ZERO TRUST

Operationalizing a Zero Trust Initiative

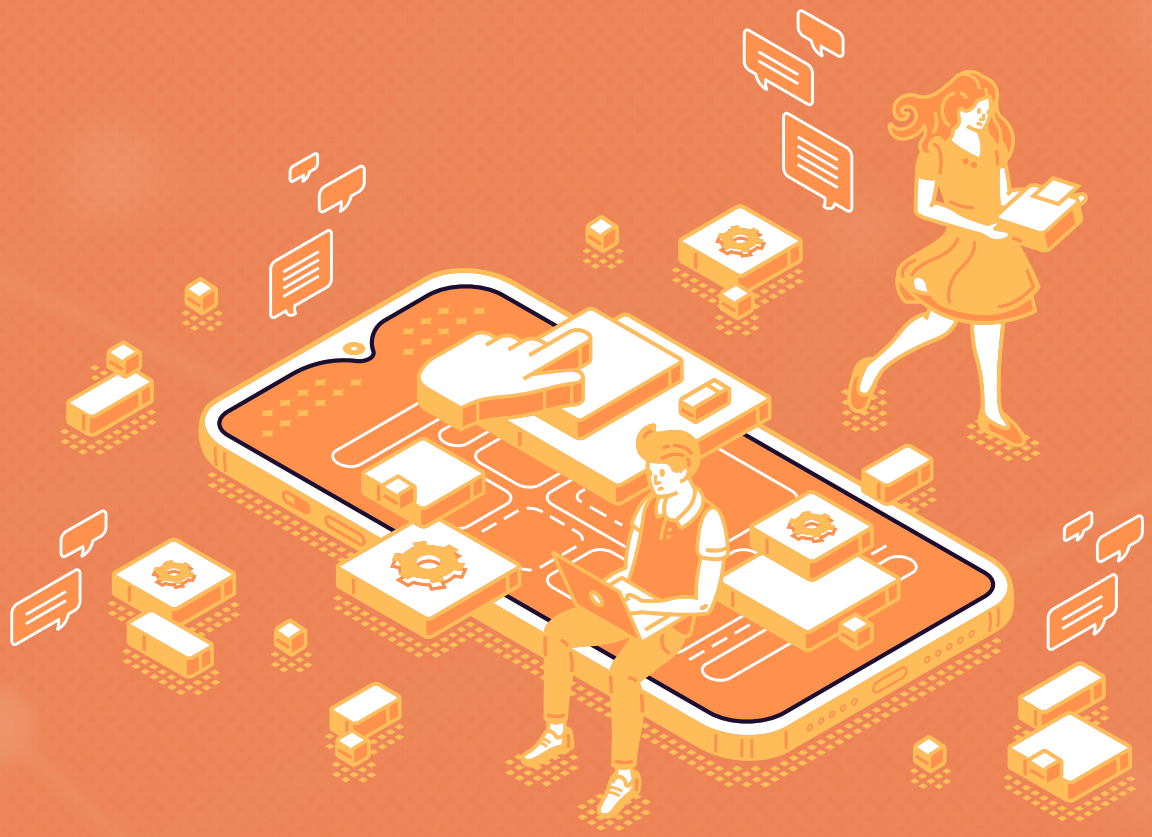
An unbiased guide for IT architects who are starting or supporting a Zero Trust initiative.

Andy Ruth, Managing Director
Jaylene Ruth, Director of Operations
Andrew Wilt, Chief Creative Officer

SUSTAINABLE **EVOLUTION** | AUGUST **2023**

Start Here

This eBook is written for IT architects who are starting or supporting a Zero Trust initiative. The guidance is framed on architectural best practice and process used for any major IT initiative. This eBook covers the key areas you'll consider when operationalizing a Zero Trust initiative.



Visit us at sustainableevolution.com

© 2023 Sustainable Evolution, Inc. All rights reserved. |

TABLE OF CONTENTS

© 2023 Sustainable Evolution, Inc. All rights reserved. |

Introduction

For many organizations, the transition from network-focused and implicit trust to asset-focused and explicit trust is challenging. Piled on top of the daily increase in signals every IT environment has seen and the number and sophistication of attacks, operationalizing zero trust demands automation and strong change management to help people get over the change hump.

Increasing automation and using change management techniques can help you integrate a Zero Trust strategy into a function SecOps environment.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

Automation

This might be the most fun part of the entire modeling process. You've got an idea of the objectives and principles for the initiative and what the target measures of success are. You have segmented each pillar of the data request and fulfillment journey and are making progress in having a complete inventory.

Now you get to firm up the actual governance model so that decisions on what identities can access what data (given the context of the journey) can be defined and enforced through an automated policy engine. Then you get to model a solution that automates the data access request-and-fulfillment function with enforcement at the API or asset level. You also get to ensure that the operational state can be monitored, anomalies detected, and automated alerts and mitigation occur.

As part of operationalizing, you create a plan that ensures that log data is available to help with tuning the environment and that your limited resource of people can move from a reactive posture of mitigating breaches to a proactive posture of hunting for breaches that haven't been exploited and collaborating with the internal insider threat team to identify potential holes in the defense fabric of the IT environment.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

Some **keys** to modeling this workstream:

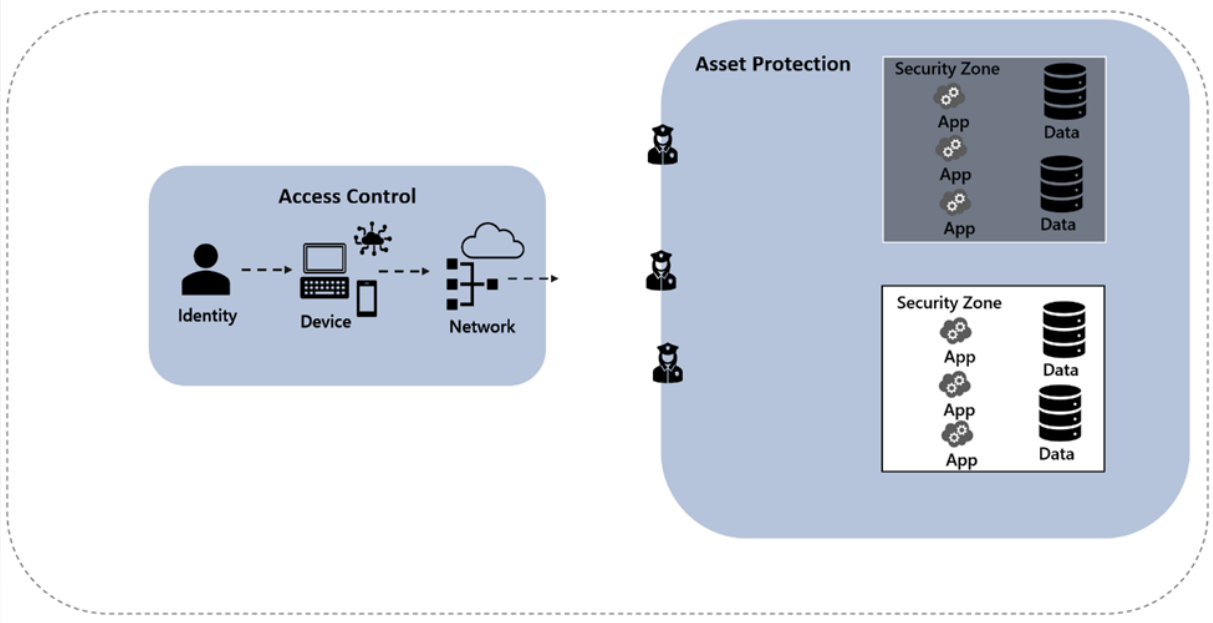
- Start by creating security zones for high-value assets.
- Determine what automation is already in use from a cybersecurity perspective. Everything that can be automated should. Start with orchestration (SAO – security automation and orchestration), governance enforcement (AAC - adaptive access control), and security monitoring, detection, and response (SIEM – security information and event management). Collaborate with the people that modeled the pillars to determine the maturity level of automation for each.
- Design a tokenization solution that reduces the threat surface area.
- Identify the policy enforcement points (PEPs), and associated policy administration, decision, information, and retrieval points (PAPs, PDPs, PIPs, PRPs).
- You can't do it all at once and certainly won't be able to get funding for everything, so put together and prioritize your automation wish list, and determine the alignment with business objectives and ROI compared to the other roadmap efforts.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

Modeling Security Zones

Security zones provide the framework or scaffolding to organize like-valued and like-requirements assets. They enable you to enforce fine-grained access controls, mitigate risks, and protect critical assets by compartmentalizing and isolating different parts of your IT environment based on trust levels and security requirements.

The exercises of modeling the identity, device, network, infrastructure, apps, and data pillars, along with the comprehensive lists of assets and their associated resources provide the information you use to define security zones. A good logical starting point for either creating security zones or evaluating existing ones is with data and assets. A starting point might look like this:



Don't let having a perfect or complete catalog of data and assets get in the way of getting started or of a good enough improvement to have an incremental impact. Consider using an approach or process like the following:

© 2023 Sustainable Evolution, Inc. All rights reserved. |

1. Create one or more zones for critical data and assets such as sensitive data and high-value assets. To do that, use the data you collected from the data modeling exercise to identify data and assets focused on customer information, intellectual property, financial records, and any other sensitive data. Create one or more security zones based on the criticality and potential impact if compromised.
2. Create one or more zones for sensitive data. Sensitive data requires higher levels of protection due to legal obligations, industry regulations, and internal policies. For instance, personally identifiable information (PII) and trade secrets may demand stronger safeguards. Create one or more zones based on the risk posed by each data category.
3. Map asset dependencies to determine if security zones or another approach is best suited to mitigate the risk. Identify the systems, applications, and infrastructure that rely on each other to function properly. By mapping these dependencies, you can identify potential weak points and ensure adequate protection is in place to maintain the integrity and availability of critical assets.
4. Use the principle of least privilege (PoLP) to restrict resource access to only what is necessary for users and systems to perform their specific functions. By minimizing privileges and implementing granular access controls, you can reduce the attack surface and limit the potential impact of compromised credentials.
5. Use network segmentation and micro-segmentation to divide your network into segments or zones based on trust levels and resource types. This segmentation helps contain potential breaches and limits lateral movement within your environment. Consider factors such as data sensitivity, user roles, and application dependencies when defining network boundaries and establishing connectivity rules.
6. Use existing risk assessment data or perform risk assessments to understand the potential threats and vulnerabilities that might compromise your data and assets. Identify internal and external risks, such as unauthorized access, insider threats, malware, or physical theft. Prioritize risks based on their likelihood and potential impact, allowing you to allocate resources efficiently and implement targeted security controls.
7. Use the results of your security zone exercise to update the initiative roadmaps. Based on the insights gained during this exercise, you can update the roadmap to include projects to update access controls, encryption, monitoring systems, intrusion detection, and incident response protocols based on the sensitivity and criticality of each data type and asset.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

Modeling Automation Tools

The primary focus of this exercise is on modeling the tools for:

- Governance enforcement
- Monitoring assets and operations for compliance with the governance
- Detection and response to anomalies such as breaches and attacks.

That said, it is also a good time to review the automation for identities, devices, networks, and infrastructure/services. Changes might be required to maintain alignment with changes to governance that enables your Zero Trust strategy. Additionally, performing evaluations between your current solution and other top-rated solutions to ensure you maintain the best cost performance and can plan for updates to platforms is critical. Automated environments that might need review include:

- Infrastructure as code (IAC) and software-defined networking (SDN) automation
- Identity and Access Management (IAM) tools
- Role-based, attribute-based, and policy-based (RBAC, ABAC, PBAC) access control
- Container, serverless, and no-code solutions
- Endpoint security automation with an eye out for any opportunity to minimize the diversity and complexity of the landscape while maintaining a balance between useability and security.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

For governance enforcement, key tools are your security automation and orchestration tools. If you have a solution in place, verify that it is still fit for function to enable your Zero Trust initiative. As you evaluate your current solution and other tools that are available, you'll want to consider budget, support and maintenance, vendor reputation, and future roadmap along with the following:

- **Ease of use and user experience** – If the solution is good but not easy to use, more time is spent manipulating the tool than operating the usage and output provided. Additionally, logs are great, but critical data can quickly get lost in a sea of logs if logging options and filtering capabilities are not useful. Evaluate its interface, customization options, and reporting capabilities. A user-friendly and intuitive tool allows security teams to quickly adopt and leverage its functionalities. Look for features like customizable dashboards, visual workflow builders, and comprehensive reporting to facilitate efficient and effective security operations.
- **Integration capabilities** – Verify that your current solution is still a good fit for your future state and evaluate other solutions to determine if there is a better solution based on your criteria for use. Evaluate its compatibility with the range of security products and technologies you currently use, such as firewalls, endpoint protection, identity and access management (IAM) systems, and SIEM platforms. Robust integration capabilities enable seamless information sharing, automated workflows, and coordinated responses across your security ecosystem.
- **Automation and orchestration features** – With all the modeling and new information uncovered, you must verify that the SAO tool that you use is still the best choice. Assess the tool's automation and orchestration capabilities in the context of Zero Trust. Look for features such as workflow automation, playbook creation, incident response automation, and policy enforcement. The tool should support the automation of security processes, such as access control, authentication, threat detection, and incident response while enabling customization to align with your Zero Trust architecture.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

- **Scalability and performance** – With digital transformation and the evolution of the workplace and products, the digital workload you must secure and support has increased exponentially. Evaluate its ability to handle the volume of security events, alerts, and workflows generated by your environment. Ensure that the tool can efficiently process and respond to events in real time without significant delays. Scalability is particularly important for larger organizations or those with complex infrastructures and high event volumes.
- **Analytics and threat intelligence** – A key feature for you to consider when you evaluate your SAO tools are their ability to provide advanced analytics and threat intelligence capabilities. These features enable you to gain insights from security events, identify patterns, and detect anomalies. The tool should leverage machine learning, behavior analytics, and threat intelligence feeds to enhance threat detection and response. The ability to correlate and analyze security data across your environment can significantly strengthen your Zero Trust implementation.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

Modeling a Tokenization Solution

As you model your tokenization solution, make sure and have the right team assembled to ensure the solution and implementation. The skills needed across the team members must enable them to:

- Consider the scope and sensitivity of the data.
- The methods and controls are aligned with initiative goals.
- Integrate with current and planned authentication and authorization systems.

The team you assemble should include the following roles:

- Security Architect
- Data Architect
- Cryptography expert
- Identity and access management specialist
- Compliance officer

The team should be sized and skilled to enable speed in decision-making with minimal friction based on personal biases. While the specific roles and titles may vary across organizations. Some roles may overlap or be fulfilled by individuals with multiple responsibilities. Effective collaboration and coordination among these roles, along with input from other stakeholders such as IT administrators and application developers, contribute to a well-designed tokenization solution for a Zero Trust initiative.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

As you start your modeling exercise start with the following three objectives and add others and discovery uncovers any gaps that might hamper success:

- Data sensitivity and tokenization scope – Tokenization replaces sensitive data with randomly generated tokens while maintaining referential integrity. The efficiency of tokenization has a significant impact on the cost and efficiency of the solution. Thoroughly assess the sensitivity of the data that requires protection and determine the scope of tokenization. As part of identifying the appropriate scope for tokenization, consider the most critical and sensitive information that requires tokenization while minimizing the impact on business processes. Identify the specific data elements or fields that need to be tokenized to minimize risk exposure. Scope creep is bad, but expansion might be easier than deflation of scope.
- Tokenization method and security controls - Evaluate different tokenization methods and select the one that aligns with your Zero Trust architecture and security requirements. There are various approaches to tokenization, including format-preserving tokenization (FPT), tokenization with encryption, and secure vault-based tokenization. Each method has its strengths and weaknesses in terms of security, performance, and maintainability. Consider factors such as the strength of tokenization algorithms, key management, and the ability to maintain data privacy and compliance standards.
- Integration with existing and planned authentication and authorization systems - Consider how the tokenization solution integrates with your authentication and authorization systems. Tokenization should support the secure exchange and validation of tokens between trusted parties. It should integrate with your identity and access management (IAM) infrastructure to ensure that only authorized users or services can access tokenized data. Seamless integration with authentication protocols such as OAuth or OpenID Connect enables secure and trusted exchanges and supports the Zero Trust principles of strict access control and authentication.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

During implementation, you must implement strong security controls to safeguard tokenization processes and storage. This includes robust access controls, encryption of tokenized data at rest and in transit, and secure key management practices. Ensure that the tokenization solution integrates seamlessly with your overall Zero Trust architecture, allowing for consistent enforcement of access controls and data protection policies across the entire ecosystem.

Ensure that the tokenization solution integrates effectively with your data storage and retrieval systems. This enables efficient token-to-data mapping, ensuring that authorized parties can retrieve the original data when necessary while maintaining the security and privacy benefits of tokenization.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

Modeling Policy Enforcement Points

With earlier efforts, most of the information you need to model a policy enforcement mechanism you have. However, you still need to process the data to determine the primary points where policy enforcement is required.

You also must ensure that you can implement and operate your enforcement points given the greater detail you uncovered while modeling the pillars. After that, you must validate that what you're proposing aligns with the Zero Trust strategy and business objectives. The three primary objectives for this modeling exercise might be the following.

We recommend that you break your team for this initiative into three small groups and run the efforts concurrently. ·Identify key entry and exit points - Identify the key entry and exit points within your infrastructure where policy enforcement is necessary. Include network gateways, firewalls, web application gateways, cloud access security brokers (CASBs), identity and access management (IAM) systems, and API gateways. Evaluate the network architecture, data flows, and user access patterns to determine the critical points where policy enforcement is required.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

- Identify key entry and exit points - Identify the key entry and exit points within your infrastructure where policy enforcement is necessary. Include network gateways, firewalls, web application gateways, cloud access security brokers (CASBs), identity and access management (IAM) systems, and API gateways. Evaluate the network architecture, data flows, and user access patterns to determine the critical points where policy enforcement is required.

- Assess existing security infrastructure - Evaluate your existing security infrastructure to identify components that can serve as policy enforcement points. Determine if any existing solutions, such as firewalls or IAM systems can be leveraged to enforce access control policies effectively. Assess their capabilities, compatibility, and scalability in the context of Zero Trust principles. This evaluation helps identify gaps that might require additional solutions or enhancements.

- Select policy enforcement mechanisms - Identify existing mechanisms and choose additional mechanisms to enforce access control policies at the identified points. Examples include technologies like network firewalls, web application firewalls (WAFs), micro-segmentation solutions, IAM systems with fine-grained authorization capabilities, and cloud-native security services. Evaluate their capabilities, integration options, scalability, and compatibility with your infrastructure.

Gather the team and review the findings and recommendations. Once some level of agreement is reached throughout the team, ensure that alignment with the Zero Trust strategy is maintained and document the measurable achievement expected along with the constraints and assumptions used in the estimation.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

Modeling the Policy Pieces

This is the point where all the other work and modeling come together to ensure your overall automation considers the information and insights collected and the operationalized solution achieve the goals of the Zero Trust initiative in a measurable and meaningful way.

The tool(s) you keep and the ones you replace must be able to enforce security policy in an automated fashion, be transparent enough to be monitored and tuned, and provide the information needed to inform incident responses and provide the hunter team to complete their mission.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

Validate the alignment of the tools you select with the mechanisms modeled as part of this initiative as well as mechanisms that are already in place. Examples include:

- Resource and security zones
- Least privilege access mechanisms
- Attribute-based access control (ABAC) and other access controls in use
- Policy enforcement points (PEPs), and associated policy administration, decision, information, and retrieval points (PAPs, PDPs, PIPs, PRPs)
- Automation and Orchestration tools (SAOs)
- Continuous monitoring and adaptive policies enablers and mechanisms

Consider reviewing SIEM templates or Sigma rule sets to verify you have a complete and holistic view of your environment and the security controls needed to achieve your initiative's goals. Regular policy reviews and updates are an absolute must. Even with the very best effort to gather insight and model solutions for the overall initiative, the IT and security environment for IT is always changing so tuning and modeling against new threats is constant.

As you define access control policies, verify the policies can and are enforced, and that baselines are set for initial implementation. Additionally, verify that the policies are necessary and align with your Zero Trust objectives and security requirements. Consider factors such as user roles, data sensitivity, device posture, network location, and contextual attributes.

The policies you design should encompass both preventive detective measures. Examples of preventative measures include blocking or allowing access based on policy rules. Examples of detective measures include logging and alerting capability to uncover suspicious activities.

Other

© 2023 Sustainable Evolution, Inc. All rights reserved. |

Modeling a Tradeoff and Prioritization Matrix

You can't do it all at once, but you should have a comprehensive list of projects. The projects should show alignment with the Zero Trust initiative and expected business value and impact on risk, as well as alignment with overall business objectives.

As you populate the matrix, make sure and capture dependencies between efforts. As you go through your prioritization effort, consider the human dynamics aspects of the prioritization. Some key things to consider include:

© 2023 Sustainable Evolution, Inc. All rights reserved. |

- Efforts to protect the highest value assets should occur as the tacit knowledge of the organization reaches the tipping point of the highest team capability, organizational visibility, and excitement and support by leadership. For example, you might tackle PII data efforts or your company's most sensitive data at the peak.

- Efforts first on the list should have a high probability of success and be able to be completed in minimal time and at minimal cost. For example, requiring multifactor authentication (MFA), using passwordless authentication mechanisms, or requiring the use of global administrative privilege must be executed on a privileged access workstation (PAW). These are good candidates because the scope of people impacted is small and includes very technically competent people. The cost for implementation, risk, and training needed should be minimal, which helps with shortening the length of the project.

There are no right or wrong answers with prioritization, just a need to get the first steps started quickly and improve as you go. We've been saying this is a one-bite-at-a-time initiative, but now, you should have a full view of what needs to be eaten, and you should have a good plan of attack.

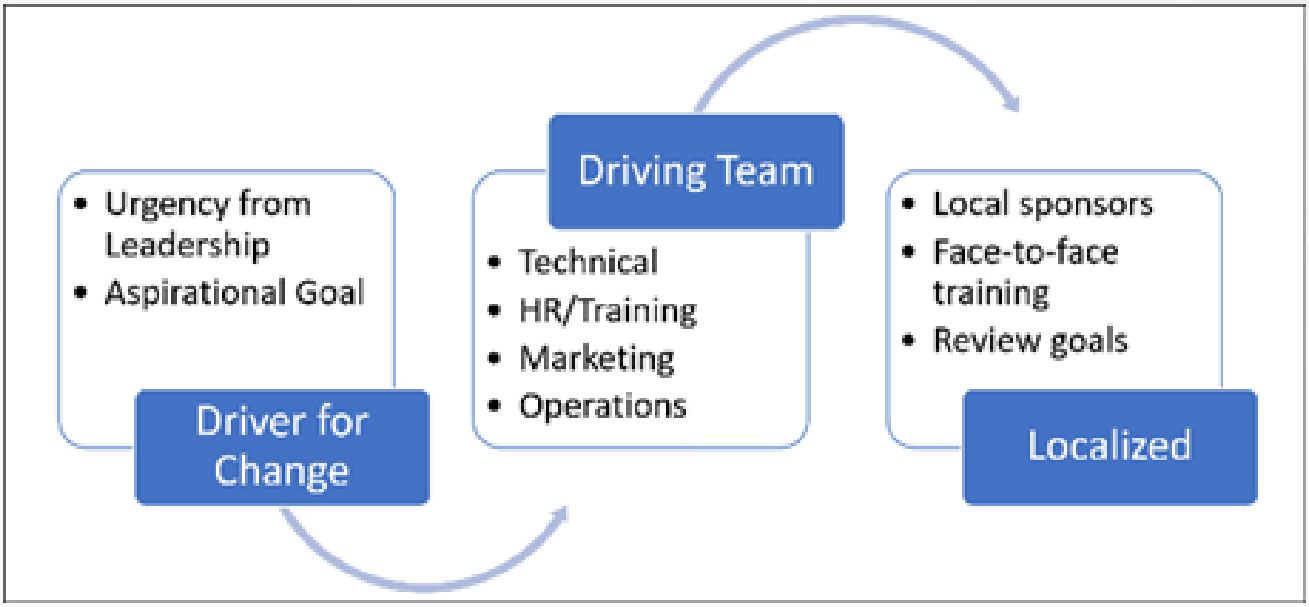
© 2023 Sustainable Evolution, Inc. All rights reserved. |

Change Management

Change management isn't any different for Zero Trust than it is for any other big initiative.

But most of us aren't very good at change management. And security and cybersecurity are not sexy. And most people want their security to be minimally invasive and as unnoticeable as possible. And most leaders get no top-line/bottom-line joy from spending money on Zero Trust initiatives. And Zero Trust doesn't drop new features and functionality for a product at the end of a sprint.

But you still need change management so that you can gain endorsement from leadership, drive urgency or aspiration in stakeholders and users, and drive long-term cultural change.



© 2023 Sustainable Evolution, Inc. All rights reserved.

Three key areas you can focus on as you get started:

- **Get leadership engaged** – If the culture of your organization is driven by urgency, craft a message and plan that leverages urgency. If the culture is driven through aspiration, use aspirational vision and goals. Either way, get leadership on board to deliver the message.

- **Create a communications strategy** – The strategy must include the rhythm and mode of communications, as well as the context and content of the communications for leadership and sponsors, leads and key centralized players, local mavens, and users. Persuasive communication is what the marketing team does well. Get them involved.

- **Training, support, and rewards** – The training does not need to be slick and pretty, but it does need to be informative and available. Online, through lunch-and-learns, recorded videos. Support must be available when someone gets stuff, and a recognition or reward system will help drive participation as a carrot, the annual review process as the stick.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

Resources

There is a change management standard created to meet ISO specifications for standards creation, and several change management processes you can use to drive change.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

ACMP

The Association of Change Management Professionals (ACMP) maintains a standard for change management that describes in about 70 pages how to create and drive a change management plan. Their standard shows a step for closing the change management process. However, we feel that Zero Trust and cybersecurity are ongoing efforts that will always require change management so closing the effort might never occur.

They also offer a certification, so if you are looking for a change management resource this is a good way to narrow down your search.

There are also several processes for change management that you can apply and align well with the ACMP standard.

As you create your strategy, determine which process, or processes you might leverage to help with driving change based on the culture of your organization.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

Changefirst

Changefirst is a methodology that breaks change management into efforts at the organizational level and efforts that must occur locally.

Organizationally:

- The **shared change purpose** is the aspirational message that the leadership must be onboard to deliver to the organization to motivate the people that must change to change.
- **Effective change leadership** is the plan you develop to guide the change effort.
- The **powerful engagement processes** are the implementation or activation of the plan.

Locally:

- **Local sponsors** are the hammer that drives the change at the end-user level.
- Build a **strong personal connection** so the person that must change knows and feels they must change.
- **Sustained personal performance** is about monitoring the people that are changing to collect feedback and make needed adjustments.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

Using multifactor authentication rollout as the change, here is an **example** of what Changefirst might look like:

Our case for change is to change authentication so that we strengthen the verification process during end-user authentication while balancing security and end-user productivity. We propose we roll out multifactor authentication (MFA) across the organization.

- *To be successful, we must enroll HR leadership to provide the MFA and training to new hires, delivery, and operations team leads to train support staff, and use a common authentication mechanism across all solutions.*
- *During an all-hands, leadership must announce their support and endorsement of zero trust and spotlight it as a big annual initiative for the organization.*
- *We must plan a local "road show" going to the list of key stakeholders to present the zero-trust initiative and get their support.*
- *For annual reviews, we must include a personal review goal that rolls up to achieving zero trust KPIs.*
- *Provide ongoing training and presentations by experts on best practices using MFA and create a feedback mechanism to solicit suggestions for improvement.*

Changefirst has two methodologies on its website. For change management, you are interested in People-Centered Implementation (PCI). There are online assets you can purchase with templates and tools for using the methodology. There's a short (3-minute) video that introduced the process or you can download a whitepaper from their site that provides additional explanation. To download, you must register, and they email you a link that you use to access the 40-page eBook.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

Kotter-Cohen

The Kotter framework has been around for almost twenty years so there is a lot of expertise and guidance available. The framework has eight steps for leading change:

- **Create** a sense of urgency is "setting the house on fire" and is the message that you ask the leadership team to deliver.
- **Build** a guiding coalition is about building out or assigning change management functions to the core team if the core team will drive the change.
- **Form** a strategic vision is about defining the vision or goal of the change management process to drive adoption of the technical implementation.
- **Enlist** a volunteer army focuses on finding the people that will help drive the change and the influencers that everyone in the organization naturally follows.
- **Enable** action by removing barriers involves running a pilot and then a stepped rollout plan and determining what must change in order to continue rolling out and gaining adoption.
- **Generate** short-term wins focuses on getting successful adoption by a group of people and using them as poster children to inspire others to change.
- **Sustain** acceleration is about creating a plan to continue driving the change after the luster of the short-term win starts to tarnish.
- **Institute** change aims to put mechanisms in place that force the change to stick over time, whether that is through rhythmic training, review process inclusion, or other methods.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

Using the MFA example, it might look like this:

The external threat to our IT environment and our data requires we change our user verification to defend against attacks from bad actors. We must change authentication so that we strengthen the verification process during end-user authentication while balancing security and end-user productivity. We propose we roll out multifactor authentication (MFA) across the organization following these steps:

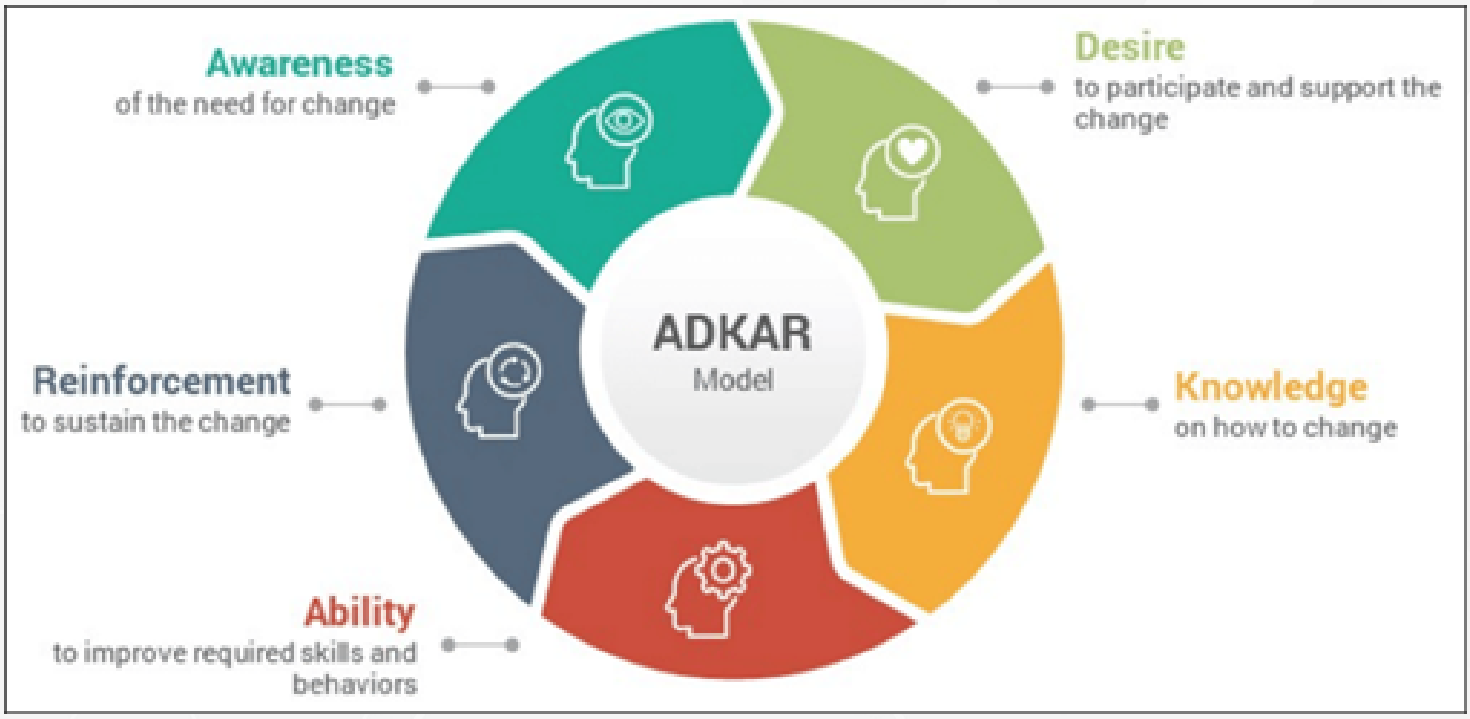
1. ***Increase Urgency**: Negotiated new hire orientation training and provisioning of MFA as part of the onboarding process by <date>*
2. ***Build the Guiding Team**: Onboard stakeholders from HR, Training, Identity Dev, IT Ops, and Ops teams to kick off.*
3. ***Get the Right Vision**: Stakeholders create or agree to the existing mission and vision for MFA.*
4. ***Communicate for Buy-in**: Socialize plan with sponsors, organizational leaders, and members of training, delivery, operations, and support teams.*
5. ***Empower Action**: Provide roadmap, architecture, constraints, and other critical information, and inform "boots on ground" teams where they must confirm and where they can stray from the plan.*
6. ***Create Short-term Wins**: Create and alpha test MFA capability with key stakeholders and early adopters.*
7. ***Don't Let Up**: Security moment at every sprint review and sprint planning meeting.*
8. ***Make it Stick**: Publish refresh training forward schedule for the next two years with HR for internal training.*

On the Kotter website are all the resources you might need to be successful. There is only one framework, however, there are also a set of change principles listed as well. On the 4 Core Change Principles webpage are a link to download an eBook and a series of short videos to describe the principles. We recommend you review the videos (4 minutes each) and download the eBook. To download the eBook, you must fill out a form and they will email a link to the eBook.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

Prosci ADKAR

ADKAR is the acronym for awareness, desire, knowledge, ability, and reinforcement which happen to be the steps in their process. Many consultancies use ADKAR as their change management process.



- **Awareness** focuses on building awareness of the need to change and messaging the nature of change.
- **Desire** is about creating a carrot big enough that people want to support the change, as well as participate and engage in the change.
- **Knowledge** defines how to change and how to implement a new set of skills and behaviors.
- **Ability** aims to get the skills in place and remove any blockers to implementing and adopting the change, as well as demonstrating the performance of the change.
- **Reinforcement** aims to put the mechanisms in place to sustain the change and to build culture and competence around the change.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

Using the MFA example, it might look like this:

For this initiative, we must change authentication so that we strengthen the verification process during end-user authentication while balancing security and end-user productivity. We propose we roll out multifactor authentication (MFA) across the organization. We will use the following change management process:

- ***Awareness**: We are going to drive awareness of the need for change by stating we must implement MFA because we assume we have been hacked and are still vulnerable to attacks.*
- ***Desire**: We need you to set an example by using MFA in a visible manner, quickly migrating to MFA for groups of accounts, and by updating any of your applications you can to MFA authentication.*
- ***Knowledge**: Take the available training on MFA or if you are an expert, host a lunch-and-learn to grow others. If possible, host a hackathon to grow our community of technologists' skills for MFA and produce innovations for its usage.*
- ***Ability**: Implement MFA and provide visibility to metrics that show the impact using numbers.*
- ***Reinforcement**: Consider doing a presentation on the impact of MFA during team meetings or all-hands meetings.*

Prosci has a few models and processes listed on their site. This one is easy to implement and meant to drive individual change. They also have a nice primer for change management.

You register and are sent a link to the actual 17-page eBook. They also have a set of six resources you can register to download that help with ADKAR. When you register for this resource, a zip file containing the six PDFs is downloaded to your device. Each file is about 3MB.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

~~VitalSmarts~~ Crucial Learning Influencer

Influencer is a model designed to change ingrained human behavior. The other frameworks presented feel like the requisite change is in the center of the framework and the people are at the edges.

This framework feels like it is centered on the human behavior that must change and the change is on the edge.

The columns are broken into defining how to motivate people to change their behavior and what competence must be added using what manner.

The rows describe the level of change from the individual to the herd, and then to structure.

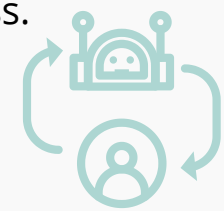
	Motivation	Ability
Personal	1 Make the Undesirable Desirable	2 Over Invest in Skill Building
Social	3 Harness Peer Pressure	4 Find Strength in Numbers
Structural	5 Design Rewards and Demand Accountability	6 Change the Environment

© 2023 Sustainable Evolution, Inc. All rights reserved. |

Using the MFA example, it might look like this:
For this initiative, we are introducing multifactor authentication. We propose we roll out multifactor authentication (MFA) across the organization providing it first to influencers and then using gamification with a reward of personal perks to motivate adoption. We'll use the following motivators to grow the abilities:

1. ***Personal Motivation**: Enable BYOD devices and work-from-home scenarios for people using MFA. Set up a trivial pursuit-style quiz with the top scorers at the top of the list for receiving MFA capability.*
2. ***Personal Ability**: Funding for training and certification, gamification, and prizes for internal leaders in growing and sharing knowledge. Set up a badge or signage program so local individuals for each product team or group can become the "floor Expert".*
3. ***Social Motivation**: Make the MFA device an employee status symbol. Award custom phone cases and badges in the employee directory to apply peer pressure.*
4. ***Social Ability**: Sponsor lunch-and-learn or hackathons for MFA development and improvement. Have the Floor Expert drive the events and act as a liaison that provides feedback to the core team.*
5. ***Structural Motivation**: Implement a "bench" program to replace people not meeting commitments in adopting MFA. Assign a temporary backup to fill their role temporarily so they have the opportunity to grow their competence in using the MFA-enabled devices. The person that provides the backfill strengthens their skill while the people in remedial training realize there are consequences.*
6. ***Structural Ability**: Shift MFA from being an optional or role-based requirement to being the required authentication method for everyone. This is setting up policy and standard operating procedure (SOP) that requires adoption. SOPs and policies are almost always driven by a nameless "They" who is requiring the policy. And it really doesn't matter whether the "They" is internal or external, good or bad actors. It is simply someone that makes this required change beyond local control.*

Vitalsmarts did have a model named Influencer. It is now part of the Crucial Learning set of courses (good courses) so it is a bit harder to find a lot of information online. This diagram represents the model when it was driven by Vitalsmarts.
Crucial Learning has books and courses, and a YouTube channel, but to effectively use it you need to pay for some training and invest time in formal education on change management. We recommend if you use this framework that you find a consultant with experience driving initiatives with this process.



© 2023 Sustainable Evolution, Inc. All rights reserved. |

Final Thoughts on Change Management

With Zero Trust, change will be constant and forever so a goal of change management should include creating a culture of change. Most people like routine work where they gain competence in their role and focus their career on execution. Creating a culture where change is constant and is not limited to Zero Trust can help.

This interview with Mike Farabelli provides lessons learned that reinforce the steps the frameworks we presented provide structure to. It's a short and worthwhile read.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

Conclusion

From a business perspective, Zero Trust strategies can be as tough as shifting to:

- Zero-based budgeting and OPEX over CAPEX
- IT resources being distributed into LOBs
- Agile development practices
- Hybrid or cloud-based computing
- Microservice/container/SaaS/serverless solutions
- BYOD and IOT (and IOT and IOT) and OT
- A digital component for every product or service

Wait. That's the change over the past two decades. But our IT security practices have not changed much during that time. Tools, yes. But change to the strategy driving security to map to the changing environment? The current strategies are largely using the same approach we used when datacenters sat inside fenced walls and secure buildings.

Zero Trust is a big change that affects every employee in an organization. The initiative must be approached like other big business strategy changes that impact the entire business. To be successful, the initiative must:

- Have executive sponsorship and endorsement from the entire C-Suite and Board of Directors.
- Be planned to start fast, show short-term success, and adapt as more insight is gathered.
- Have stakeholders from across the entire organization invested, with something to lose if it fails, and have one of their leaders on the core collaboration team.
- Have collaboration between offense and defense, with architecture and delivery teams being offense and SecOps and Ops being defense.

Perhaps most importantly, for Zero Trust initiatives to succeed, **automation** and **change management** are **required**, not optional.

© 2023 Sustainable Evolution, Inc. All rights reserved. |

Additional Resources

Zero Trust for Architects course

Sustainable Evolution's Zero Trust for Architects course is designed to help you understand how to drive an initiative to gain a Zero Trust security posture for your IT environment. The training is based on the guidance available from government entities, standards groups, and cloud-based products and services companies.

This instructor-guided online course is fourteen classroom hours long. Our typical delivery is six weeks long and includes suggested reading as homework between each session. The course starts with planning a Zero Trust initiative and takes you through the process of planning for the key pillars of a Zero Trust framework.

We share our experience and strategies on how to assemble a team, scope out each pillar, and assess your current security state. We provide links to Zero Trust content for the major cloud service providers.

COURSE OBJECTIVES

By the end of this course, you will be able to:

- Create a set of principles to guide a Zero Trust initiative.
- Assess your current Zero Trust maturity state.
- Use Forrester TEI reports to perform cost-benefit analysis on Zero Trust initiatives.
- Use causality mapping to roadmap Zero Trust initiatives to business objectives.
- Plan Zero Trust solutions to achieve boundary and segment restructuring.
- Determine the skills needed for core and extended teams on Zero Trust initiatives.
- Set a Zero Trust strategy for identities.
- Set a Zero Trust strategy for endpoints.
- Set a Zero Trust strategy for networks.
- Set a Zero Trust strategy for infrastructure.
- Set a Zero Trust strategy for applications.
- Set a Zero Trust strategy for data access and management.
- Automate security policy management.
- Use logged information to perform manual and automated intrusion detection and response.
- Create a change management plan for Zero Trust initiatives.
- Create a communications plan for projects and initiatives related to Zero Trust.

Sign up at sustainableevolution.com/training

© 2023 Sustainable Evolution, Inc. All rights reserved.