Fortifying your Cyber House: The Path to Zero Trust with Integrated Solutions

January 29, 2025/Jennifer Zientek, Field CTO

Abstract

This presentation explores how integrating various security tools mirrors the systems of a well-secured home, where every element, from the front door locks to the motion detection sensors, plays a vital role in ensuring safety. By connecting these tools, organizations can move beyond isolated solutions and achieve the Zero Trust model- ensuring that no threat, external or internal, can breach the walls of their digital infrastructure.

Goals for Today

- Introduce ideas and talking points
- Use some basic block drawings to use in guiding discussion
- Talk about different scenarios and how integrations are core items in any useful solution

- **NOT** intended to give you an actual architecture for any solution- but to get you **THINKING** about key integrations and solutions

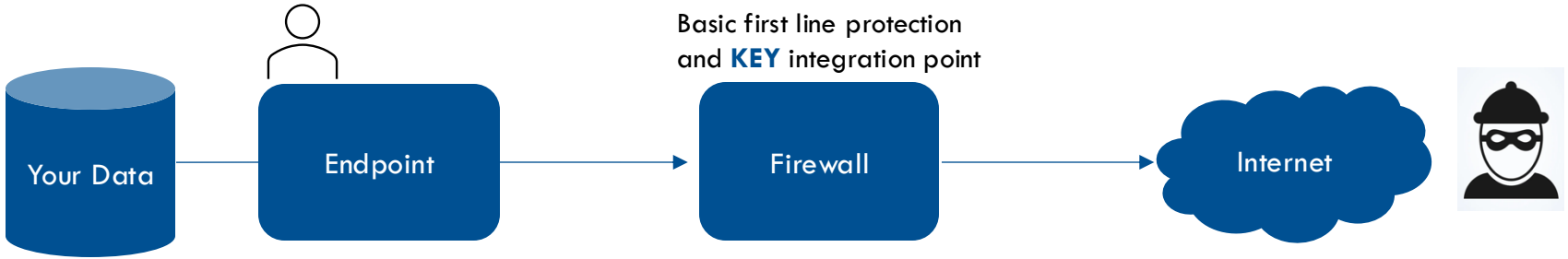
My House

My House- Key talking points

- Top priorities are safety of family
- Integration example: If carbon monoxide sensor goes off anywhere in house, key integrations should signal HVAC system to shutdown to prevent spread of fumes and then call emergency services to assess leak and health of family.
- Mirrored example: Data leak

Case Study: Data Leak

Basic, generic path from a user logged into any endpoint to the Internet through a standard firewall (hopefully application-layer based!!). The firewall is core to most active integrations and a **VERY** important decision for vendor integrations.

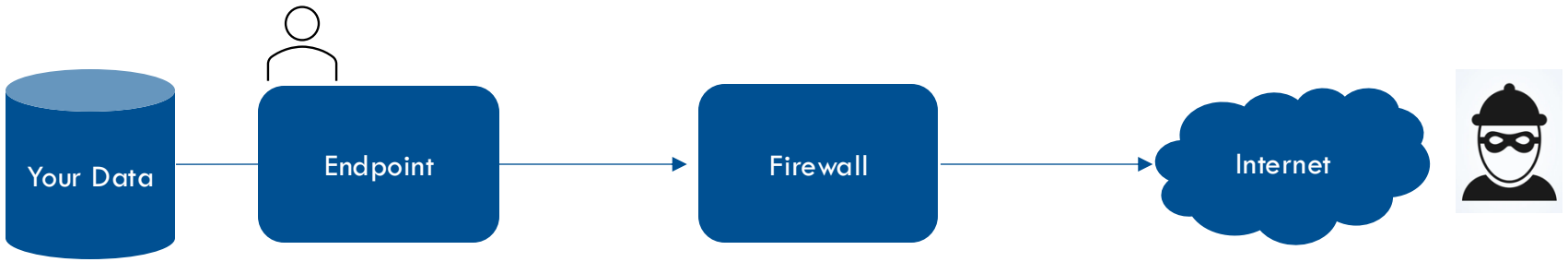


Case Study: Data Leak

SIEM — Generate alerts based on suspicious activity

SOAR — Utilize integrations to automate response actions

User Behavior Analytics (UBA) — Watch for anomalous behavior



Add in a layer of log collection, analytics and orchestration/automation that is at the core of any integrated solution.

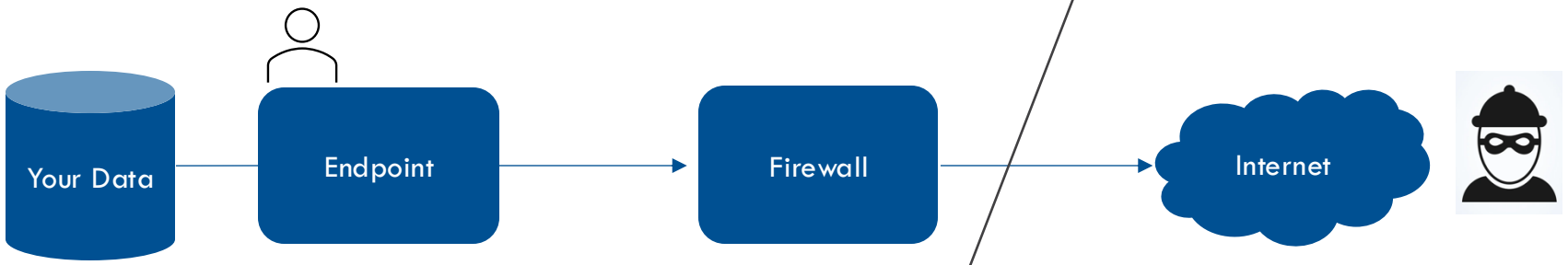
Case Study: Data Leak

SIEM

SOAR

User Behavior Analytics (UBA)

Finally, add in tools that provide additional visibility and ability to prevent certain actions.



Endpoint Detect & Respond (EDR)

Watch for anomalous behavior

Data Loss Prevention (DLP)

Check for potential leak per policies

Email Security

Check for potential leak per policies

The White House

White House- Key talking points*

- Top priorities are safety of WH residents and staff and National Security

- Integration example: If an external actor breached the perimeter gates information about that breach would need to be shared among multiple internal and external groups quickly to kick-off responses. Integration among groups and certain automations are key in order respond to the threat and protect VIPs.

- Mirrored example: Network perimeter breach and stolen identity credentials

***All talking points on this slide are based on fictional examples.**

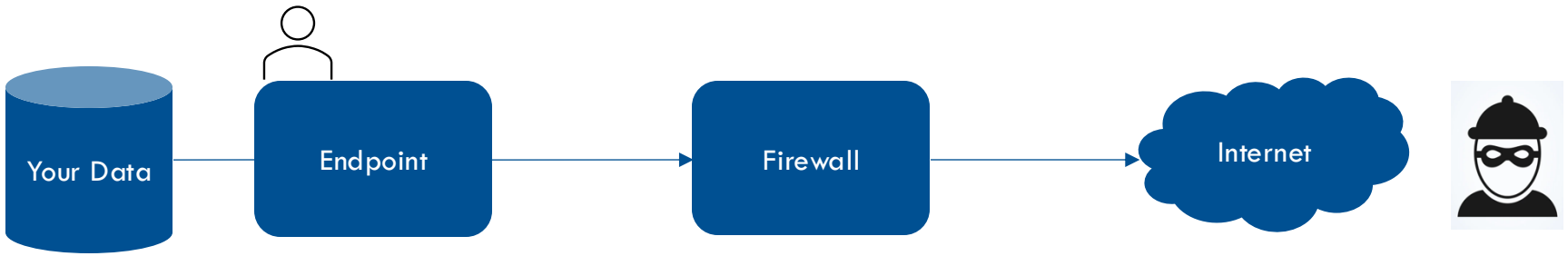
Case Study: Network Perimeter Breach

SIEM

SOAR

User Behavior Analytics (UBA)

We still have the usual suspects in the log and analytics layer with some base tools.



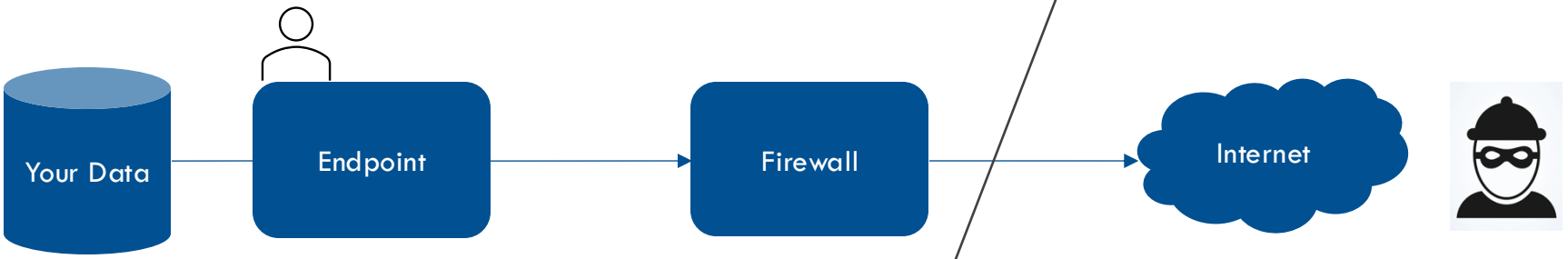
Case Study: Network Perimeter Breach

SIEM

SOAR

User Behavior Analytics (UBA)

Notice how we still have EDR but have now added additional proactive monitoring tools for finding threat vectors and active IOCs.



Endpoint Detect & Respond (EDR)

Generate alerts based on suspicious activity

Network Detect & Respond (NDR)

Pen Testing (Red team)

Continuous monitoring for potential threat vectors

Threat Intelligence Platform (TIP)

Provide insights into actual threats

OPTIV + ClearShark

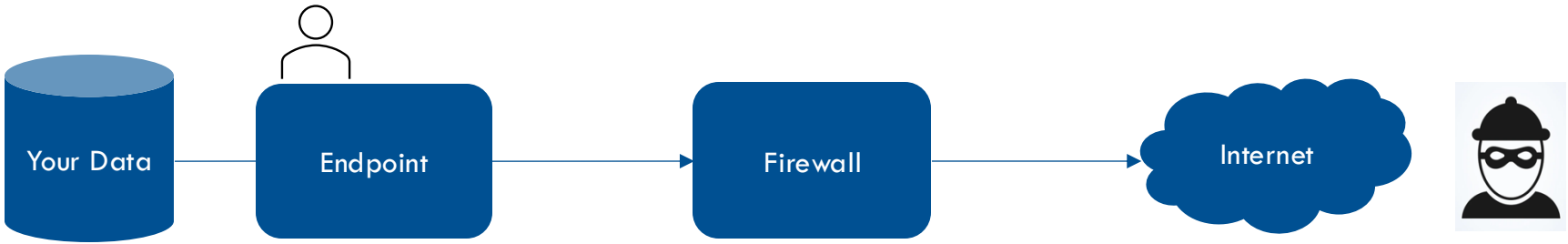
Case Study: Stolen Identity Credentials

SIEM

SOAR

User Behavior Analytics (UBA)

Continuing the theme- we still have the same core tools in the log and analytics layer. Identity information is **CORE** to any SIEM tool having actionable information.



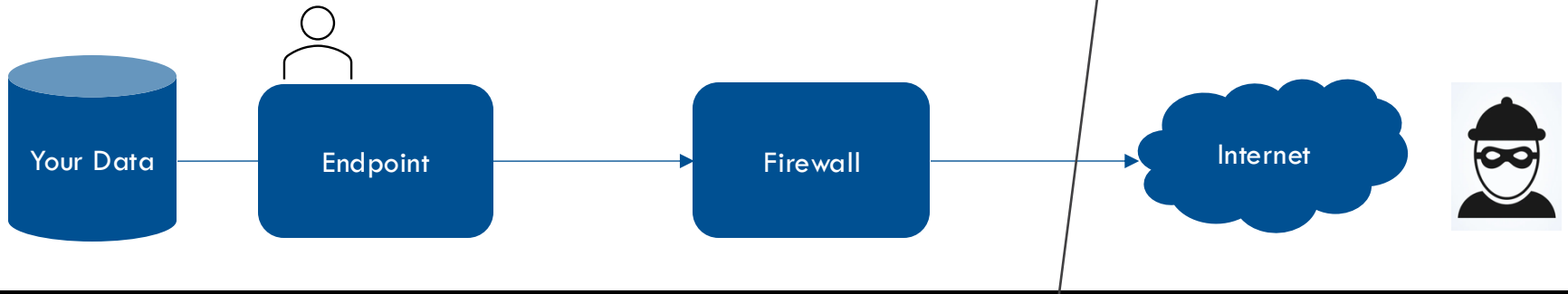
Case Study: Stolen Identity Credentials

SIEM

SOAR

User Behavior Analytics (UBA)

EDR is still a main tool (not shown) but now we have additional proactive and monitoring tools focused on identity.



Identity Threat Detection and Response (ITDR)

Generate alerts based on suspicious activity

Identity/ Credential Management

Core management of user accounts

Privileged Access Management (PAM)

Prioritize management of admin accounts

Multi-Factor Authentication (MFA)

Additional protection for compromised accounts

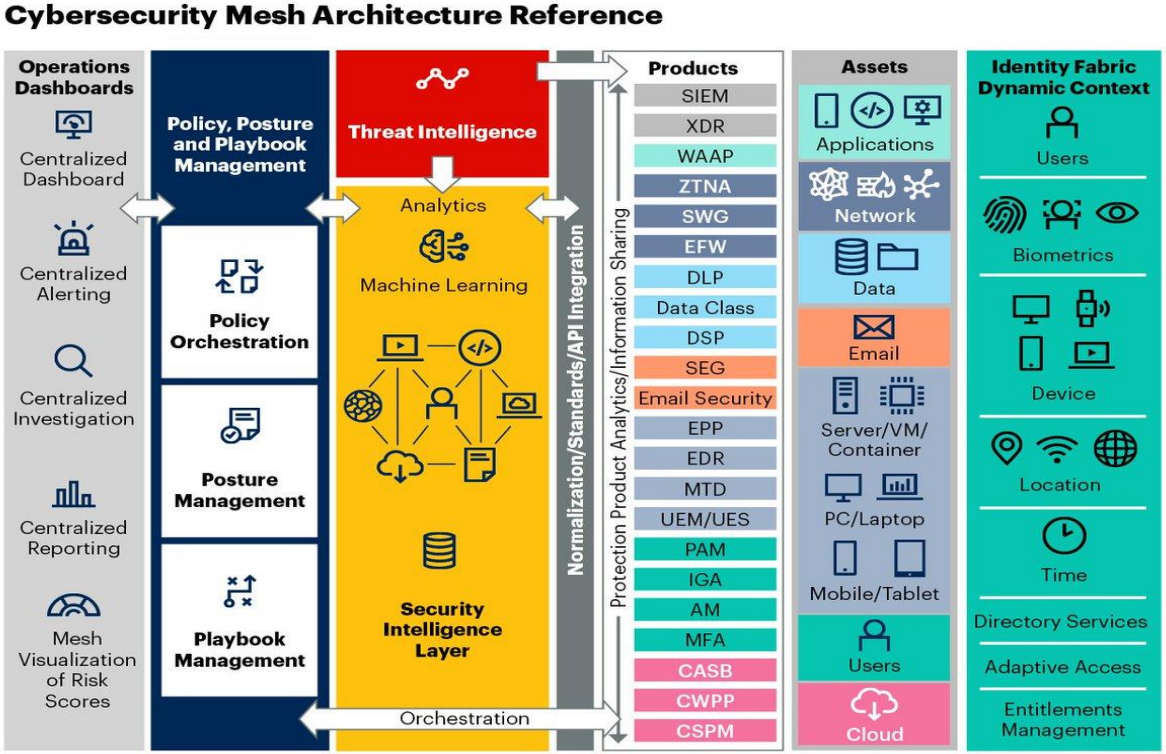
OPTIV + ClearShark

What to look for when selecting tools

- Open extensible APIs
- List of technology partners and descriptions of integrations
- Look for rich integrations and not just surface level
- Ability to work with automation/orchestration software and/or create custom automations/ orchestration
- Software development toolkit to add custom integrations
- Red flags

  - Integrated only with other tools from same vendor
  - Integrations have not been updated in years
  - Limited documentation on integration

Gartner Cyber Security Mesh Architecture (CSMA)



Source: Gartner

Note: Products included in the diagram are not all of the products that can be included but an example list of possible tools that protect assets

754315_C

Gartner

CSMA & ZTA Final Thoughts

Cybersecurity mesh, or cybersecurity mesh architecture (CSMA), is a collaborative ecosystem of tools and controls to secure a modern, distributed enterprise. It builds on a strategy of integrating composable, distributed security tools by centralizing the data and control plane to achieve more effective collaboration between tools. Outcomes include enhanced capabilities for detection, more efficient responses, consistent policy, posture and playbook management, and more adaptive and granular access control — all of which lead to better security. ---Gartner

- ZTA is about creating strict boundaries around users, devices and data, where CSMA is about integrating a diverse set of security tools into a unified, interoperable mesh.
- To achieve success with both architectures the tools you select must offer deep technical integrations and support orchestration and automation as core principles.