The Need for Zero Trust Security

Gary Forde
Senior Sales Specialist

Daryl Crook
Senior Sales Engineer

Forcepoint

Agenda

- Introduction of Zero Trust
- Why ZT is Important
- Reducing Malware Risk

Forcepoint

Born with a Passion

TO BE A FORCE FOR GOOD

Our Manifesto

what we believe in

We are like no other technology company

Trusted cybersecurity: combining speed/agility of commercial business with the high-assurance demanded by high-consequence missions

We are not for everyone

Our customers run highly complex and hyper-distributed IT environments where high-assurance and trust mean something

Technology to enable good

We deliver deep technology and cybersecurity innovations that serve a higher purpose and make the world a better place

We are problem solvers

We are experienced at meeting the complex challenges of high-assurance, high-consequence environments. Responding when needed even “after hours”

We face big consequences, everyday

We are a pre-eminent team of engineers and technologists with world-class experience for high-assurance innovations

Zero Trust – What is it?

Improvement on "Trust but Verify"

Castle/Moat Standard

- Users are granted access by being employees
- Once users are across the moat (network boundary) they can access all of the castle

Zero Trust Principle

- Deny all access explicitly – no user by default gets to cross the moat
- Limit castle resource access to those users that need it (only allow armory access to soldiers)
- Verify access through enhanced methods – MFA, Push Notification, etc.

Industry & Government Perspectives On Modern Cyber Security

Forrester Zero Trust

- *Never trust, always verify*
- *Maturity of people, skills, technology and capabilities*
- *7 Pillars*


FORRESTER

NOT LICENSED FOR DISTRIBUTION

Future-Proof Your Digital Business With Zero Trust Security

Vision: The Security Architecture And Operations Playbook

by Jeff Pollard

March 28, 2018

Why Read This Report

As CIOs develop hybrid cloud strategies to help their organization become fast, flexible, and innovative, it's the perfect time to migrate to a Zero Trust security architecture. Security and risk (S&R) leaders can use their organization's mandate for digital transformation to escape from legacy networks full of "security debt" stemming from tradeoffs and competing priorities. Security can exploit this migration to build in — rather than bolt on — Zero Trust security architectural principles.

This is an update of a previously published report; Forrester reviews and updates it periodically for continued relevance and accuracy.

Key Takeaways

Hybrid Cloud Is A Path To Zero Trust

Organizational inertia is a recurring theme that impedes enterprisewide transformation. Hybrid cloud, with staggered adoption and migration, is a unique chance for S&R pros to try a new approach to security architecture.

In A Data Economy, CISOs Must Protect Data Throughout The Digital Supply Chain

More than one-third of enterprises are commercializing data, and that percentage is growing. Chief information security officers (CISOs) must understand data, how it flows, and how the organization collects, transmits, stores, and shares it. Most important, CISOs must understand in concrete economic terms data's value to the organization to provide meaningful guidance.

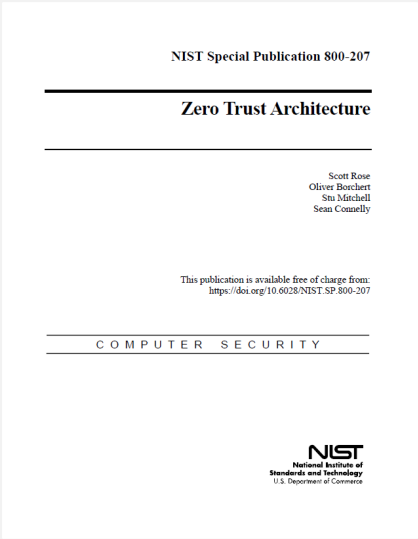
S&R Pros Now Secure Systems Of Engagement And Insights

S&R pros are no longer just responsible for securing back-end systems of record and supporting infrastructure. Cloud adoption has diminished some of this as a priority; however, as organizations undergo digital transformation, this brings a new paradigm in which S&R pros must focus on securing new customer engagement models, applications, and the systems of insights that collect reams of sensitive data.

FORRESTER.COM

NIST SP 800-207

- *Identity-Driven approach*
- *Policy Driven Access*
- *Continuous Monitoring*
- *Reauthentication and Reauthorization*
- *Microsegmentation*


NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

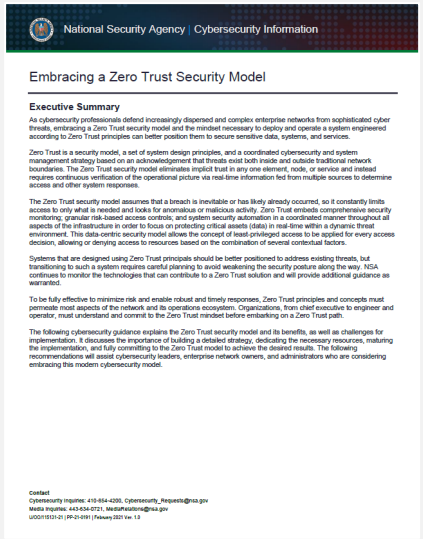
This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NSA Zero Trust

- *Maturity Levels*
- *Risk Informed Decisions (Tuple)*
- *Decision Engine*


National Security Agency | Cybersecurity Information

Embracing a Zero Trust Security Model

Executive Summary

As cybersecurity professionals defend increasingly dispersed and complex enterprise networks from sophisticated cyber threats, embracing a Zero Trust security model and the mindset necessary to deploy and operate a system engineered according to Zero Trust principles can better position them to secure sensitive data, systems, and services.

Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information fed from multiple sources to determine access and other system responses.

The Zero Trust security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting critical assets (data) in real-time within a dynamic threat environment. This data-centric security model allows the concept of least-privileged access to be applied for every access decision, allowing or denying access to resources based on the combination of several contextual factors.

Systems that are designed using Zero Trust principals should be better positioned to address existing threats, but transitioning to such a system requires careful planning to avoid weakening the security posture along the way. NSA continues to monitor the technologies that can contribute to a Zero Trust solution and will provide additional guidance as warranted.

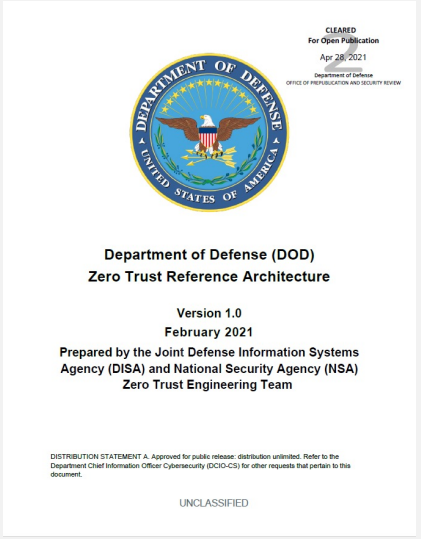
To be fully effective to minimize risk and enable robust and timely responses, Zero Trust principles and concepts must permeate most aspects of the network and its operations ecosystem. Organizations, from chief executive to engineer and operator, must understand and commit to the Zero Trust mindset before embarking on a Zero Trust path.

The following cybersecurity guidance explains the Zero Trust security model and its benefits, as well as challenges for implementation. It discusses the importance of building a detailed strategy, dedicating the necessary resources, maturing the implementation, and fully committing to the Zero Trust model to achieve the desired results. The following recommendations will assist cybersecurity leaders, enterprise network owners, and administrators who are considering embracing this modern cybersecurity model.

Contact
Cybersecurity Inquiries: 410-854-4200, Cybersecurity_Requests@nsa.gov
Media Inquiries: 443-634-0721, MediaRelations@nsa.gov
U/OO/115531-21 | PP-21-0191 | February 2021 Ver. 1.0

DoD Zero Trust

- *7 pillars*
- *Maturity levels*
- *Unified Analytics – Data, Assets, Applications and Services (DAAS)*


CLEARED
For Open Publication
Apr 28, 2021
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Department of Defense (DOD)
Zero Trust Reference Architecture

Version 1.0
February 2021

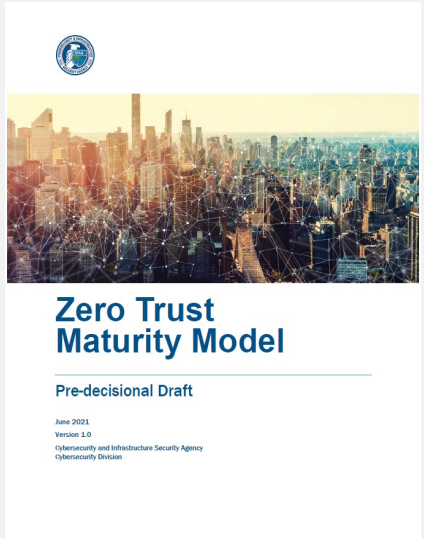
Prepared by the Joint Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited. Refer to the Department Chief Information Officer Cybersecurity (DCIO-CS) for other requests that pertain to this document.

UNCLASSIFIED

CISA ZT Maturity Model

- *5 pillars*
- *Incorporates NIST, NSA & DoD*
- *Maturity Model*
- *Continuous Evaluation*
- *Micro-segmentation*

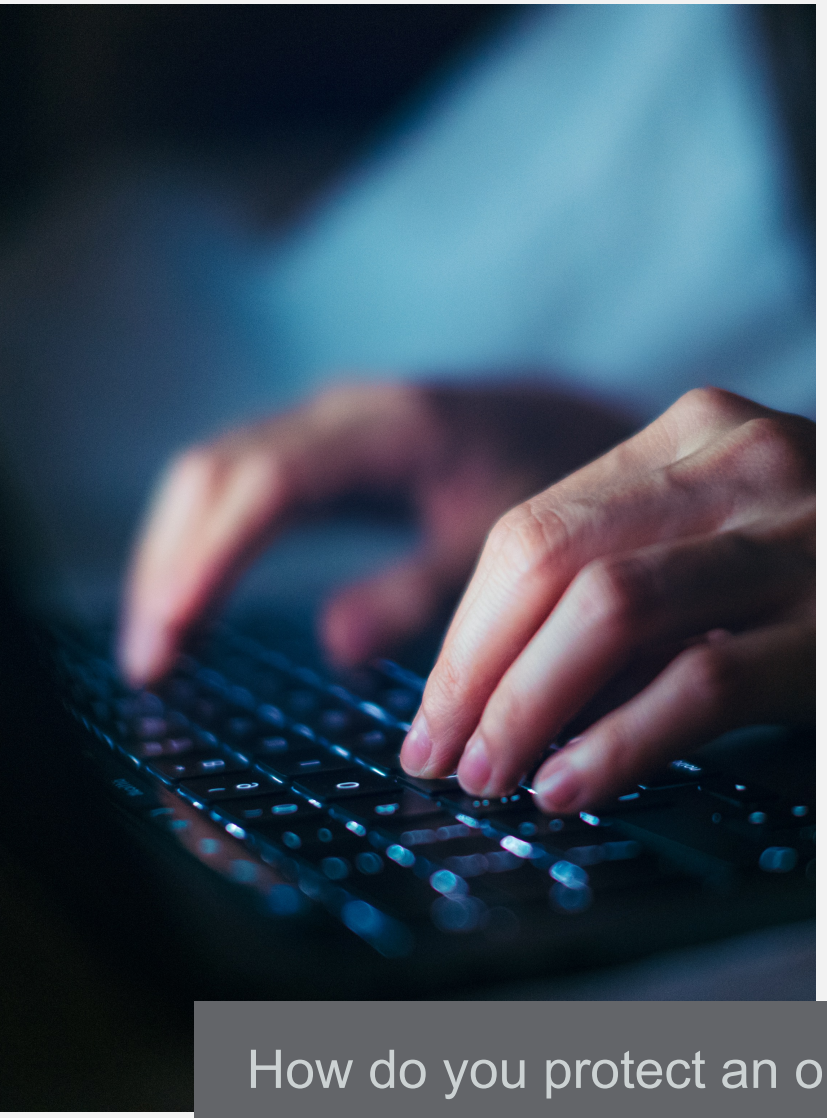


Zero Trust Maturity Model

Pre-decisional Draft

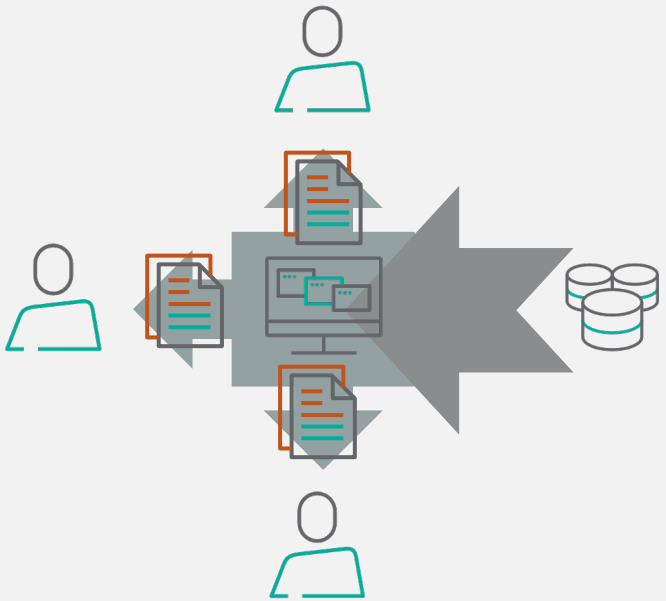
June 2021
Version 1.0
Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

The Problem with Data Sharing



To receive information, you must accept data …

… but data can carry ***malware***



To share information, you must send data …

... but data can carry ***extra information***

How do you protect an organization when you can't detect what the newest threats are?

The Zero Trust CDR Approach – Simplified

Zero Trust CDR

UNSAFE DIGITAL CONTENT

SAFE DIGITAL CONTENT

EXTRACT

content from original data, discard unwanted content

VERIFY

that the information is safe

BUILD

and deliver safe information and data

- **Extract** only the business information – nothing else
- **Transform and simplify everything,** trust no data or complex software
- **Stop malware** without the need to detect it

Secure Web Browsing with Zero Trust CDR

Zero Trust CDR ensures that downloads are always free from both known and zero-day threats

Challenge

- Attackers use modern file formats to conceal malware which is downloaded from websites.
- Web defenses like web gateways and firewalls are vulnerable to previously unknown (zero-day)

Solution

- Integrating Zero Trust CDR with your existing Secure Web Gateways and firewalls provides users with a totally safe browsing environment
- Zero Trust CDR will soon integrate with Remote Browser Isolation (RBI), combining safe malware-free downloads and secure web access

Outcomes

- Enable productive, malware-free web browsing

- Eliminate known and zero-day malware concealed in downloads

- Stop covert data loss concealed in images

Demos:

Stop malware in Web email

Stop malware in Web downloads

Stop malware in Web ads

Secure Email with Zero Trust CDR

Zero Trust CDR ensures that email messages and attachments are always free from both known and zero-day malware

Challenge

- Attackers use modern file formats to conceal malware which is delivered via email messages and attachments
- Traditional Email Security Gateways are vulnerable to previously unknown (zero-day) malware

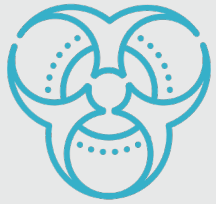
Solution

- Integrating Zero Trust CDR alongside your existing Email Security Gateways, anti-spam filters and perimeter anti-virus technology provides users with a totally safe messaging environment

Outcomes

Enable productive, malware-free email use

Eliminate known and zero-day malware concealed in messages and attachments



Stop covert data loss concealed in images

Demos:

Stop inbound malware in attachments

Stop data leakage via steganography

Secure Custom Applications with Zero Trust CDR

Zero Trust CDR ensures applications that handle files from untrusted locations are always free from both known and zero-day threats

Challenge

- Applications that handle content from untrusted sources are at risk from opening, processing and onward sharing
- Hidden malware in the content can either attack the system on which the application resides, attack back-end databases, or could be downloaded to user desktops

Solution

- Using simple HTTP API calls, Zero Trust CDR ensures that the files do not contain malware and can be shared and opened in safety
- Can operate directly on files in AWS S3 buckets and Azure container

Outcomes

- Eliminates zero day, evasive and undetectable threats

- Serverless and stateless no infrastructure to build or maintain

- Lower TCO with no maintenance and no false positives

Demo:  Secure Custom Applications

The Zero Trust CDR Advantage

Security

- Defeats all Malware
- Evasion Proof
- Future Proof

ROI

- No False Positives
- No Updates to Manage
- No Need to Rush Patches Out
- No Immediate Need to Replace Vulnerable Legacy Applications.

Flexibility

- Cloud Native
- On-Premises
- Virtual

Performance

- Fast Stateless Processing
- Scalable, Non-Stop Operation
- Near Real-Time

We call our implementation **Zero Trust CDR**
trust nothing and **transform everything**

Moving to an Optimal Zero Trust State

Identity

Traditional	Advanced	Optimal
Password or multifactor authentication Limited risk assessment	MFA Some identity federation with cloud on on-premises	Continuous Validation in real time for just in time, just enough access and policy enforcement

Network

Traditional	Advanced	Optimal
Large macro-segmentation Minimal or external traffic encryption	Defined by ingress / egress micro-perimeters Basic analytics	Fully distributed ingress / egress micro-perimeters

Device

Traditional	Advanced	Optimal
Limited visibility into compliance Simple inventory	Compliance enforcement employed Data access depends on device posture on first access	Constant device security monitoring and validation

Application Workloads

Traditional	Advanced	Optimal
Access based on local authorization Minimal integration with workflow Some cloud accessibility	Access based on centralized authentication Basic integration into application workflow	Access is authorized continuously

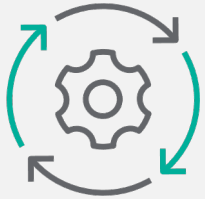
Data

Traditional	Advanced	Optimal
Not well inventoried static controls unencrypted	Least privilege controls Data stored in cloud or remote environments are encrypted at rest	Dynamic support All data is encrypted

Visibility/Analytics + Automation/Orchestration + Governance

The **Forcepoint** Difference

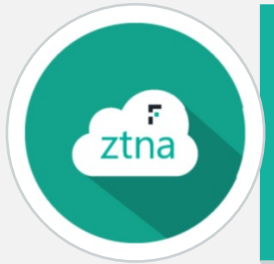
Prevention, not reaction



Built-in, not bolted on

Comprehensive, not piecemeal

Why Forcepoint: Proven Zero Trust Technologies



Zero Trust Network Access

- Private Access • IdP Federated Identity • Risk-Adaptive
- Cloud • Web • Email • Endpoint • DLP
- Cyber Threat Prevention • Zero Trust CDR

bitglass websense Cyberinc DEEP SECURE FedRAMP Gartner Magic Quadrant FORRESTER® WAVE LEADER 2020 Zero Trust eXtended Ecosystem Platform

Data-Centric Enterprise

- L7 NGFW & IPS • SD-WAN • Micro-segmentation • Cloud
- DLP Discovery • Endpoint • Network • Web • Cloud
- Cyber Threat Prevention • Zero Trust CDR • CDS

McAfee Firewall Next-Gen Enterprise STONESOFT Sidewinder websense Raytheon Gartner Magic Quadrant FORRESTER® WAVE LEADER 2020 Zero Trust eXtended Ecosystem Platform Raise the Bar NCSDMO

Visibility & Analytics

- Enterprise-wide Continuous Monitoring
- UEBA • Dynamic Data Protection • Insider Threat • CE
- Zero Trust Policy Orchestration • ICAM • SIEM / SOAR

REDOWL ANALYTICS FORRESTER® WAVE LEADER 2020 Zero Trust eXtended Ecosystem Platform

ZERO TRUST BUILT ON INDUSTRY-LEADING TECHNOLOGIES

Built on products trusted *by Government* to protect critical missions *for over 20 years*

Forcepoint