Control Assurance

Getting More From What We've Got

Chris Peltz, Senior Security Engineer

GuidePoint SECURITY

What is Control Assurance?

Control assurance are activities aimed at getting more functional output out of a security control set.

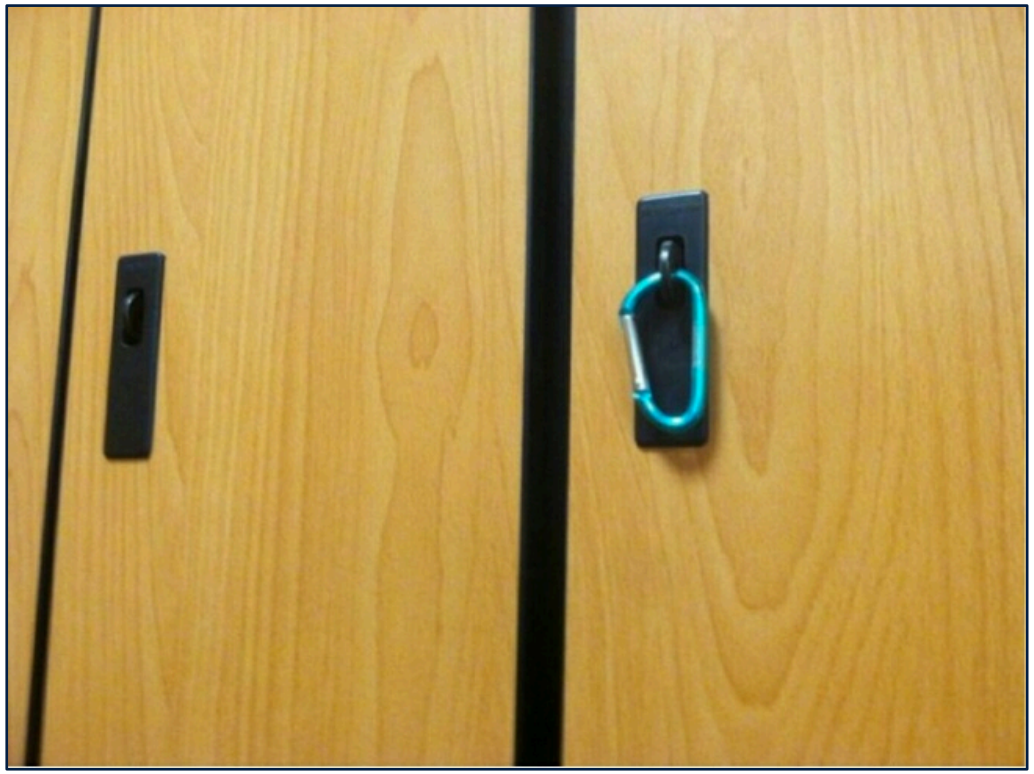
The facets of control assurance are coverage, optimization, and validation.

Why do we care about this?

The deployment and configuration of a tool matter just as much as its quality/efficacy.

Often times we perform gap analysis, but it is less frequent to engage in control assurance.

Why do we care about this?



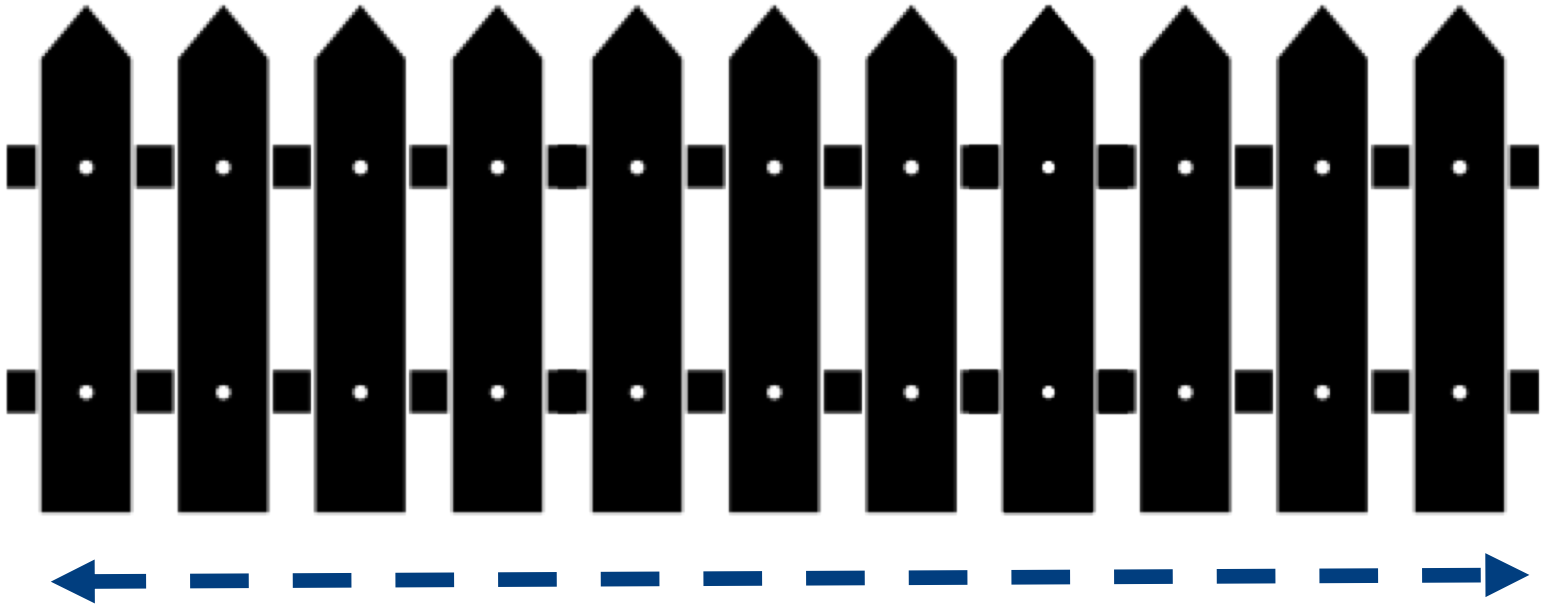
Control Gap Analysis

Control Assurance

How would you protect a pool?

GuidePoint SECURITY

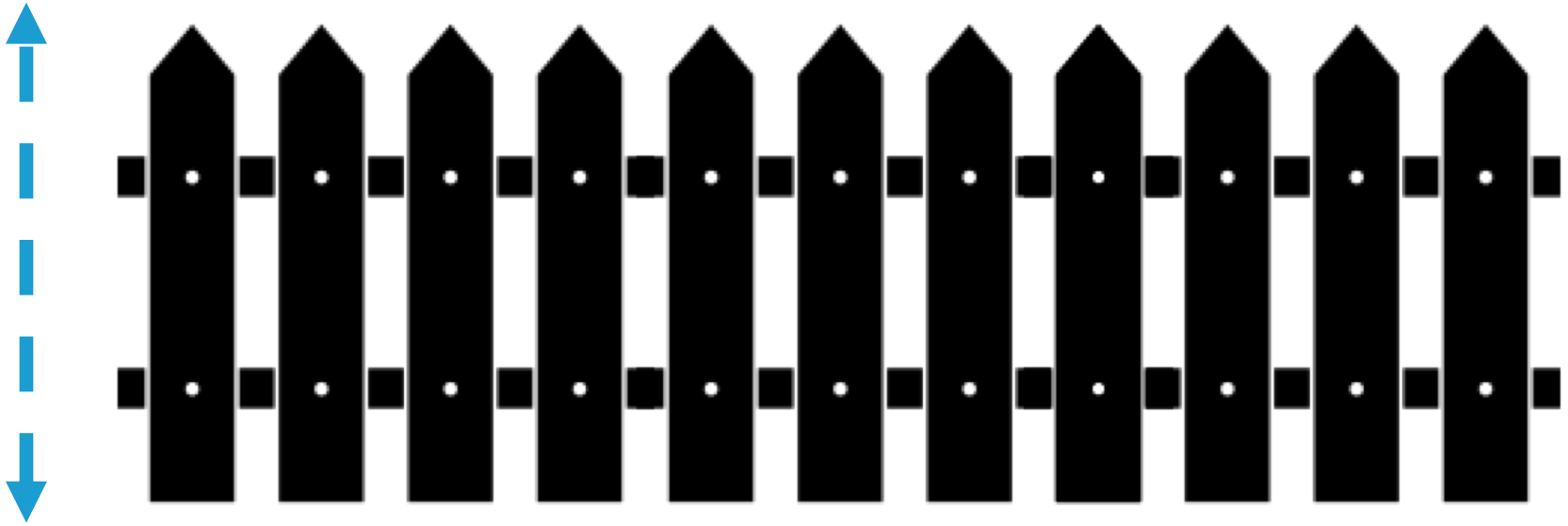
Coverage



Coverage is how much of the pool is surrounded by the fence.

Any part of the pool not covered by the fence is easily accessible.

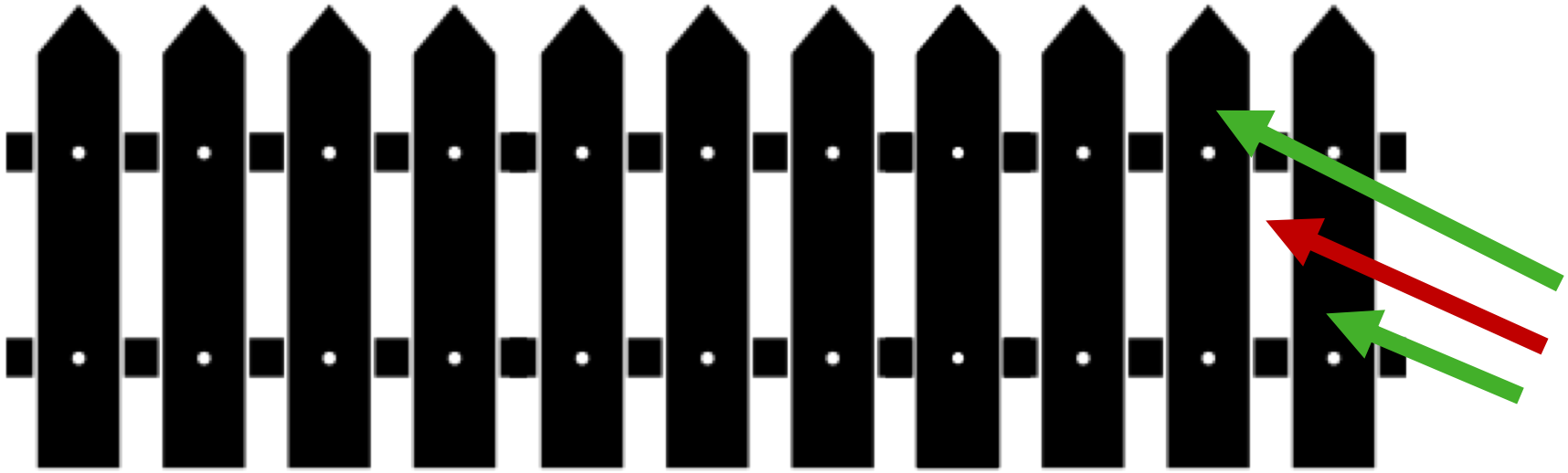
Optimization



Optimization is the height of the fence.

A fence that fully surrounds the pool, but is only 1-foot high is not nearly as effective as a 10-foot fence that fully surrounds the pool.

Validation



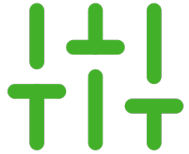
Validation is the strength and integrity of the fence.

Does the fence actually keep anyone out? It may be tall and surrounds the pool, but is it inconsistent or weak, leading to an intruder simply walking through?

Tenets of Control Assurance

COVERAGE

The consistency of a control's implementation.



OPTIMIZATION

The maturity and business relevance of a control's configuration.

VALIDATION

The integrity of a control's functional state.

GuidePoint SECURITY

Coverage

The consistency of a control's implementation across the enterprise.

- Endpoint agent coverage

Do we have agents deployed across all endpoints in the environment?

- Network coverage

Are all network subnets/locations within the scope of control?

- OS/Device type coverage

Does this control function with the different operating systems and devices in the environment?

- Environmental coverage

Is this control deployed across all physical and logical areas of the environment?

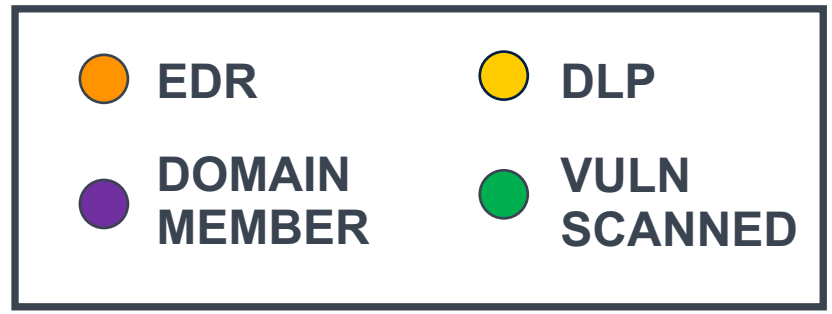
GuidePoint SECURITY

What are some examples of control Coverage?

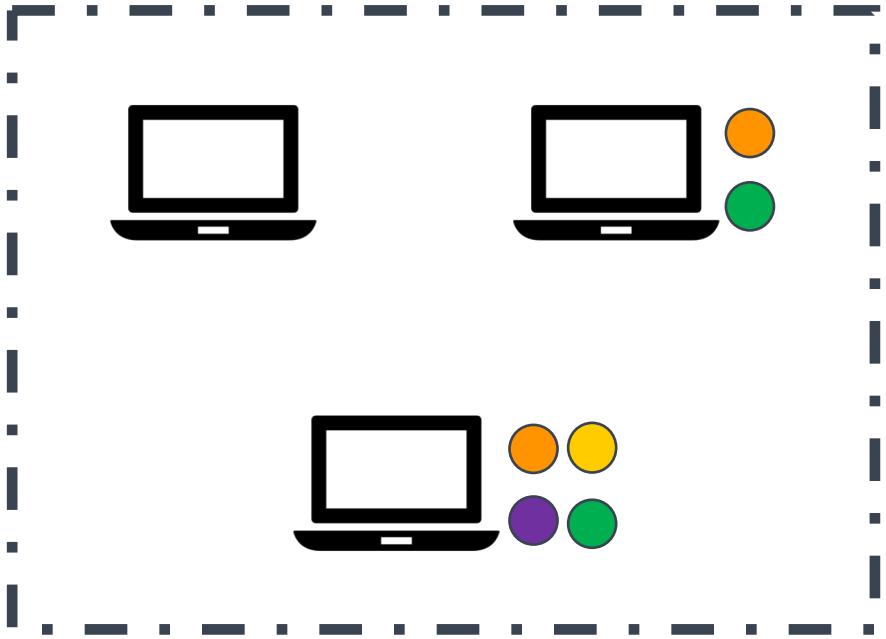
- Not all the network is in scope of a scanning or network security tool.
- The organization has adopted a cloud resource or new workflow that is not under the scope of a tool.
- Agents are not consistently distributed across the environment.
- There is not full feature parity with a given device type/OS.

GuidePoint SECURITY

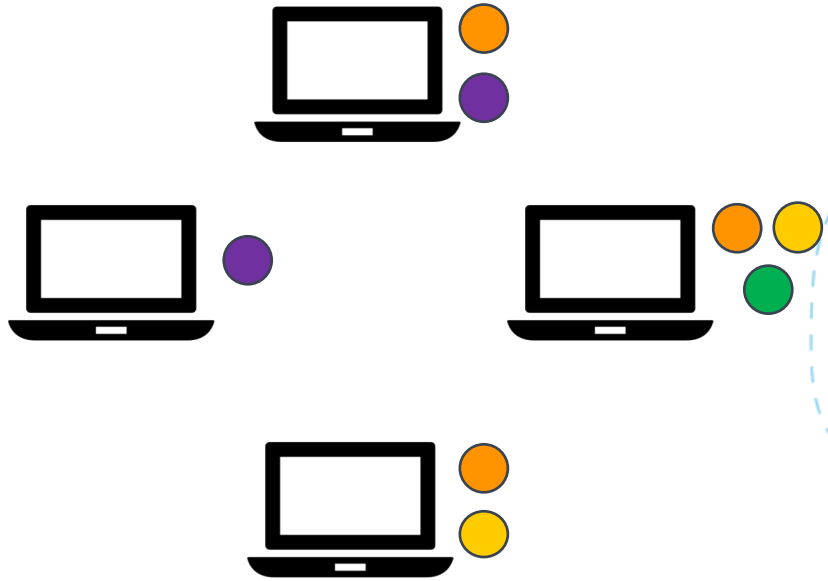
Endpoint Agent Coverage



ON PREMESIS



OFF PREMESIS



GuidePoint SECURITY

Optimization

The maturity and business relevance of a control's implementation.

- Control alignment

Does the implementation of the control align with adopted business policies, standards, frameworks, etc.?

- Control platform hygiene

Is the implementation of the control in keeping with best practices? For instance, is it fully patched? Are there unused features, functions, modules, etc.?

GuidePoint SECURITY

What are some examples of control Optimization?

- Authentication rates on vulnerability scanning are low.
- The settings of a tool do not consider an adopted framework.
- The system hasn’t been patched or had a health check in some time.
- There is no sense of asset classification in the tool.
- An integration is possible with other tools/systems but isn’t configured.

GuidePoint SECURITY

Validation

The functional integrity of a control's state.

- Control testing

Does the control have the intended response when prompted with a simulated attack? This could include tool-based testing or a Red Team exercise.

- Control functional drift

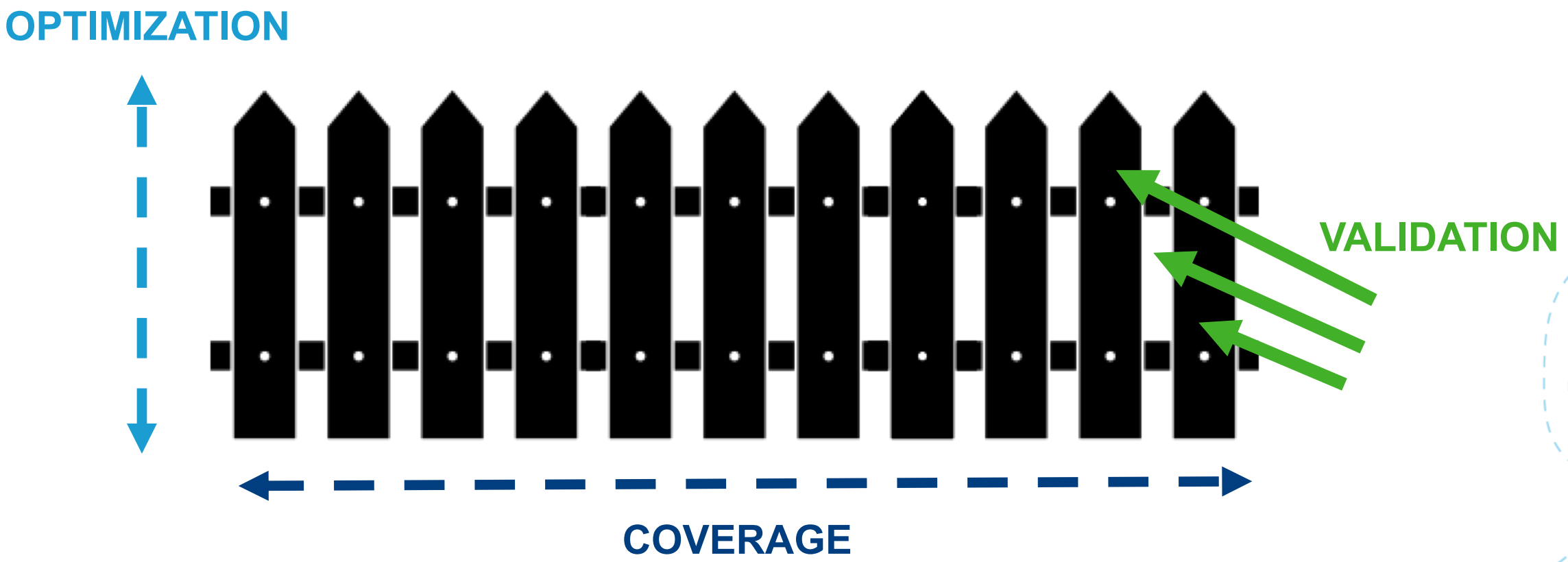
If a control is functioning today, how are we to know if it fails to react as expected in the future?

GuidePoint SECURITY

What are some examples of control Validation?

- Penetration test/Red Team exercise was very “successful”.
- Fuzzing an application has significant results.
- An automated runbook detects environmental drift.
- A bounty program was very expensive.

An effort in improving the coverage, optimization, and validation of controls is a way to boost environmental security without a major investment in product.



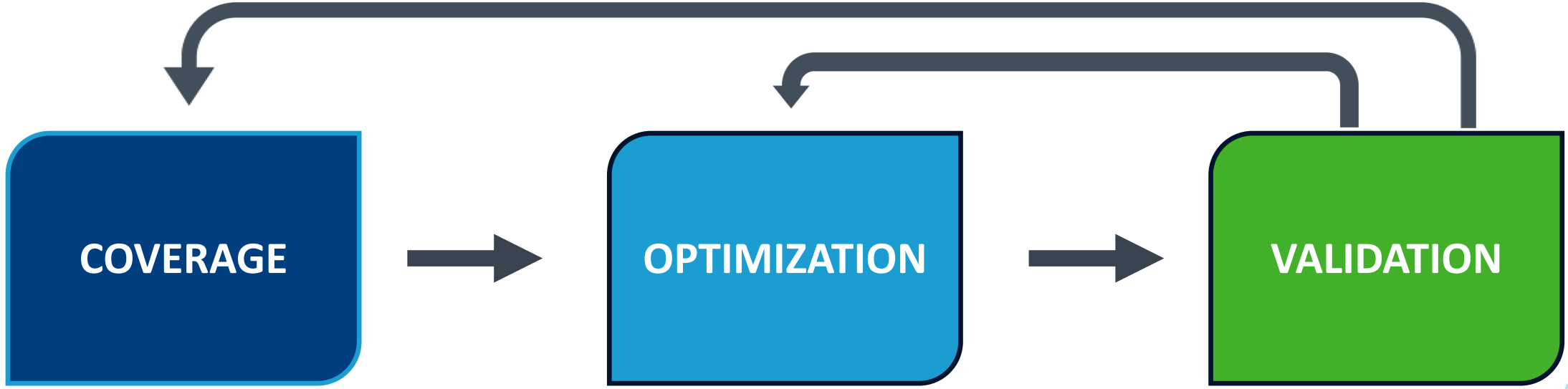
GuidePoint SECURITY

When is Control Assurance especially important?

- New CISO's, CIO's, Directors, etc. seeking to understand the scope of the control set beyond just a gap analysis.
- Organizations that have invested heavily on controls over the last few years.
- Mergers and acquisitions.
- Organizations adopting a new framework/standard or being subject to new regulation.
- Recovering from an event/breach/Red Team exercise.

GuidePoint SECURITY

Control Assurance Lifecycle



If sized correctly:

- Little or no new product
- No new infrastructure
- Out-of-band
- Light lift

If scoped correctly:

- Little or no new product
- Some changes needed
- In-band
- Moderate lift

- Some new product
- Some new infrastructure
- No changes needed
- Out-of-band
- Moderate lift

GuidePoint SECURITY

Thank You!

Chris Peltz, GuidePoint Security

chris.peltz@guidepointsecurity.com

315-664-0246