A Story about a Strategy for Aligning Security and the Business

PROJECT ZERO TRUST

GEORGE FINNEY

Foreword by John Kindervag

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada and the United Kingdom.

ISBN: 978-1-119-88484-2
ISBN: 978-1-119-88485-9 (ebk.)
ISBN: 978-1-119-88486-6 (ebk.)

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

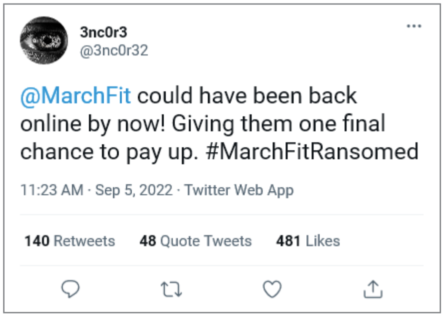
For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

If you believe you’ve found a mistake in this book, please bring it to our attention by emailing our Reader Support team at wileysupport@wiley.com with the subject line “Possible Book Errata Submission.”

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Control Number: 2022938397

Cover images: © Alhovik/Shutterstock; © venimo/Shutterstock
Cover design: Wiley



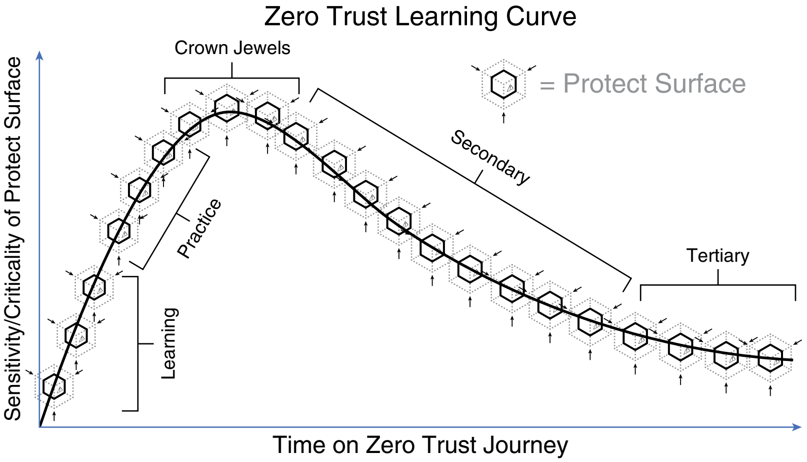
3nc0r3
@3nc0r32

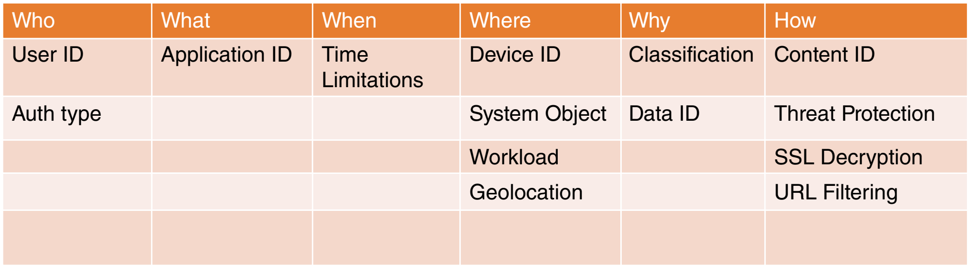
@MarchFit could have been back online by now! Giving them one final chance to pay up. #MarchFitRansomed

11:23 AM · Sep 5, 2022 · Twitter Web App

140 Retweets 48 Quote Tweets 481 Likes

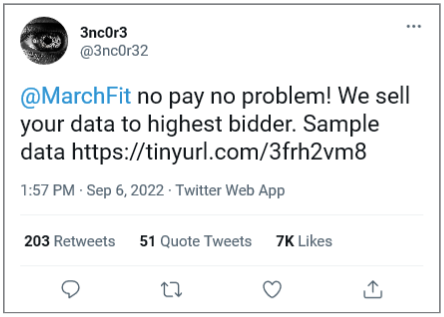
A tweet from the cybercriminal 3nc0r3 publicly threatening MarchFit and confirming rumors of a cyberattack


Zero Trust Learning Curve
Crown Jewels
= Protect Surface
Secondary
Tertiary
Practice
Learning
Sensitivity/Criticality of Protect Surface
Time on Zero Trust Journey



Who	What	When	Where	Why	How
User ID	Application ID	Time Limitations	Device ID	Classification	Content ID
Auth type			System Object	Data ID	Threat Protection
			Workload		SSL Decryption
			Geolocation		URL Filtering

John Kindervag's Kipling Method for developing security policies for individual protect surfaces
Courtesy of ON2IT



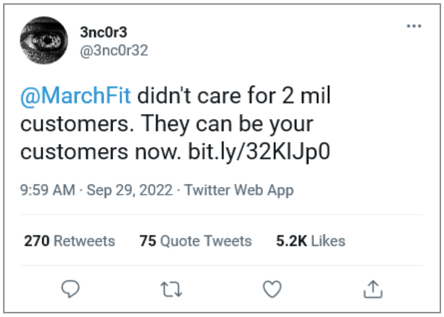
3nc0r3
@3nc0r32

@MarchFit no pay no problem! We sell your data to highest bidder. Sample data https://tinyurl.com/3frh2vm8

1:57 PM · Sep 6, 2022 · Twitter Web App

203 Retweets 51 Quote Tweets 7K Likes

Tweet from the cybercriminal 3nc0r3 sharing a link to sample data online to prove that he had actually stolen MarchFit information



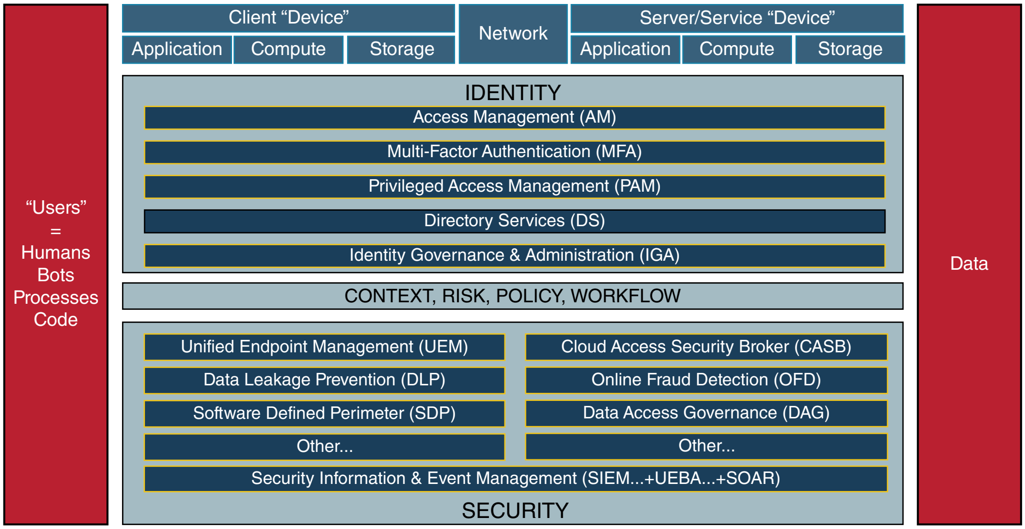
3nc0r3
@3nc0r32

@MarchFit didn't care for 2 mil customers. They can be your customers now. bit.ly/32KIJp0

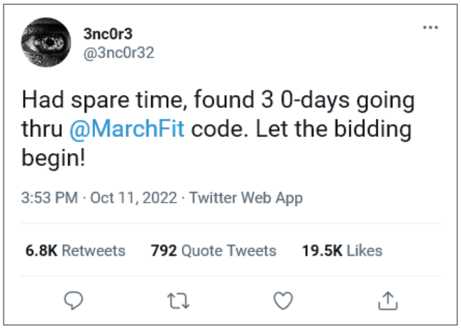
9:59 AM · Sep 29, 2022 · Twitter Web App

270 Retweets **75** Quote Tweets **5.2K** Likes

Tweet from 3nc0r3 publicly posting all of MarchFit’s stolen data in an attempt to embarrass the company after they refused to pay the ransom


"Users"
=
Humans
Bots
Processes
Code
Client "Device"
Application
Compute
Storage
Network
Server/Service "Device"
Application
Compute
Storage
IDENTITY
Access Management (AM)
Multi-Factor Authentication (MFA)
Privileged Access Management (PAM)
Directory Services (DS)
Identity Governance & Administration (IGA)
CONTEXT, RISK, POLICY, WORKFLOW
Unified Endpoint Management (UEM)
Cloud Access Security Broker (CASB)
Data Leakage Prevention (DLP)
Online Fraud Detection (OFD)
Software Defined Perimeter (SDP)
Data Access Governance (DAG)
Other...
Other...
Security Information & Event Management (SIEM...+UEBA...+SOAR)
SECURITY
Data

Identity-defined security reference architecture
Courtesy Identity Defined Security Alliance

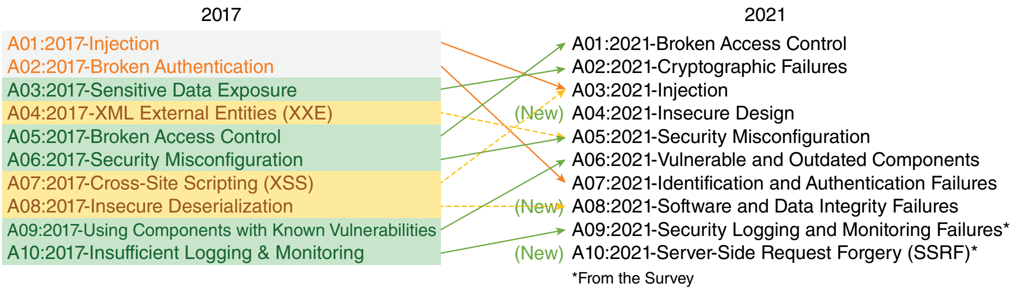

3nc0r3
@3nc0r32

Had spare time, found 3 0-days going thru @MarchFit code. Let the bidding begin!

3:53 PM · Oct 11, 2022 · Twitter Web App

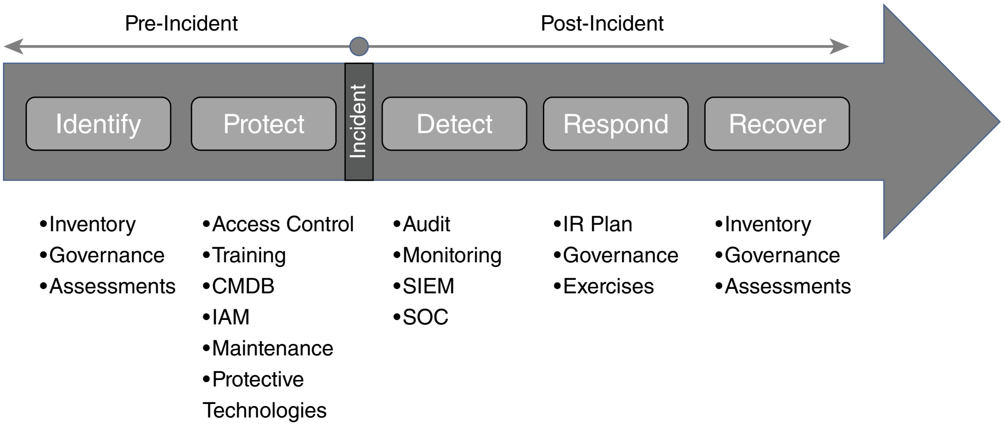
6.8K Retweets 792 Quote Tweets 19.5K Likes

Tweet from the hacker 3nc0r3 claiming that he had found three zero days in MarchFit's code offering to sell to the highest bidder.


2017
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
*From the Survey

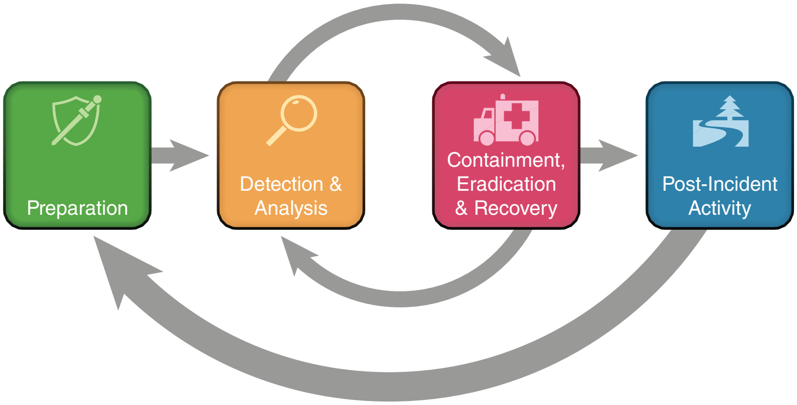
OWASP Top 10 vulnerabilities

SOURCE: OWASP Top Ten / OWASP Foundation, Inc.



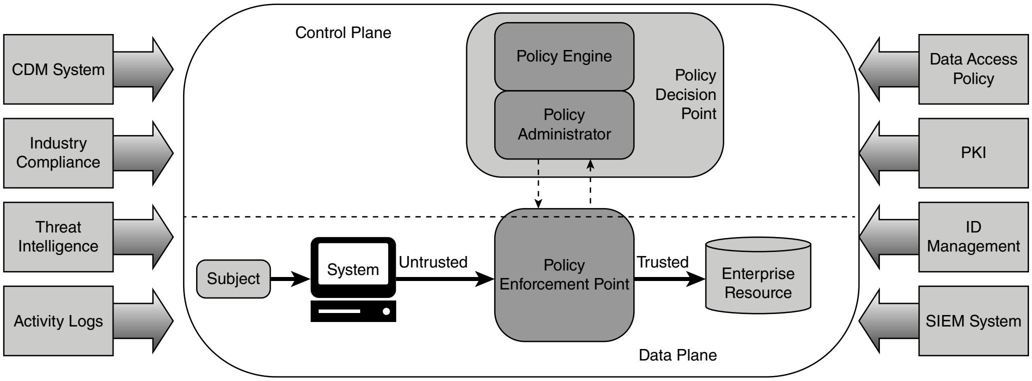
NIST Cybersecurity Framework

SOURCE: Adapted from NIST Cybersecurity framework

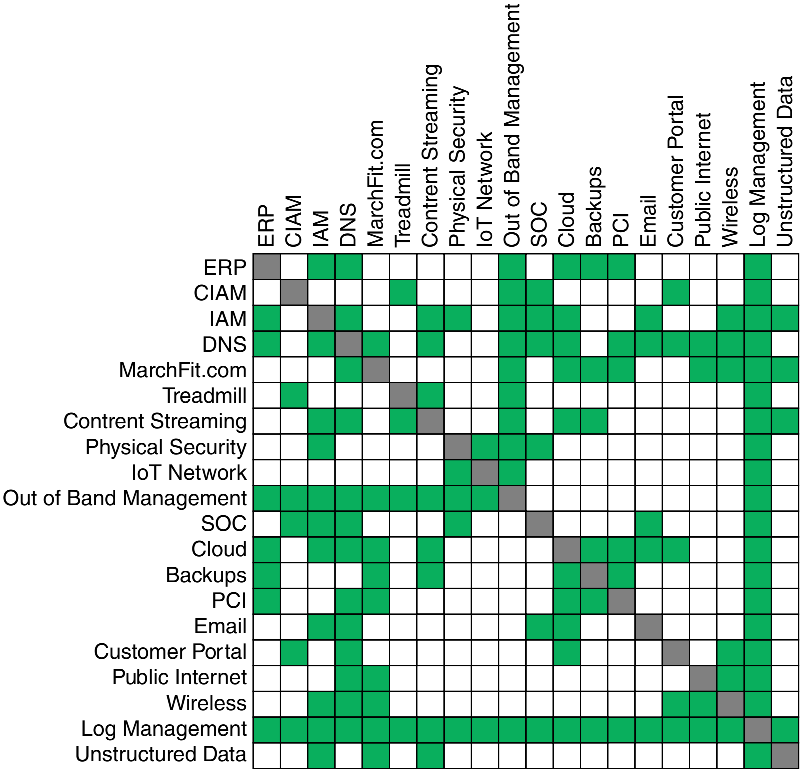


NIST SP 800-61 Incident Response Lifecycle

SOURCE: P Cichonski et al., (2012)/NIST/Public domain

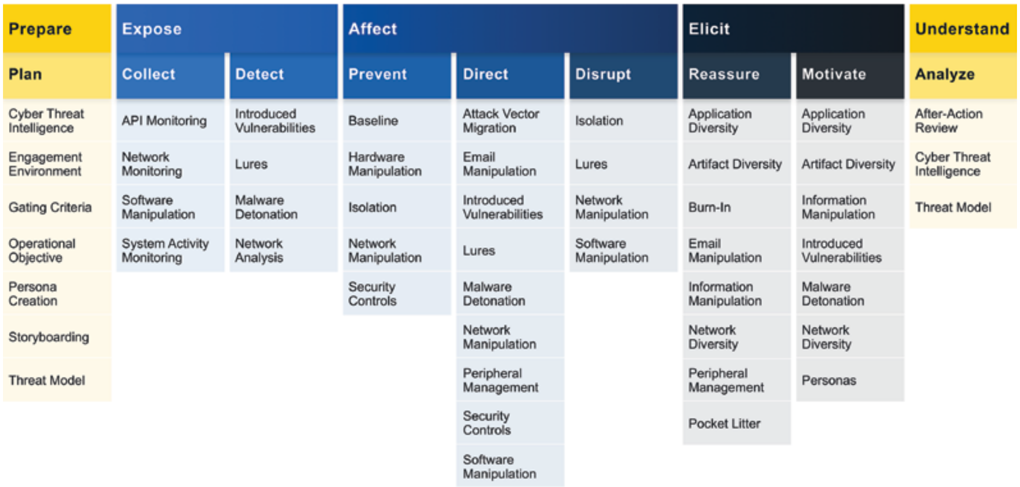


NIST SP 800-207 Core Zero Trust logical components



	ERP	CIAM	IAM	DNS	MarchFit.com	Treadmill	Contrent Streaming	Physical Security	IoT Network	Out of Band Management	SOC	Cloud	Backups	PCI	Email	Customer Portal	Public Internet	Wireless	Log Management	Unstructured Data
ERP	■		🟩	🟩						🟩		🟩	🟩	🟩					🟩	
CIAM		■				🟩				🟩	🟩					🟩			🟩	
IAM	🟩		■	🟩			🟩	🟩		🟩	🟩	🟩			🟩			🟩	🟩	🟩
DNS	🟩		🟩	■	🟩		🟩			🟩	🟩	🟩		🟩	🟩	🟩	🟩	🟩	🟩	
MarchFit.com				🟩	■					🟩		🟩	🟩	🟩			🟩	🟩	🟩	🟩
Treadmill		🟩				■	🟩			🟩									🟩	
Contrent Streaming			🟩	🟩		🟩	■			🟩		🟩	🟩						🟩	🟩
Physical Security			🟩					■	🟩	🟩	🟩								🟩	
IoT Network								🟩	■	🟩									🟩	
Out of Band Management	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	■									🟩	
SOC		🟩	🟩	🟩				🟩			■				🟩				🟩	
Cloud	🟩		🟩	🟩	🟩		🟩					■	🟩	🟩	🟩	🟩			🟩	
Backups	🟩				🟩		🟩					🟩	■	🟩					🟩	
PCI	🟩			🟩	🟩							🟩	🟩	■					🟩	
Email			🟩	🟩							🟩	🟩			■				🟩	
Customer Portal		🟩		🟩								🟩				■		🟩	🟩	
Public Internet				🟩	🟩												■	🟩	🟩	
Wireless			🟩	🟩	🟩											🟩	🟩	■	🟩	
Log Management	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	■	🟩
Unstructured Data			🟩		🟩		🟩												🟩	■

Transaction Flow Map One—All the protect surfaces are defined, and the transaction flow matrix can show which protect surfaces are allowed to communicate with one another.



Prepare	Expose		Affect			Elicit		Understand
Plan	Collect	Detect	Prevent	Direct	Disrupt	Reassure	Motivate	Analyze
Cyber Threat Intelligence	API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity	After-Action Review
Engagement Environment	Network Monitoring	Lures	Hardware Manipulation	Email Manipulation	Lures	Artifact Diversity	Artifact Diversity	Cyber Threat Intelligence
Gating Criteria	Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation	Threat Model
Operational Objective	System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation	Introduced Vulnerabilities	
Persona Creation			Security Controls	Malware Detonation		Information Manipulation	Malware Detonation	
Storyboarding				Network Manipulation		Network Diversity	Network Diversity	
Threat Model				Peripheral Management		Peripheral Management	Personas	
				Security Controls		Pocket Litter		
				Software Manipulation				

MITRE Engage Matrix—The Engage Matrix depicts five stages of creating an active defense to disrupt cyberattacks using deception technologies.

Appendix A
Zero Trust Design Principles and Methodology

The Four Zero Trust Design Principles

1. **Define business outcomes**: Ask the question "What is the business trying to achieve?" This aligns Zero Trust to the grand strategic outcomes of the organization and makes cybersecurity a business enabler instead of the business inhibitor that it is often seen as today.
2. **Design from the inside out**: Start with the data, applications, assets, and services (DAAS) elements and the protect surfaces that need protection and design outward from there.
3. **Determine who or what needs access**: Determine who needs to have access to a resource in order to get their job done. It is very common to give too many users too much access to sensitive data for no business reason.
4. **Inspect and log all traffic**: All traffic going to and from a protect surface must be inspected and logged for malicious content and unauthorized activity, up through Layer 7.

The Five-Step Zero Trust Design Methodology

1. **Define the protect surface**: Identify the DAAS elements: data, applications, assets, and services, that you want to protect.
2. **Map the transaction flows**: Zero Trust is a system, and in order to secure the system, understanding how the network works is imperative to a successful Zero Trust deployment. The mapping of the transaction flows to and from the protect surface shows how various DAAS components interact with other resources on your network and, therefore, where to place the proper controls. The way traffic moves across the network, specific to the data in the protect surface, determines the design.
3. **Build a Zero Trust architecture**: Part of the magic of the five-step model is that the first two steps will illuminate the best way to design the Zero Trust architecture. The architectural elements cannot be predetermined. Each Zero Trust environment is tailor-made for each protect surface. A good rule of thumb in design is to place the controls as close as possible to the protect surface.
4. **Create a Zero Trust policy**: Ultimately, instantiate Zero Trust as a Layer 7 Policy Statement. Therefore, it requires Layer 7 controls. Use the Kipling Method of Zero Trust policy writing to determine who or what can access your protect surface.
5. **Monitor and maintain the environment**: One of the design principles of Zero Trust is to inspect and log all traffic, all the way through Layer 7. The telemetry provided by this process will not just help prevent data breaches and other significant cybersecurity events, but will provide valuable security improvement insights. This means that each protect surface can become more robust and better protected over time. Telemetry from cloud, network, and endpoint controls can be analyzed using advances in behavioral analytics, machine learning, and artificial intelligence to stop attacks in real time and improve security posture over the long term.

Appendix B
Zero Trust Maturity Model

Because Zero Trust is a strategic initiative, it's important to benchmark your Zero Trust journey and measure your improvements over time. The Zero Trust Maturity Model documents improvements made to your individual Zero Trust environments. Designed using a standard Capability Maturity Model, the Zero Trust Maturity Model leverages the five-step methodology for implementing Zero Trust and should be used to measure the maturity of an individual protect surface containing a single DAAS element.

Step	**Initial (1)**	**Repeatable (2)**	**Defined (3)**	**Managed (4)**	**Optimized (5)**
	The initiative is undocumented and performed on an ad hoc basis with processes undefined. Success is dependent on individual efforts.	The process is documented and is predictably repeatable, using lessons learned in the initial phase.	Processes for success have been defined and documented.	Processes are monitored and controlled; efficacy is measurable.	The focus is on continuous optimization.
1. Define your protect surface. Determine which single DAAS element will be protected inside the defined protect surface.	The DAAS element is unknown or discovered manually; data classification is not done or is incomplete.	The use of automated tools to discover and classify DAAS elements has begun, but is not standardized.	Data classification training and processes have been introduced and are maturing; protect surface discovery is becoming automated.	New or updated DAAS elements are immediately discovered, classified, and assigned to the correct protect surface in an automated manner.	Discovery and classification processes are fully automated.

2. Map the transaction flows. The mapping of the transaction flows to and from the protect surface shows how various DAAS components interact with other resources on your network and, therefore, where to place the proper controls.	Flows are conceptualized based on interviews and workshops.	Traditional scanning tools and event logs are used to construct approximate flow maps.	A flow mapping process is in place. Automated tools are beginning to be deployed.	Automated tools create precise flow maps. All flow maps are validated with system owners.	Transaction flows are automatically mapped across all locations in real time.
3. Architect a Zero Trust environment. A Zero Trust architecture is designed based upon the protect surface and the interaction of resources based upon the flow maps.	With little visibility and an undefined protect surface, the architecture cannot be properly designed.	Protect surface is established based on current resources and priorities.	The basics of the protect surface enforcement is complete, including placing segmentation gateways in the appropriate places.	Additional controls are added to evaluate multiple variables (e.g., endpoint controls, SAAS, and API controls).	Controls are enforced using a combination of hardware and software capabilities.

4. Create Zero Trust policy. Create Zero Trust policy following the Kipling Method of Who, What, When, Where, Why, and How.	Policy is written at Layer 3.	Additional “who” statements are starting to be identified to address business needs; user IDs of applications and resources are known, but access rights are unknown.	The team works with the business to determine who or what should have access to the protect surface.	Custom user-specific elements are created and defined by policy, reducing policy space and number of users with access.	Layer 7 policy is written for granular enforcement; only known traffic and legitimate application communication are allowed.
5. Monitor and maintain. Telemetry from all controls in the protection chain are captured, analyzed, and used to stop attacks in real time and enhance defenses to create more robust protections over time.	Visibility into what is happening on the network is low.	Traditional SIEM or log repositories are available, but the process is still mostly manual.	Telemetry is gathered from all controls and is sent to a central data lake.	Machine learning tools are applied to the data lake for context into how traffic is used in the environment.	Data is incorporated from multiple sources and used to refine steps 1–4; alerts and analyses are automated.

Appendix C
Sample Zero Trust Master Scenario Events List

The Master Scenario Events List (MSEL) comes from the NIST Special Publication 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. This standard details all of the aspects of creating, running, and debriefing after a tabletop exercise. The most important part of a tabletop will be the planning—identifying the audience, defining the objectives, and creating a realistic scenario will all help maximize the organization's cybersecurity potential by improving their security incident response plans, identifying potential weaknesses or gaps in controls, and preparing individuals for playing their respective roles during an incident.

The Master Scenario Events List is a timeline of the scripted events to be injected into exercise play by a moderator to generate participant activity based on the objectives identified by the organizers. This script ensures that necessary events happen to generate discussion of policies, procedures, and plans and to help identify weaknesses based on real-world conditions. The MSEL should be used to track participant responses to injects and deviations from expected behaviors and to help reinforce the learning points associated with those actions.

Objective 1—Can the team avoid a disruption to operations during an incident?

Objective 2—Can the team tell the difference between a real issue and a false positive?

Objective 3—Identify any gaps in technology controls, incident response procedures, resources, or training that could impact the organization if this were a real incident.

Inject	**Expected Outcome**	**Learning Points**	**Maximum (Minutes) for Each Message**
"Injects" are events within the scenario that prompt participants to implement the plans, policies, and/or procedures to be tested during the exercise. Each inject should be considered its own "event" within the timeline of the scenario.	Expected outcomes represent management/administration's desired responses or actions to the questions or messages proposed during the delivery of injects.	Learning points are the specific takeaways that participants will learn from the inject and discuss afterward.	It is necessary to limit the time for the discussion of each inject so that all injects can be addressed during the given exercise time frame.

Inject	Expected Outcome	Learning Points	Maximum (Minutes) for Each Message
8:35 a.m.: Several customers report to support services that their TreadMarch units appear to start, but only display a blue screen and will not connect to the network.	1. Follow/Initiate incident response process with appropriate escalation. 2. Investigate for further information.	Not all incidents are related to hacking.	15 minutes
8:45 a.m.: Security operations center reports suspicious activity on several user accounts. Nothing outside what their accounts are allowed to do.	1. How is suspicious activity detected? 2. How do you define suspicious activity? 3. Review account permissions and recent activity.	Are staff trained to detect suspicious behavior? Is there enough information to correlate events?	15 minutes
9:00 a.m.: Call center reports that call volume is higher than normal for a weekday.	1. Will the team be distracted by the lack of information and jump to the conclusion that a problem is more widespread than it actually is?	Does the organization have operational monitoring of treadmills, operational status, firmware versions, etc. to evaluate trends?	10 minutes

Inject	Expected Outcome	Learning Points	Maximum (Minutes) for Each Message
9:30 a.m.: Technician reinstalls firmware on malfunctioning treadmill. Reports that a security dongle has been missing for several days.	1. What is the appropriate reporting process for lost or stolen equipment? 2. Does identity management allow for fast decommissioning of hardware tokens?	How will incident response team receive communications from impacted teams in real time?	10 minutes
10:07 a.m.: After reviewing account activity, security team member personally knew one of the users and texted to see what they were doing. User is on vacation.	1. Can team communicate with impacted users? 2. Does the organization have adequate monitoring to review activity logs?	Can the organization detect suspicious or anomalous user activity?	15 minutes
10:15 a.m.: PR department indicates social media sources show there may be a protest about labor conditions outside headquarters.	1. Is there a public information plan in place and has team been trained?	Public messaging is an important part of major exercises and PR personnel need to be in the communication path early on.	10 minutes

Inject	Expected Outcome	Learning Points	Maximum (Minutes) for Each Message
10:29 a.m.: CIO is removed from the scenario due to unexpected circumstances.	1. Does the incident response plan account for personnel changes during the response phase?	A streamlined process should include communications "warm handoff" for incident response leaders.	10 minutes
11:01 a.m.: Logs show successful two-factor authentications for user with suspicious activity. User mistakenly clicked Approve.	1. Are users trained to report mistaken MFA approvals? 2. When does an incident begin to impact business operations?	Mistakes should be something that you prepare for and learn from, not something that you avoid.	15 minutes
11:12 a.m.: SOC detects port-scanning activity originating from the treadmill firmware update server.	1. Are IoT networks trusted to talk to anything in the environment?	Many sophisticated attacks begin with or target IoT or OT networks.	10 minutes

Inject	Expected Outcome	Learning Points	Maximum (Minutes) for Each Message
11:45 a.m.: Protesters gather outside the building to complain about the working conditions in one of the factories where the treadmills are being produced. Media is now onsite.	1. Is the organization prepared to publicly acknowledge a cyberattack? At what point in the incident response plan is this required? 2. When is the organization required to notify customers or other partners?	Acknowledging and being transparent about an incident to protect the community is a better PR strategy than concealment.	10 minutes
12:25 p.m.: In reviewing traffic logs, the network team sees successful connections from the update server to another server . . . the network vulnerability scanning server.	1. Are necessary network logs available to capture lateral movement from server to server? 2. How long are these logs maintained? Do they contain only metadata or are they full packet captures to view payloads?	Would it have been possible to correlate suspicious activity in real time to have proactively prevented this scenario from escalating?	15 minutes

Inject	Expected Outcome	Learning Points	Maximum (Minutes) for Each Message
12:45 p.m.: Several staff members report seeing a drone flying close to the building.	1. Are sensitive areas visible from outside the building? 2. What protective controls might be available for these areas?	Has the organization performed a physical security audit?	10 minutes
1:05 p.m.: Logs show that the scanning server has been sending unknown traffic to nearly every server and client in the organization over the last several hours.	1. What trust relationships are created to facilitate known security activities? 2. How can these permissions be limited?	Do security controls and policy apply equally to all departments in the organization? Or have exceptions been made and are they well known and understood?	15 minutes
Overnight: Incident response firm worked overnight to determine that malware was installed that had a data exfiltration tool.	1. How would the organization determine what data may have been stolen? 2. Does the organization have a retainer with an incident response firm? 3. When is the appropriate time to notify cyber risk insurers?	How does the organization define a breach and when does data exfiltration necessitate victim notifications?	15 minutes

Appendix D
For Further Reading

Standards, Frameworks, and Other Resources

Center for Internet Security: The 18 CIS Critical Security Controls—www.cisecurity.org/controls/cis-controls-list

Cybersecurity & Infrastructure Security Agency: CISA Tabletop Exercise Packages—www.cisa.gov/cisa-tabletop-exercises-packages

Executive Order on Improving the Nation’s Cybersecurity—www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity

NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations—https://doi.org/10.6028/NIST.SP.800-53r5

NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide—https://doi.org/10.6028/NIST.SP.800-61r2

NIST Special Publication 800-84: Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities—https://doi.org/10.6028/NIST.SP.800-84

NIST Special Publication 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations—https://doi.org/10.6028/NIST.SP.800-171r2

NIST Special Publication 800-207: Zero Trust Architecture—https://doi.org/10.6028/NIST.SP.800-207

OWASP API Security Project—https://owasp.org/www-project-api-security

OWASP Top 10—https://owasp.org/Top10

Case Studies

Adobe'sCaseStudyonZeroTrust—www.youtube.com/watch?v=IGFhMoRXTqg&t=7s

How Akami Implemented a Zero Trust Security Model—www.akamai.com/us/en/multimedia/documents/case-study/how-akamai-implemented-a-zero-trust-security-model-without-a-vpn.pdf

LogRhythm's Journey to Zero Trust—www.youtube.com/watch?v=Fj4ifrMfD8w&feature=emb_logo

Google BeyondCorp Papers

An overview: "A New Approach to Enterprise Security"—https://research.google.com/pubs/pub43231.html

How Google did it: "Design to Deployment at Google"—https://research.google.com/pubs/pub44860.html

Google's front-end infrastructure: "The Access Proxy"—https://research.google.com/pubs/pub45728.html

Migrating to BeyondCorp: "Maintaining Productivity while Improving Security"—https://research.google.com/pubs/pub46134.html

The human element: "The User Experience"—https://research.google.com/pubs/pub46366.html

Secure your endpoints: "Building a Healthy Fleet"—https://ai.google/research/pubs/pub47356

Books

Cyber Warfare—Truth, Tactics, and Strategies. Dr. Chase Cunningham, Packt Publishing, 2020.

Zero Trust Networks. Evan Gilman, Doug Barth, O'Reilly Media, 2017.

Zero Trust Security: An Enterprise Guide. Jason Garbis, Jerry W. Chapman, Apress, 2021.

Hardening Guides

Best Practices for Securing Active Directory—`https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory`

Cisco Router Hardening Guide—`www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html`

Docker Hardening—`https://docs.docker.com/engine/security`

Kubernetes Hardening Guide—`https://media.defense.gov/2021/Aug/03/2002820425/-1/-1/0/CTR_Kubernetes_Hardening_Guidance_1.1_20220315.PDF`

Microsoft Security Baselines—`https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines`

Securing Distribution Independent Linux—`www.cisecurity.org/benchmark/distribution_independent_linux`

VMWare Security Hardening Guides—`www.vmware.com/security/hardening-guides.html`

Windows Server Security Documentation—`https://docs.microsoft.com/en-us/windows-server/security/security-and-assurance`

Glossary

Asserted identity Identity is always an assertion of the abstraction of a user on a network. The identity system "asserts" that a device is generating packets under the control of the asserted.

Attack surface An attack surface of an organization is made up of all of the different elements where a threat actor can attempt to exploit weaknesses to obtain unauthorized access into an environment. One strategy for security involves reducing your organization's attack surface; however, in practice this is difficult to do since many services require access to the Internet and consequently the whole world can be an attack surface.

Bring your own device (BYOD) Many organizations allow employees to bring their own consumer devices into the organization to access company resources or services. For many security teams BYOD comes with the challenge of applying security controls to all the various types of personally owned devices.

Cloud access security broker (CASB) Many organizations are not able to obtain the same visibility into or control over cloud-based services. CASB services use proxies or API integrations to assist security teams with providing security controls into cloud-based services.

Data, applications, assets, and services (DAAS) DAAS is an acronym that stands for data, applications, assets, and services, which define the sensitive resources that should go into individual protect surfaces. DAAS elements include:

- Data—This is sensitive data that can get an organization in trouble if it is exfiltrated or misused. Examples of sensitive data include payment card information (PCI), protected health information (PHI), personally identifiable information (PII), and intellectual property (IP).
- Applications—Typically these are applications that use sensitive data or control critical assets.
- Assets—Assets could include IT (information technology), OT (operational technology), or IoT (Internet of Things) devices such as point-of-sale terminals, SCADA controls, manufacturing systems, and networked medical devices.
- Services—These are sensitive services that are very fragile that your business depends upon. The most common services that should be protected in a Zero Trust manner include DNS, DHCP, Active Directory, and NTP.

Data toxicity Data toxicity is the doctrine that sensitive data becomes "toxic" to your organization if it has been stolen or exfiltrated from your networks or systems into the control of malicious actors. This exfiltration leads to a negative impact on the business. The data has become toxic as its theft leads to lawsuits or regulatory action on the organization. Every organization has both nontoxic and toxic data. An easy way to recognize toxic data types is to remember the 4Ps of toxic data: PCI (credit card data), PII (personally identifiable information), PHI (patient health information), and IP (intellectual property). Most toxic data falls into this simple framework.

DevOps DevOps is a software development philosophy that shortens the software development life cycle by continuously and rapidly deploying software updates and results in higher-quality, more innovative software.

Endpoint detection and response (EDR) The previous generation of antivirus used file hashes as signatures to identify malware, requiring huge amounts of human effort to identify malicious code, but this approach led to attackers modifying code to evade detection. EDR takes a different approach, applying machine learning to identify how malicious code interacts with the operating system and allows investigators to identify and correlate security events on endpoints and take action on those alerts.

Granular access control Granular access control is the outcome of an explicitly defined Zero Trust Kipling Method Policy statement. Multiple access control criteria provide fine-grained policy for access to a protect surface, making it substantially more difficult to perform a successful attack against that protect surface.

Identity Identity is the validated and authenticated "who" statement that is part of the Kipling Method Policy assertion: "Who" should have access to a resource?

Identity and Access Management (IAM) Identity and Access Management are the organization-specific policies and controls that help manage the life cycle of an identity through its journey from creation to removal. Typically there are four areas where organizations manage identities: authentication, authorization, user management, and directory services. In addition, individual identities may inherit permissions from groups, so managing groups of users is also important to an IAM program. The most critical part of an IAM program is the governance of how identities are managed and how policies are created and changed.

Internet of Things (IoT) Many of the devices on a network today aren't desktops or laptops where a human is the primary source of activity. Cameras, card readers, printers, building control systems, personal mobile devices, personal assistants, TVs, gaming devices, and wearables all may attempt to connect to the company network.

Kipling Method Policy (KMP) Zero Trust policy is created using the Kipling Method, named after the writer Rudyard Kipling, who gave the world the idea of Who, What, When, Where, Why and How in a poem in 1902. Since the idea of WWWWWH is well known worldwide, it crosses languages and cultures and allows easily created, easily understood, and easily auditable Zero Trust policy statements for various technologies. A KMP determines what traffic can transit the microperimeter at any point in time, preventing unauthorized access to your protect surface, while preventing the exfiltration of sensitive data into the hands of malicious actors. True Zero Trust requires Layer 7 technology to be fully effective. The Kipling Method describes a Layer 7 Zero Trust granular policy.

Using the Kipling Method, you can create Zero Trust policy effortlessly by answering the following questions:

- *Who should be allowed to access a resource?* The validated "asserted identity" will be defined in the Who statement. This replaces the source IP address in a traditional firewall rule.

- *What application is the asserted identity allowed to use to access the resource?* In almost all cases, protect surfaces are accessed via an application. The application traffic should be validated at Layer 7 to keep attackers from impersonating the application at the port and protocol level and using the rule maliciously. The What statement replaces port and protocol designations in traditional firewall rules.
- *When defines a time frame?* When is the asserted identity allowed to access the resource? It is common for rules to be instantiated 24/7, but many rules should be time limited and turned off when authorized users are not typically using the rule. Attackers take advantage of these always-on rules and attack when approved users are away from the system, making the attacks more difficult to discover.
- *Where are the locations from which a resource will be accessed?* Where are the resources located? Where defines the position of a specific location, object, or device. The Where statement replaces the destination IP address in traditional firewall rules. The geolocation of a resource should always be known, and impossible travel rules will alert administrators to spoofing attempts.
- *Why are we protecting this resource?* The classification of a resource as public, private, secret, or top secret should be aligned with the controls. Many applications mix multiple types of data within the same protect surface, so it is critical to have an inventory that includes compliance requirements, privacy impact, intellectual property, and business considerations.
- *How will the resource be protected?* This can include all of the controls that should be applied to the protect surface, including encryption and decryption, URL filtering, sandboxing, signatures, anomaly detection, etc.

Least-privilege access Least-privilege access asks the question “Does a user need to have access to a specific resource to get their job done?” We give too much access to most users based upon the broken trust model. By mandating a least-privilege, or need-to-know, policy, the ability of a user to perform malicious actions against a resource is severely limited. This mitigates against both stolen credential and insider attacks.

Managed Security Service Provider (MSSP) Because of the challenges of hiring or retaining security staff, many organizations have turned to MSSPs to provide security consulting, SOC, forensics, and incident response, among other key service needs. One of the main benefits of an MSSP is that it has the ability to correlate data from attacks against hundreds or thousands of customers across various industries. It is important to note, however, that an organization can’t outsource the responsibility or accountability of security, so there should be an owner of security inside the organization.

Microperimeter When a segmentation gateway (SG) connects to a protect surface and a Layer 7 Kipling Method Policy is deployed, then a microperimeter is placed around the protect surface. The microperimeter ensures that only known approved and validated traffic has access to the protect surface, based upon policy. One architectural principle of Zero Trust is to move your SG as close as possible to the protect surface for the most effective preventative controls enforced by the microperimeter.

Microsegmentation Microsegmentation is the act of creating a small segment in a network so that attackers have difficulty moving around and accessing internal resources. Many networks are "flat," meaning that there are no internal segments, so if an attacker gets a foothold in the network, they can move around unnoticed to attack resources and steal data. A microperimeter is a type of microsegment. The microperimeter defines a Layer 7 boundary for protections of a DAAS element. Some organizations may choose to use Layer 3 microsegmentation technology inside a microperimeter.

National Institute for Standards and Technology (NIST) NIST is a U.S. government entity that creates and publishes standards across many different industries. The philosophy of NIST is that through creating standards, organizations can better innovate and compete in a global economy. NIST has created a number of indispensable standards when it comes to cybersecurity, including the ones mentioned in this book:

- 800-53—Security and Privacy Controls for Information Systems and Organizations
- 800-61—Computer Security Incident Handling Guide
- 800-84—Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
- 800-171—Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- 800-207—Zero Trust Architecture

Operational technology (OT) Increasingly, sophisticated threat actors have moved from targeting user desktops or laptops to targeting the control systems that help manage factories, buildings, oil pumps, or smart cities. OT systems interact with the physical environment of an organization and are often a blind spot for security teams.

Policy engine A policy engine was proposed in NIST SP 800-207 to help focus Zero Trust implementations around the concepts of least privilege and identity. In theory, a policy engine could help organizations provide just-in-time access to resources where authentication is happening continuously.

Privileged access management (PAM) One of the biggest targets inside an organization are its privileged accounts like Active Directory Domain Admin accounts. If compromised, these accounts can allow an attacker to take any action they choose inside an organization and it becomes increasingly difficult to remove an attacker after they have obtained one of these accounts. PAM tools help protect these accounts and assist organizations in auditing and tracking admin activities to help detect a compromise.

Protect surface The protect surface is the opposite of an attack surface. An attack surface is massive and includes the entire Internet while a protect surface is limited to systems under your control. A Zero Trust strategy focuses on applying tailored controls to protect surfaces rather than attempting to manage a huge attack surface. Each protect surface contains a single DAAS element. Each Zero Trust environment will have multiple protect surfaces.

Secure Access Services Edge (SASE) With the rise of remote access required after the onset of the 2020 pandemic, many organizations wanted to ensure that workers could work from anywhere while enforcing the same levels of security on user devices. SASE tools can take many forms but often come as an agent that limits network access to a device based on policy, provides for remote browser isolation when accessing the Internet, proxies access to cloud services.

Secure web gateway (SWG) One of the most common ways of infecting a computer with malware is to have a user click a malicious web address that downloads malware to the user's computer. SWGs help protect users from visiting these malicious websites by acting as a proxy for outbound user traffic from an organization to enforce company policies.

Security Information Event Management (SIEM) Threat actors will commonly attempt to hide or destroy any evidence that a system has been compromised. For logs that remain on a compromised system, this is easy for an attacker to accomplish. In response, security teams now send logs to a centralized logging server that maintains a forensically secure copy of these logs in the event an organization experiences a breach. SIEM tools will typically parse and normalize log data that allows these systems to help correlate suspicious activity and alert admins when malicious activity has been detected.

Security Operations Center (SOC) Many organizations choose to employ a SOC to provide 24x7 monitoring of security telemetry from SIEM systems, network detection and response tools, or API integrations with an organization's, EDR, SOAR, SWG, CASB, PAM, or SASE tools.

Security orchestration, automation, and response (SOAR) SOCs typically gather inputs from many different sources and require analysts to review information from multiple systems for investigations and then take action in many different additional systems to respond to threats. SOAR systems rely on playbooks designed by organizations to correlate specific types of activity and then create automated responses based on those detections, reducing the time it takes to respond to a threat from hours to seconds.

Segmentation gateway (SG) A segmentation gateway is a Layer 7 gateway designed to segment networks based upon users, applications, and data. Segmentation gateways are the primary technology used to enforce Layer 7 policy in Zero Trust environments. Segmentation gateways can be physical (PSG) when used in traditional on-premise networks, or virtual (VSG) when used in public or private clouds. Next-generation firewalls traditionally function as segmentation gateways when they are deployed in Zero Trust environments.

Software as a Service (SaaS) SaaS is the model of selling software that is delivered to a user through a cloud-based platform rather than the typical licensing model of installing the software on a user's computer. The SaaS model has the advantage to customers in terms of speed of delivery, while software companies benefit from only supporting the current version of the software rather than many legacy versions. The challenge of SaaS for security teams is the lack of visibility and control over user activity in this model, and many organizations choose to implement a CASB in order to get this control back.

Trust levels The existing cybersecurity paradigm is based upon a broken trust model where all systems external to the corporate networks are considered "untrusted" and those inside the corporate networks are known as "trusted." It is this flaw that undergirds Zero Trust. Trust is a human emotion injected into digital systems for no technical reason. It is not measurable. Trust is binary. All successful cyberattacks exploit trust in some manner, making trust a dangerous vulnerability that must be mitigated. In Zero Trust, all packets are untrusted and are treated exactly the same as every other packet flowing across the system. The trust level is defined as zero, hence the term Zero Trust.

Web application firewall (WAF) A traditional firewall is used to manage policies at an IP or TCP/UDP port level. These traditional firewalls lack awareness of what happens at the application layer of a session and can't protect from web-based attacks like SQL injection or cross-site scripting. In contrast, a WAF operates only at the application layer and provides signature-based rules to stop common OWASP attacks as well as enforcing input validation on sites or detection of credential stuffing attacks where threat actors use compromised passwords to attempt to access sensitive resources.

Zero Trust Zero Trust is a strategic initiative that helps prevent successful data breaches by eliminating digital trust from your organization. Rooted in the principle of "never trust, always verify," Zero Trust is designed as a strategy that will resonate with the highest levels of any organization yet can be tactically deployed using off-the-shelf technology. Zero Trust strategy is decoupled from technology, so while technologies will improve and change over time, the strategy remains the same.

Zero Trust architecture Your Zero Trust architecture is the compilation of the tools and technologies used to deploy and build your Zero Trust environment. This technology is fully dependent upon the protect surface you are protecting, as Zero Trust is designed from the inside out, starting at the protect surface and moving outward from there. Typically, the protect surface will be protected by a Layer 7 segmentation gateway that creates a microperimeter that enforces Layer 7 controls with Kipling Method Policy. Every Zero Trust architecture is tailor made for an individual protect surface.

Zero Trust environment A Zero Trust environment designates the location of your Zero Trust architecture, consisting of a single protect surface containing a single DAAS element. Zero Trust environments are places where Zero Trust controls and policies are deployed. These environments include traditional on-premises networks such as data centers, public clouds, private clouds, endpoints, or across an SD-WAN.

Zero Trust Network Access (ZTNA) Created by Gartner in 2019, the term ZTNA refers to a category of tools that help facilitate providing secure access to private networks through authenticated access. This term helps broaden the definition of remote access through older technologies like virtual private networks (VPNs) to secure web gateways (SWGs) or Secure Access Service Edge (SASE) agents.