/ PROGRAM BRIEF

Zscaler Security and Risk Assessment

Manage and Reduce Real Cyber Risk

The Security and Risk Assessment (SRA) takes a deep look at your organization's security strategies and capabilities, and ensures that the Zscaler platform's features support a valid and required outcome.

About the Zscaler CISO organization

The Zscaler CISO team is comprised of security practitioners and former Zscaler customer CISOs. They bring real-world experience delivering security programs and improvement to organizations, and in this engagement go beyond simple deployment to focus on customer consumption of Zscaler services.

Who it's for

The Security and Risk Assessment (SRA) is designed for a customer CISO or head of information security who owns or is implementing an organization's current or future security strategy, and considering:

- Cost/resource justification
- Complementary or non-technical control coverage
- Control/compliance relationships
- Alignment to business security goals

Deliverables

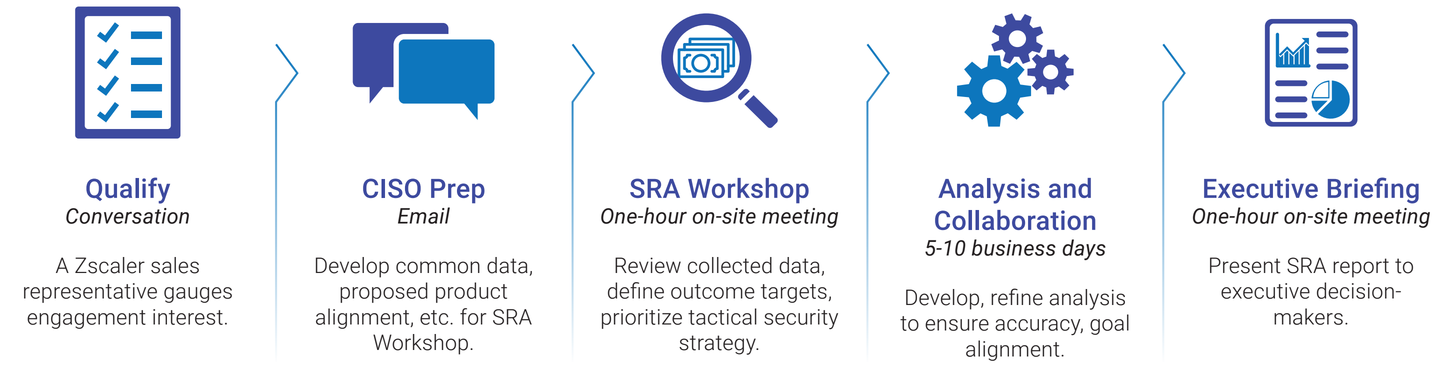
The SRA provides a roadmap for successful security outcomes based on objectives, priorities, and targets developed during interviews, and is based in part on the CISO team's security expertise. This roadmap shares sample success indicators, and highlights key components needed to deliver that success, including configurations, operational processes, other technologies, and Zscaler component deployment. For reference, the SRA also provides a comprehensive view of security outcomes delivered by the broader Zscaler platform services.

Benefits

SRA customers benefit from an enhanced understanding of how Zscaler helps them meet (and exceed) security requirements and goals, and allows for a much closer relationship with the platform. The SRA provides:

- Clear alignment of security/network spend against strategy
- Well-defined success criteria for Zscaler outcomes
- Metrics for maximum value delivery, and assurance of maximum risk reduction vs cost

Zscaler Security and Risk Assessment engagement workflow



Qualify
Conversation

A Zscaler sales representative gauges engagement interest.

CISO Prep
Email

Develop common data, proposed product alignment, etc. for SRA Workshop.

SRA Workshop
One-hour on-site meeting

Review collected data, define outcome targets, prioritize tactical security strategy.

Analysis and Collaboration
5-10 business days

Develop, refine analysis to ensure accuracy, goal alignment.

Executive Briefing
One-hour on-site meeting

Present SRA report to executive decision-makers.

Process and timing

Through an on-site or virtual SRA Workshop with the security leadership team, the Zscaler CISO team will work to assess a customer's level of engagement with the various outcomes supported by the platform, including existing technology, teams and processes. The CISO team then compiles its findings and delivers an SRA Report deck and reference for the customer.

The Security and Risk Assessment approach

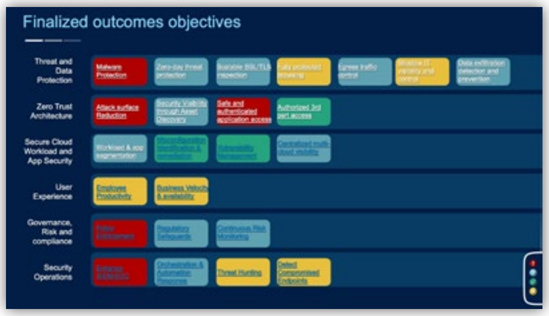
- We qualify your willingness to participate and provide essential insight into your security program.
- We provide clear insight/background into all of our counsel.
- We provide clear transparency on how we use your information.
- Results are easily understood and provide value long after deployment is complete.
- Output can easily be turned into a novel security program or integrated into an existing one.

The Security and Risk Assessment – possible outcomes

The Zscaler Zero Trust Exchange cloud platform enables digital transformation, letting enterprises secure internet traffic, secure access to apps, secure workloads, and preserve user experience. But such innovative security controls are worthless unless they support business objectives. SRA modelling ties Zscaler security services to specific business outcomes. The SRA gives customers a tool for assessing both security standards in terms of business priorities.

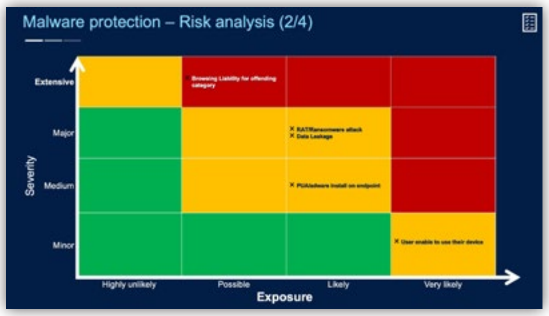
As part of the SRA, each service element of the Zscaler Zero Trust Exchange – and each feature of each of those elements – is assessed for security delivery outcome. Those security targets are based on the NIST Cyber Security Framework, and the SRA provides detailed contextual information, including justification, risks managed/reduced, common operational requirements, and success criteria. The delivered SRA analysis can then contribute to a broader security Target Operating Model.

Sample Output

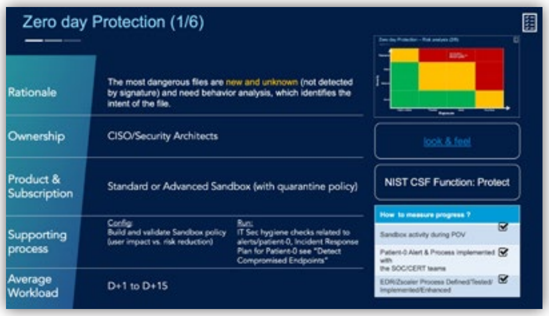


Finalized outcomes objectives

Threat and Data Protection	Malware Protection	Zero-day threat protection	Scalable SSL/TLS inspection	Fully protected browsing	Egress traffic control	Shadow IT visibility and control	Data exfiltration detection and prevention
Zero Trust Architecture	Attack surface Reduction	Security Visibility through Asset Discovery	Safe and authenticated application access	Authorized 3rd part access			
Secure Cloud Workload and App Security	Workload & app segmentation	Misconfiguration identification & remediation	Vulnerability Management	Centralized multi-cloud visibility			
User Experience	Employee Productivity	Business Velocity & availability					
Governance, Risk and compliance	Policy Enforcement	Regulatory Safeguards	Continuous Risk Monitoring				
Security Operations	Enhance SIEM/SOC	Orchestration & Automation Response	Threat Hunting	Detect Compromised Endpoints			



Malware protection – Risk analysis (2/4)



Zero day Protection (1/6)

Rationale	The most dangerous files are new and unknown (not detected by signature) and need behavior analysis, which identifies the intent of the file.	
Ownership	CISO/Security Architects	
Product & Subscription	Standard or Advanced Sandbox (with quarantine policy)	
Supporting process	Config: Build and validate Sandbox policy (user impact vs. risk reduction)	Run: IT Sec hygiene checks related to alerts/patient-0, Incident Response Plan for Patient-0 see "Detect Compromised Endpoints"
Average Workload	D+1 to D+15	

look & feel

NIST CSF Function: Protect

How to measure progress ?	
Sandbox activity during POV	☑
Patient-0 Alert & Process implemented with the SOC/CERT teams	☑
EDR/Zscaler Process Defined/Tested/ Implemented/Enhanced	☑

Possible outcomes

Category	Outcome	CSF Function	Z-Service Mapping
Threat and data protection	Malware protection	Protect	ZIA
	Zero-day threat prevention	Protect	ZIA, CS
	Scalable SSL/TLS inspection	Protect	ZIA
	Fully protected browsing	Protect	ZIA, CBI
	Egress traffic control	Protect/Detect	CF
	Shadow IT visibility and control	Identify/Protect/Detect	ZIA, CASB, CBI
	Data exfiltration detection and prevention	Protect/Detect	ZIA, DLP, CASB
Zero Trust Architecture	Attack surface reduction/ De-perimeterization	Protect	ZPA, ZIA
	Security visibility through asset discovery	Identify/Respond	ZPA
	Safe and authenticated application access	Protect	ZPA
	Authorized 3rd party secure access and control	Protect	ZPA, B2B
Cloud workload & application security	Workload and application segmentation	Identify/Protect	ZWS
	Misconfiguration identification and remediation	Identify/Protect/Respond	CSPM
	Vulnerability management	Identify/Protect/Detect	CSPM
	Centralized multi-cloud visibility	Identify/Detect/Respond	CSPM, ZWS, CASB
User experience	Employee productivity	Identify	ZDX, ZPA, ZIA
	Business velocity and operational availability	Protect	ZDX, ZPA, ZIA
Governance, risk and compliance	Policy enforcement	Protect	ZIA, ZPA, CASB, DLP, CF
	Regulatory compliance safeguards	Identify/Protect	ZIA, ZPA, CASB, DLP, CF, CSPM, ZWS
	Continuous risk monitoring	Detect/Respond	All
Security operations	Threat hunting and response	Detect/Respond	NSS, LSS, ZIA, CSPM
	Orchestration and automation response	Detect/Respond	NSS, LSS, ZWS, CSPM
	Security event management enhancement	Detect/Respond	NSS, LSS, CSPM, ZWS
	Detect compromised endpoints	Detect/Respond	NSS, ZIA

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 SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com