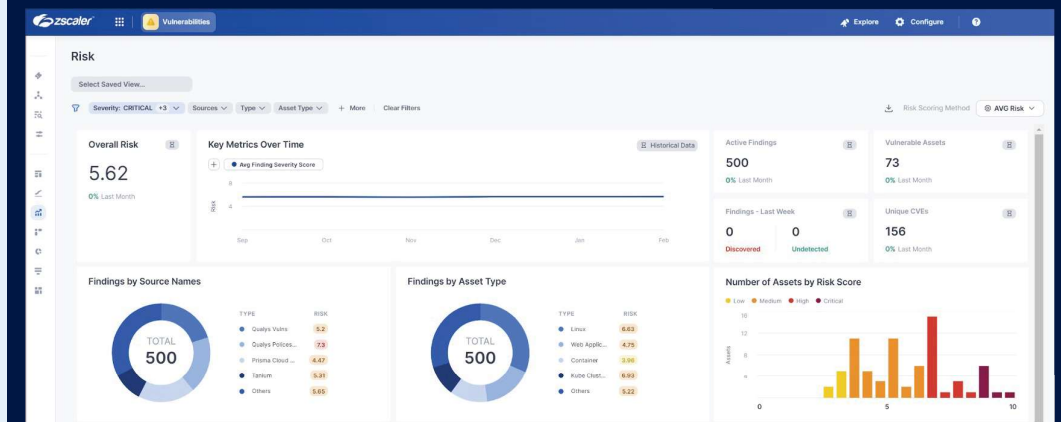
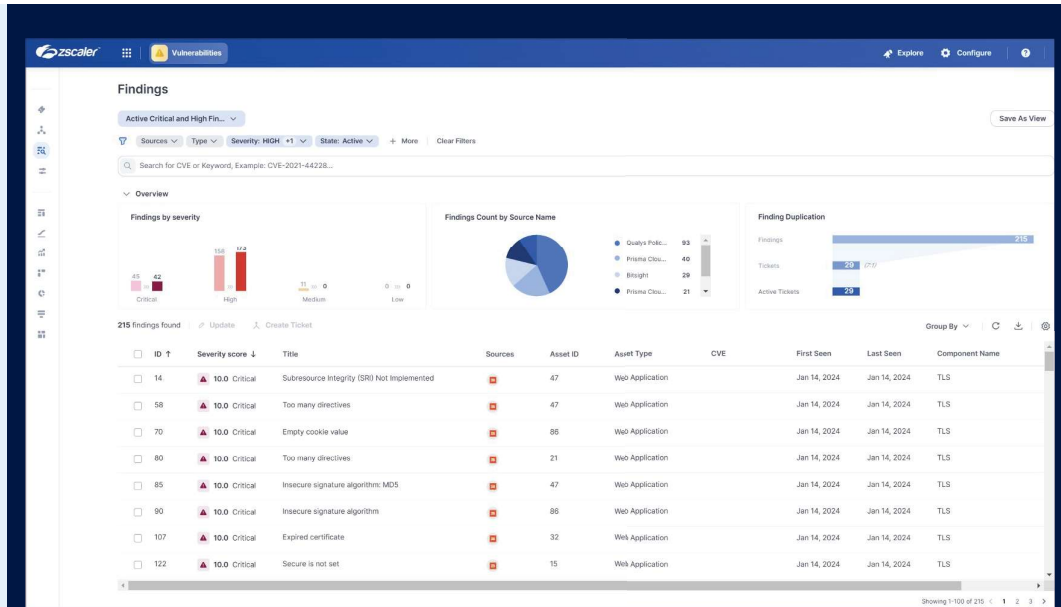
Contributing Factors to Organizational Risk Score

External Attack Surface: 23.81 | Compromise: 23.63 | Lateral Propagation: 12.20 | Data Loss: 21.71

Factor	Category	Your Score ↓	Last 30 Days	Entities	Licensed?	Recommended Actions	Include
Exposed Servers (Services Exposed)	External Attack Surface	6.76 / 4.76			N	Investigate 263 exposed servers'...	<input checked="" type="checkbox"/>
DLP Policy Violations	Data Loss	3.03 / 3.05			N	Investigate user activity resulting in active DLP policy triggers.	<input checked="" type="checkbox"/>
Severe Botnet Infections Observed	Compromise	2.72 / 2.27			N	Quarantine infected machines.	<input checked="" type="checkbox"/>
Application Segments with Open Ports	Lateral Propagation	2.03 / 2.03			N	Restrict ports for private application segments where possible.	<input checked="" type="checkbox"/>
Unsecured SSL Traffic	Compromise	1.54 / 2.62			N	Enable inspection for 64.74% qualified SSL traffic.	<input checked="" type="checkbox"/>
Namespace Exposure on Internet	External Attack Surface	1.13 / 1.19			N	Rename namespace for 82 keyword based domains with ambiguous names to ...	<input checked="" type="checkbox"/>
Application Segmentation	Lateral Propagation	0.62 / 0.08			N	Disable application segments for 1737 unsegmented FQDNs.	<input checked="" type="checkbox"/>
Data Uploaded to Unsanctioned Application	Data Loss	0.92 / 4.57			N	Investigate users uploading data to unsanctioned apps. Consider labeling ...	<input checked="" type="checkbox"/>
Risky Application Usage	Data Loss	0.71 / 3.05			N	Investigate the business use case for access to risky SaaS applications.	<input checked="" type="checkbox"/>
USBA	Data Loss	0.33 / 2.13			N	Investigate users flagged with these alerts and take necessary actions.	<input checked="" type="checkbox"/>

Unified Vulnerability Management

- A synthesized view of all your exposures
- Exposures prioritized by your risk factors and mitigating controls
- Detailed recommendations for remediation
- Automated workflows with two-way ticket reconciliation



Vielen Dank

“never trust always verify”

