Seven Elements of a Highly Successful Zero Trust Architecture

Cyber Security Summit Webinar Series
March 28th, 2023

Speaker: Brian Deitch, Chief Technology Evangelist, Zscaler

Moderator: Judy Hatchett, VP, CISO, Surescripts

Report Author: Joseph Mathias, Executive Coordinator, Cyber Security Summit

Speaker Bio:
Brian Deitch is the Chief Technology Evangelist at Zscaler and has been in the security industry for more than a decade. Brian is passionate about helping organizations adopt secure, reliable, and scalable cloud-based solutions that make the internet safer for everyone. He's an expert in cloud security, zero trust, and SASE/SSE and how to use these principles to design and implement digital, network, and application transformation.

Introduction:
Zero Trust Architecture is a cyber security strategy where every access to the network is treated exactly the same, as a threat. Only by using specific authentications can you access and send data through the network. At its core Zero Trust has three tenants; terminating every connection, protecting the data using context based policies, and reducing risk by eliminating attack surfaces.

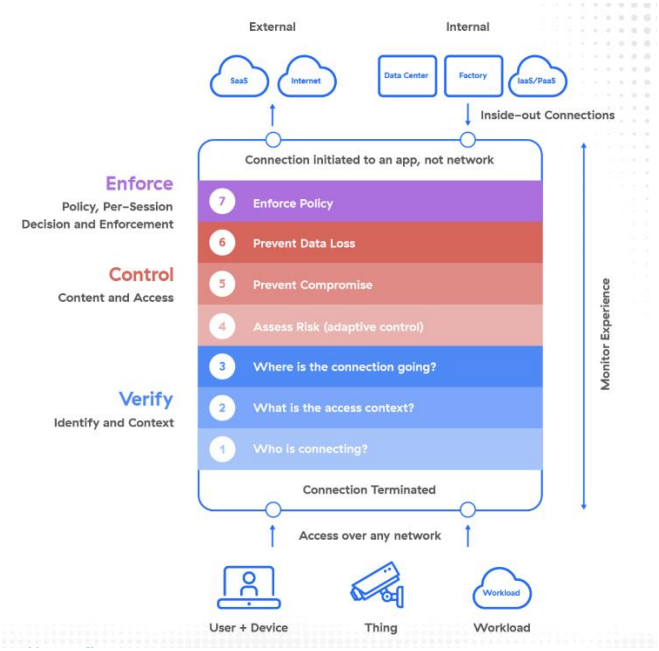
Terminating every connection deals with malicious files. By just using firewalls it can be too late to prevent anything from happening but by blocking the connection using Zero Trust Architecture before any file can be moved it greatly reduces the risk of damage. Protecting the data using context based policies deals with verifying access requests and rights based on the context, such as device, location, applications requested and the policies can be altered to deal with sudden changes. Finally reducing risk by eliminating attack surfaces deals with connecting to applications, by using Zero Trust Architecture users are connected directly to the resources they need eliminating the risk of compromised devices infecting other resources.

The Seven Elements:
The Seven Elements are broken down into three sections; Verify, Control, and Enforce. Each of these have specific functions but they all work together in order to enforce Zero Trust in your cloud and applications. The first steps are Verifying that the person accessing the info has the correct identity. The things that are looked for are who is the user, what's the access content, and where is it going. So who is the user? By checking the identity of the user against who is allowed access using a multitude of verification methods we can confirm the identity of the user. The next part is looking at what device they are coming from. Is it a company owned device or a personal pc, where are they going to access the content are just some of the questions looked at to identify the user. And finally, where is the user attempting to go. If the access is coming from a sanctioned device is it trying to access the private cloud, a SAAS application, or the internet. Based on these reasons access can be denied or granted very easily.

The second step in the Seven Elements is Control. Whether the user has been verified or not, you have control using the Zero Trust Architecture. The three sections of control are assessing the risk, preventing compromise, and data loss prevention. For assessing the risk, we have to look at what files the user is

trying to access or upload. If they are attempting to upload something nefarious to the internet or cloud then this action can be stopped immediately before it goes anywhere. The second section is preventing compromise. With Zero Trust you can identify malicious files before they ever enter your systems. Brian Deitch developed a system for his website that allows people to upload files for posts and if the file is detected to be malicious it gives it a score out of 100 in how dangerous it is and can prevent the file from being uploaded. The final section deals with data loss prevention, something that is impossible to avoid but accidental data loss can be prevented. Using things like exact data match, index document matching, and azure information protection you can help prevent these accidental data losses. There might be a lot of false positives when checking for data loss, so you have to make sure to filter out the white noise when looking at alerts.

The final step of the Seven Elements is Enforce. Three great ways of enforcing the policy are isolation, blocking, and deceiving the user. The first method is isolation which can allow users to view certain files or websites but not be able to download anything from them. The second method is directly blocking access to certain files, firewalls, and actions. In order to prevent malicious acts such as data theft actions such as copying and pasting from certain documents can be completely blocked. The final method is deceiving the user. A great example of this would be a user attempting to access a firewall they aren't supposed to have access to, instead of accessing the firewall they are redirected to a decoy that captures their information and can be sent to the SOC team for further investigation.



Conclusion:

Zero Trust Architecture is not a method to clean out your systems but rather a method that prevents any malicious files/software from entering your system in the first place. The main steps of implementing Zero Trust are Verify, Control, and Enforce. Verifying guarantees that the right person is getting access to the files. Control is making sure that if they have the right access they can only access appropriate information for their clearance. And finally enforcing your policy allows you to root out potential bad actors in your company while keeping your information safe. Zero Trust is a method we

should move towards because it allows for some of the greatest protections available at the moment without slowing the processes down horrendously.