Assessment Overview

Zero Trust Maturity Model (ZTMM) assessment results

Assessment of <*CompanyName*> by Andrew Aken
Last updated on 2021-06-06 19:16:00

Current Zero Trust maturity level: 2.00

Summary of scores

Domain	Number of items at each assessment level								Total Items	Current ZTMM Assessment	Estimated Current Risk Reduction
	0	1	2	3	4	5	N/A	Unscored			
Identity / People	0	2	6	3	12	2	1	0	26	3.24	% 31.25
Data	4	4	0	5	7	0	0	0	20	2.00	% 20.22
Network	5	1	1	2	4	1	0	0	14	2.00	% 22.03
Workload / Applications	4	2	6	4	8	1	0	0	25	2.00	% 25.07
Devices / Endpoints	4	0	3	5	10	3	0	0	25	2.00	% 39.95
Visibility & Analytics	0	0	1	2	8	0	0	0	11	3.64	% 46.08
Orchestration & Automation	5	1	1	2	1	0	0	0	10	2.00	% 8.31
Total	22	10	18	23	50	7	1	0	131	2.00	% 27.56

Zero Trust Maturity Across All Domains
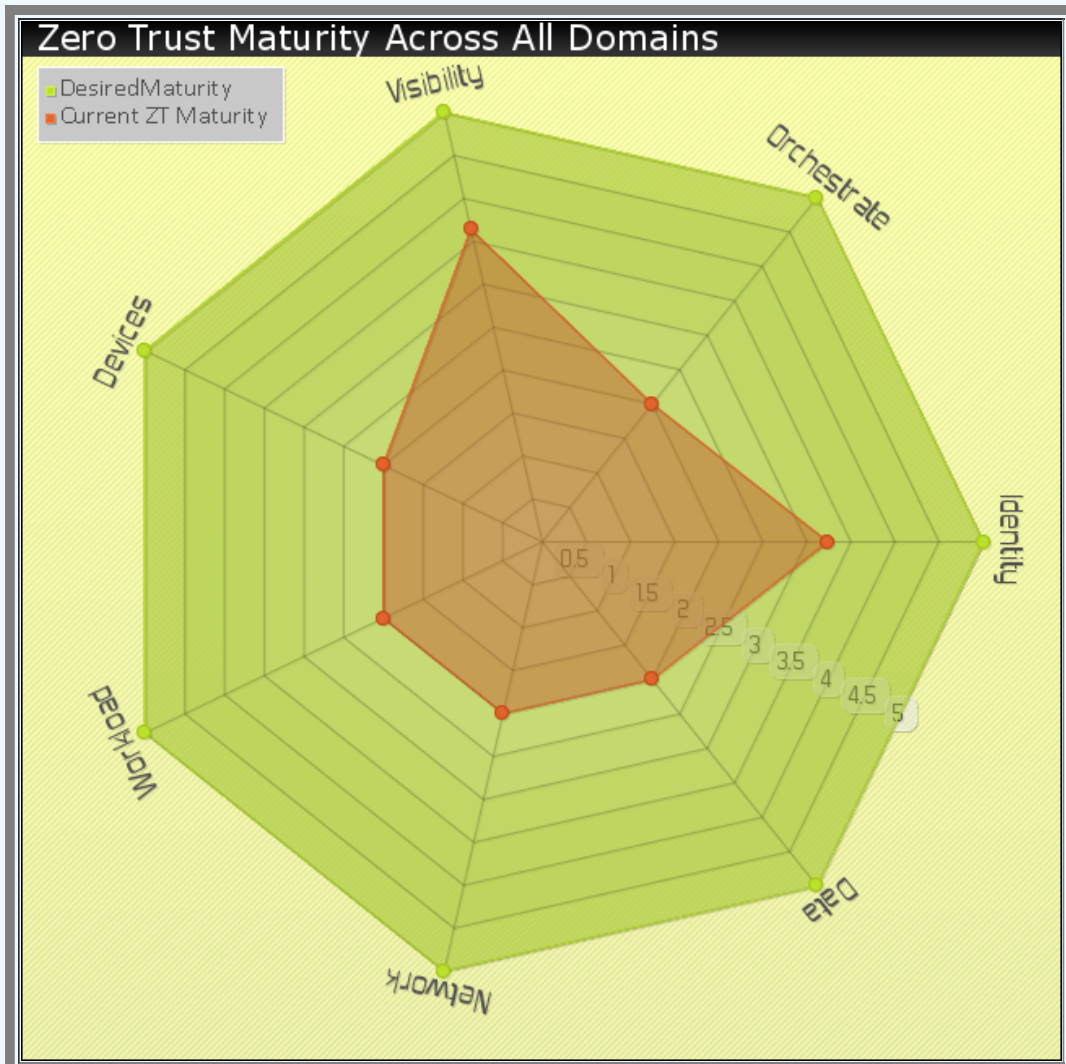
Comparative Analytics

Not enough data available at this time

Comparative Analytics - by Industry

Not enough data available at this time

Comparative Analytics - by Organizational Size

Not enough data available at this time

The overall ZT maturity assessment value is the minimum maturity level of any of the 5 pillars (Identity, Data, Network, Workload, and Devices) if any of the maturity levels of the pillars is less than 3. This is because maturity levels 1-2 cover the foundational elements of cyber security and they must be implemented before the rest of the journey towards higher levels of Zero Trust maturity can yield truly meaningful results. Once each of the pillars has achieved at least a level 3 maturity, the overall ZT maturity will be the average of the maturity levels across all 7 domains of ZT (the pillars plus visibility & analytics and orchestration & automation).

Identity / People

Summary for the 'Identity / People' domain's Zero Trust maturity

Maturity level: 3.24

Summary of scores

Item Maturity Level	Item Count	Maturity Scores								Average	Min	Max
		0	1	2	3	4	5	N/A	Unscored			
1	4	0	0	0	0	3	0	1	0	4.00	4	4
2	3	0	0	0	0	3	0	0	0	4.00	4	4
3	11	0	0	2	2	5	2	0	0	3.64	2	5
4	4	0	1	2	0	1	0	0	0	2.25	1	4
5	4	0	1	2	1	0	0	0	0	2.00	1	3
Total	26	0	2	6	3	12	2	1	0	3.24		

Assessment Responses

Item ID	Item Maturity	Assessment Item/Control	Maturity Level	Risk Reduction	Notes/Source
ID_01	1	Security awareness training	N/A		
ID_02	1	Lifecycle management of system and application accounts (creation, use, dormancy, & deletion)	4	%1.36	
ID_03	1	Self-service password resets and password replication	4	%0.68	
ID_04	1	Standardized naming convention for account information	4	%0.68	Just got it operational
ID_11	2	Analytics technologies used to improve visibility into user login behavior and anomalies	4	%2.72	
ID_12	2	Processes and tools to track/control/prevent/correct the use, assignment, and configuratoin of administrative privileges	4	%2.72	
ID_13	2	Access management systems to provide authentication for cloud-based applications	4	%1.36	
ID_21	3	Role-Based Access Controls (RBAC) or Attribute-Based Access Controls (ABAC) implemented	4	%4.08	
ID_22	3	Least Privilege is implemented	3		
ID_23	3	Resource permissions provisioned to users or roles/groups	4	%2.04	
		•••			
ID_53	5	Real-time analysis of device, location, and user behavior for continuous risk-based authentication	2		
ID_54	5	Implemented Secure Access Service Edge (SASE) technologies	2		

Data

Summary for the 'Data' domain's Zero Trust maturity

Maturity level: 2.00

Summary of scores

Item Maturity Level	Item Count	Maturity Scores								Average	Min	Max
		0	1	2	3	4	5	N/A	Unscored			
1	2	0	0	0	0	2	0	0	0	4.00	4	4
2	5	0	0	0	2	3	0	0	0	3.60	3	4
3	7	2	2	0	2	1	0	0	0	1.71	0	4
4	4	2	1	0	0	1	0	0	0	1.25	0	4
5	2	0	1	0	1	0	0	0	0	2.00	1	3
Total	20	4	4	0	5	7	0	0	0	2.35		

Assessment Responses

Item ID	Item Maturity	Assessment Item/Control	Maturity Level	Risk Reduction	Notes/Source
Data_11	1	Centralized repositories for all sensitive data	4	%3.24	
Data_12	1	Processes and tools to properly back up critical information and test for the ability to recover the data	4	%4.85	
Data_21	2	Implemented data classification with tagging by sensitivity, criticality, location, device, and hosting models	4	%2.43	
Data_22	2	Encrypt all sensitive data at rest	3		
Data_23	2	Data access governed by perimeter controls	3		

. . .

| Data_52 | 5 | DLP systems in place with the ability to track where the data is | 1 | | |

Network

Summary for the 'Network' domain's Zero Trust maturity

Maturity level: 2.00

Summary of scores

Item Maturity Level	Item Count	Maturity Scores								Average	Min	Max
		0	1	2	3	4	5	N/A	Unscored			
1	1	0	0	0	0	1	0	0	0	4.00	4	4
2	5	1	0	0	1	2	1	0	0	3.20	0	5
3	2	0	0	1	0	1	0	0	0	3.00	2	4
4	5	3	1	0	1	0	0	0	0	0.80	0	3
5	1	1	0	0	0	0	0	0	0	0.00	0	0
Total	14	5	1	1	2	4	1	0	0	2.14		

Assessment Responses

Item ID	Item Maturity	Assessment Item/Control	Maturity Level	Risk Reduction	Notes/Source
Net_11	1	Limitations and controls on network ports, protocols, and services	4	%4.97	
Net_21	2	All publicly accessible on-premises systems placed in a demilitarized zone (DMZ)	3		
Net_22	2	Ingress dynamic filtering with packet inspection	0		

. . .

| Net_14 | 5 | Ability to inspect encrypted packets at the border and system level | 0 | | |

Workload / Applications

Summary for the 'Workload / Applications' domain's Zero Trust maturity

Maturity level: 2.00

Summary of scores

Item Maturity Level	Item Count	Maturity Scores								Average	Min	Max
		0	1	2	3	4	5	N/A	Unscored			
1	1	0	0	0	0	1	0	0	0	4.00	4	4
2	8	1	0	2	1	3	1	0	0	3.00	0	5
3	10	1	0	4	2	3	0	0	0	2.60	0	4
4	3	1	0	0	1	1	0	0	0	2.33	0	4
5	3	1	2	0	0	0	0	0	0	0.67	0	1
Total	25	4	2	6	4	8	1	0	0	2.52		

Assessment Responses

Item ID	Item Maturity	Assessment Item/Control	Maturity Level	Risk Reduction	Notes/Source
App_11	1	Standardized application development methodology	4	%0.67	

. . .

Item ID	Item Maturity	Assessment Item/Control	Maturity Level	Risk Reduction	Notes/Source
App_51	5	User and resource access segmented for each workload (application microsegmentation)	1		
App_52	5	Web browsing through Remote Browser Isolation (RBI)	0		
App_53	5	Dynamic controls and in-session monitoring for all applications	1		

Devices / Endpoints

Summary for the 'Devices / Endpoints' domain's Zero Trust maturity

Maturity level: 2.00

Summary of scores

Item Maturity Level	Item Count	Maturity Scores								Average	Min	Max
		0	1	2	3	4	5	N/A	Unscored			
1	1	0	0	0	0	0	1	0	0	5.00	5	5
2	8	0	0	0	2	5	1	0	0	3.88	3	5
3	9	2	0	0	2	4	1	0	0	3.00	0	5
4	5	2	0	1	1	1	0	0	0	1.80	0	4
5	2	0	0	2	0	0	0	0	0	2.00	2	2
Total	25	4	0	3	5	10	3	0	0	3.04		

Assessment Responses

Item ID	Item Maturity	Assessment Item/Control	Maturity Level	Risk Reduction	Notes/Source
Device_11	1	Anti-malware installed on all applicable endpoints and servers	5	%3.66	
Device_21	2	Bring your own device (BYOD) security policy	3		

. . .

Item ID	Item Maturity	Assessment Item/Control	Maturity Level	Risk Reduction	Notes/Source
Device_44	4	Real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities	4	%4.68	
Device_45	4	Unauthorized devices are blocked and alerts raised if they try to connect to corporate assets	3		
Device_51	5	Access control granted based upon device risk for corporate and BYOD devices	2		
Device_52	5	Cross-system and infrastructure controls utilized to prevent unauthorized communications	2		Estimated

Visibility & Analytics

Summary for the 'Visibility & Analytics' domain's Zero Trust maturity

Maturity level: <u>3.64</u>

Summary of scores

Item Maturity Level	Item Count	Maturity Scores								Average	Min	Max
		0	1	2	3	4	5	N/A	Unscored			
1	1	0	0	0	0	1	0	0	0	4.00	4	4
2	3	0	0	0	0	3	0	0	0	4.00	4	4
3	3	0	0	0	0	3	0	0	0	4.00	4	4
4	3	0	0	1	1	1	0	0	0	3.00	2	4
5	1	0	0	0	1	0	0	0	0	3.00	3	3
Total	11	0	0	1	2	8	0	0	0	3.64		

Assessment Responses

Item ID	Item Maturity	Assessment Item/Control	Maturity Level	Risk Reduction	Notes/Source
Vis_11	1	Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack	4	%5.76	
Vis_21	2	Information Technology Infrastructure Library (ITIL) or IT Service Management (ITSM) based ticketing systems	4	%2.88	

. . .

Vis_51	5	User and Entity Behavior Analytics (UEBA) tools	3		

Orchestration & Automation

Summary for the 'Orchestration & Automation' domain's Zero Trust maturity

Maturity level: <u>2.00</u>

Summary of scores

Item Maturity Level	Item Count	Maturity Scores								Average	Min	Max
		0	1	2	3	4	5	N/A	Unscored			
1	1	0	0	0	0	1	0	0	0	4.00	4	4
2	1	1	0	0	0	0	0	0	0	0.00	0	0
3	2	1	0	0	1	0	0	0	0	1.50	0	3
4	4	2	1	1	0	0	0	0	0	0.75	0	2
5	2	1	0	0	1	0	0	0	0	1.50	0	3
Total	10	5	1	1	2	1	0	0	0	1.30		

Assessment Responses

Item ID	Item Maturity	Assessment Item/Control	Maturity Level	Risk Reduction	Notes/Source
Orch_11	1	Incident response infrastructure for discovering an attack, containing the damage, eradicating the attacker's presence, and restoring network & system integrity	4	%8.31	

. . .

Orch_52	5	Security Orchestration, Automation, & Response (SOAR) systems	3		