**The Zero Trust Security Model Using the Five-Step Approach**

Here we see the 5-step approach with a short explanation of each point.

1. **Define the Protect Surface.**

* **Data** – It is possible to have Personally Identifiable Information (PII), Payment Card Information (PCI), Personal Health Information (PHI), organization financial or intellectual property on the Protect Surface.
* **Application** – Identify business applications, listing first the critical ones, all the way to eliminating frivolous applications no longer in use on the Protect Surface.
* **Assets –** List all assets including Storage Servers, SQL servers, AD Servers, controls, endpoint devices such as computers, laptops, printers, tablets, phones, IoT devices such as door scanners, POS machines and equipment on the Protect Surface.
* **Services –** List the services supported by the data, applications and assets that will be affected negatively if there is a breach from most to least critical on the Protect Surface.

1. **Map the Transaction Flows.**

* **Map** - Graphically map the current process flow and identify all breach points.
* **Revise** – Rework the flow process from inside to outside to eliminate flaws and monitor breach points.

1. **How to Architect a Zero-Trust Environment.**

* **Design** – Design for the new process with hardware, software, and training.

1. **Create Zero Trust Policy.**

Use who, what, when, where, why and how to develop network policies. Use the least privilege access rule of the Zero Trust Security Model to segment the network to protect the data.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Who** | **What** | **When** | **Where** | **Why** | **How** |
| **Method** | User-ID | App-ID | Time limits | System object | Classification | Content-ID |
| **On**  **Premise** | Users | Inventory Program | Working hours | Onsite | Toxic (high value) | Decrypt, inspect (security profiles), log traffic |
| **Cloud** | Accounting | QuickBooks | Working hours | USA | Toxic (data has high value) | Decrypt, inspect (security profiles), log traffic |

1. **Monitor and Maintain the Network.**

* [Log](https://docs.paloaltonetworks.com/best-practices/9-0/decryption-best-practices.html) all internal and external traffic to an analytics database.
* Update policies and add new protect surfaces based on the intelligence gathered.
* Identify unusual behavior that may show an intrusion or threat.
* Identify the root cause of alerts and respond immediately.
* Highlight any new protect surface you did not originally consider.
* Use an industry tool to help measure progress toward a best-practice configuration and posture.
* Continue to m[onitor](https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring.html) network activity using standard and custom reports.
* Create training to ensure that existing and new members of your team understand the strategy and the implementation of it.
* Continue to automate actions and responses.