Zero Trust

Zero Trust is a security philosophy and strategy based on the premise that everyone and everything inside a network is potentially suspect.

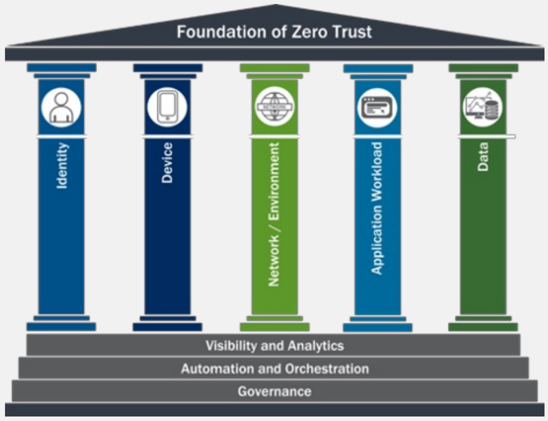
A Zero Trust approach helps mitigate the threat of ransomware crews, state actors, and insider threats through a common approach of revalidation and access decisions based on rights and risk assessments.

Understanding Zero Trust

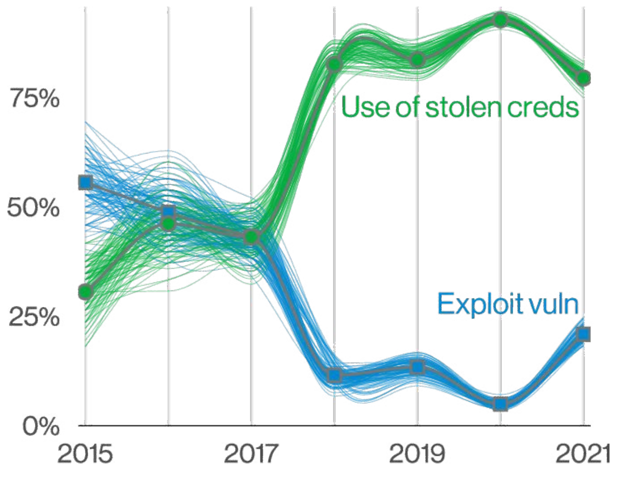
If your organization:

- Has a distributed workforce, i.e. employees and contractors working remotely or from home;
- Is involved in mergers and acquisitions activities;
- Is using cloud services (e.g. SAAS, PAAS, IAAS); and/or
- Has regulatory or legal risks that require demonstratable control for sensitive information

We suggest you consider:



https://www.cisa.gov/zero-trust-maturity-model



Exploit vulnerability vs. Stolen credentials over time in Basic Web Application Attacks breaches[1]

Stolen Credentials vs Exploiting Vulnerabilities

There is a larger trend in terms of using stolen credentials vs. exploiting vulnerabilities. There has been an almost 30% increase in stolen credentials since 2017, cementing it as one of the most tried-and-true methods to gain access to an organization for the past four years. Focusing on disabling these attack vectors is now critical.

Zero trust shifts the security focus from being location-centric to data-centric. Since data is no longer only in the data center, the defensive boundaries have changed. By focusing on minimizing the attack surface of Web applications (i.e SSE and CASB solutions) and re-enforcing the trust level of identity (i.e. MFA, FIDO2[2], and Risk assessment-based access models), a Zero Trust Strategy helps break the kill chain before the organization is impacted.

[1] Verizon DBIR 2022 - https://www.verizon.com/business/resources/T13/reports/dbir/2022-data-breach-investigations-report-dbir.pdf

[2] FIDO 2 Standard - https://fidoalliance.org/fido2/

RF-221108

Our Approach to Zero Trust

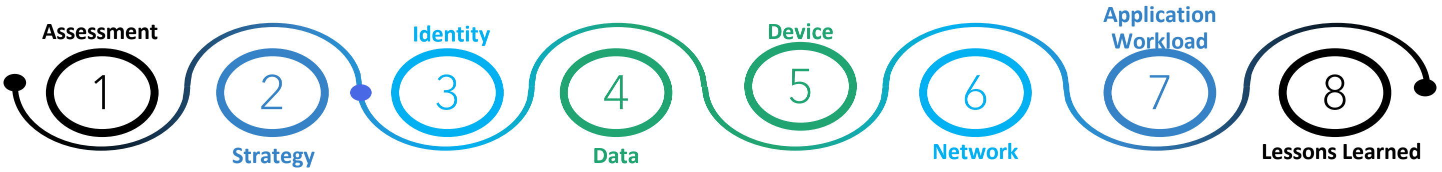
We offer a Zero Trust Assessment to help your organization understand your current Zero Trust maturity and create a path forward. With industry-standard models and technical subject matter expertise, we can help your team define your Zero Trust strategy and approach to transforming your IT services into flexible and secure solutions.

A Zero Trust Strategy and Roadmap should:

- Leverage a dynamic and flexible approach based on the Agile and PMBOK methodologies;
- Account for currently deployed technologies and organizational fit; and,
- Define how it enables the organization

The e360 Zero Trust Roadmap

This roadmap defines how organizations should implement the Zero Trust pillars to achieve a cohesive end-state Zero Trust Architecture. Each phase of the road map can be executed individually or in groups but should always begin with Assessment, followed by Strategy, and end with Lessons Learned.



	Assessment	Strategy	Identity	Data
Activities	Determine your current Zero Trust maturity level	Determine target Zero Trust maturity level and how to get there	Centralize user and admin management	Establish data baseline
Outcomes	Baseline Zero Trust maturity level (As-Is)	Zero Trust Strategy and Roadmap (To-Be)	Unified/centralized Identity Authority deployed	Data inventory with classifications and protection requirements deployed

	Device	Network	Application Workload	Lessons Learned
Activities	Establish and deploy device security standards	Secure the transport layer	Secure the application environments	Post-Cycle Review
Outcomes	Secure device configurations for all devices are globally enforced	Secure LAN/WAN sessions from end user to IT services are globally enforced	Secure application configurations and architectures are globally enforced	Determine what worked, what didn’t, and how to address challenges in the future

Contact us to learn more.

1855 Gateway Blvd. Suite 730
Concord, CA 94520

info@e360.com

e360.com

Brad Bussie
SVP of Cyber Security
e360 Cyber Risk Services
Brad.Bussie@e360.com

Trevor Hogan
Field CISO
e360 Cyber Risk Services
Trevor.Hogan@e360.com

The information, content, and materials are for general guidance on matters of interest only and does not constitute professional advice. As such, it should not be used as a substitute for consultation with a professional or other competent advisers. Before making any decision or taking any action, you should consult an e360 professional.