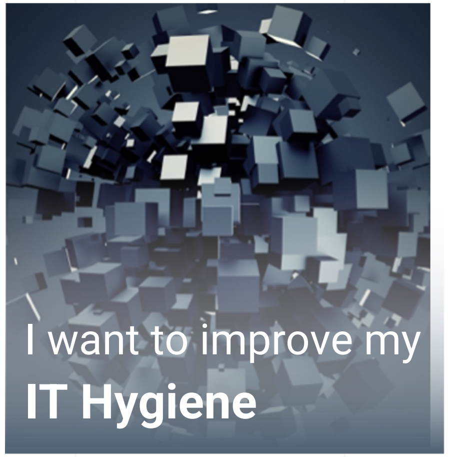
EXPANSE

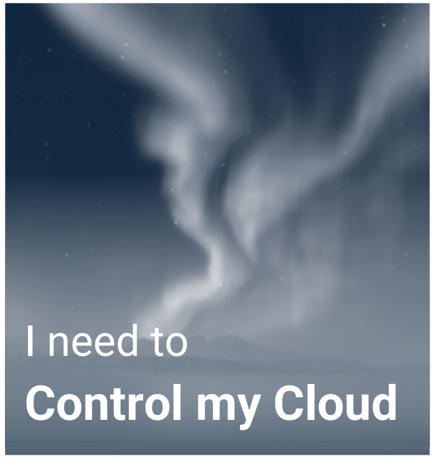
IOM Solutions

Sales Kick-Off

I want to reduce my company's **Attack Surface**



I want to improve my **IT Hygiene**



I need to **Control my Cloud**

I rely on my

Expanse System of Record

as the source of truth

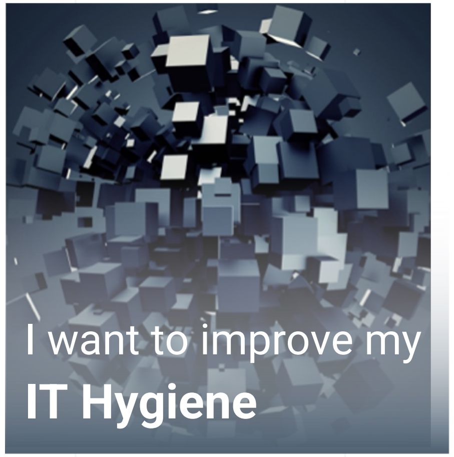
I deploy the

Internet Operations Management Platform

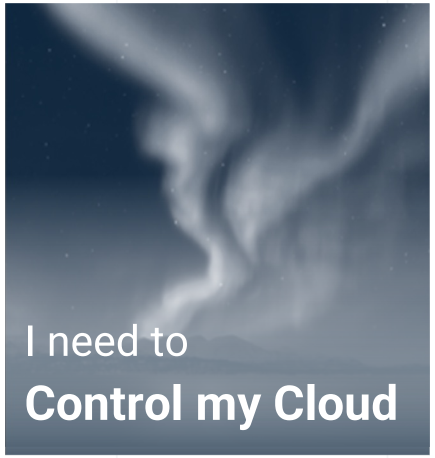
to govern my Internet

Attack Surface Reduction

I want to reduce my company's **Attack Surface**



I want to improve my **IT Hygiene**



I need to **Control my Cloud**

I reply on my

Expanse System of Record

as the source of truth

I deploy the

Internet Operations Management Platform

to govern my Internet

What Makes Up Your Attack Surface

Acquisitions

All the companies bought...

On-Prem Assets

IP Ranges, Certs, Domains...

My Attack Surface

Strategic Suppliers

All the irreplaceable and essential...

Cloud Environments

AWS, Azure, GCS...

Attack Surface Reduction

Expanse provides organizations a **continuously updated view** of their attack surface via **public Internet asset discovery, attribution** of those assets to organizations, and **monitoring** of those assets for security risks.

Reducing the Attack Surface
Why Organizations Care

1. **Reduce** risk of getting hacked

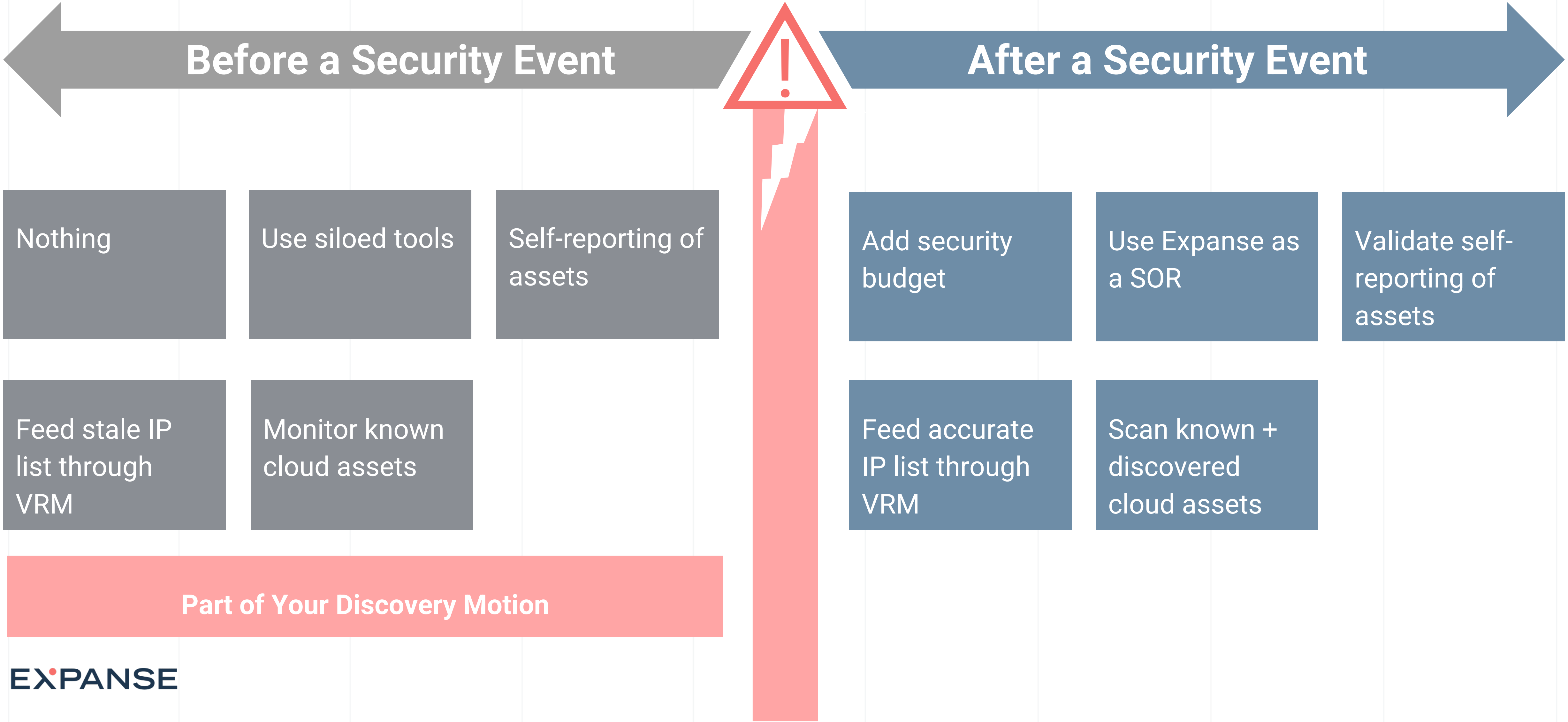
2. Know **where** they are at risk and their attack surface

3. Have a central source of **truth**, aka SOR

4. Do more with fewer **people** and fewer tools

5. **Prioritize** activities based on risk

What Organizations Do for ASR



Before a Security Event

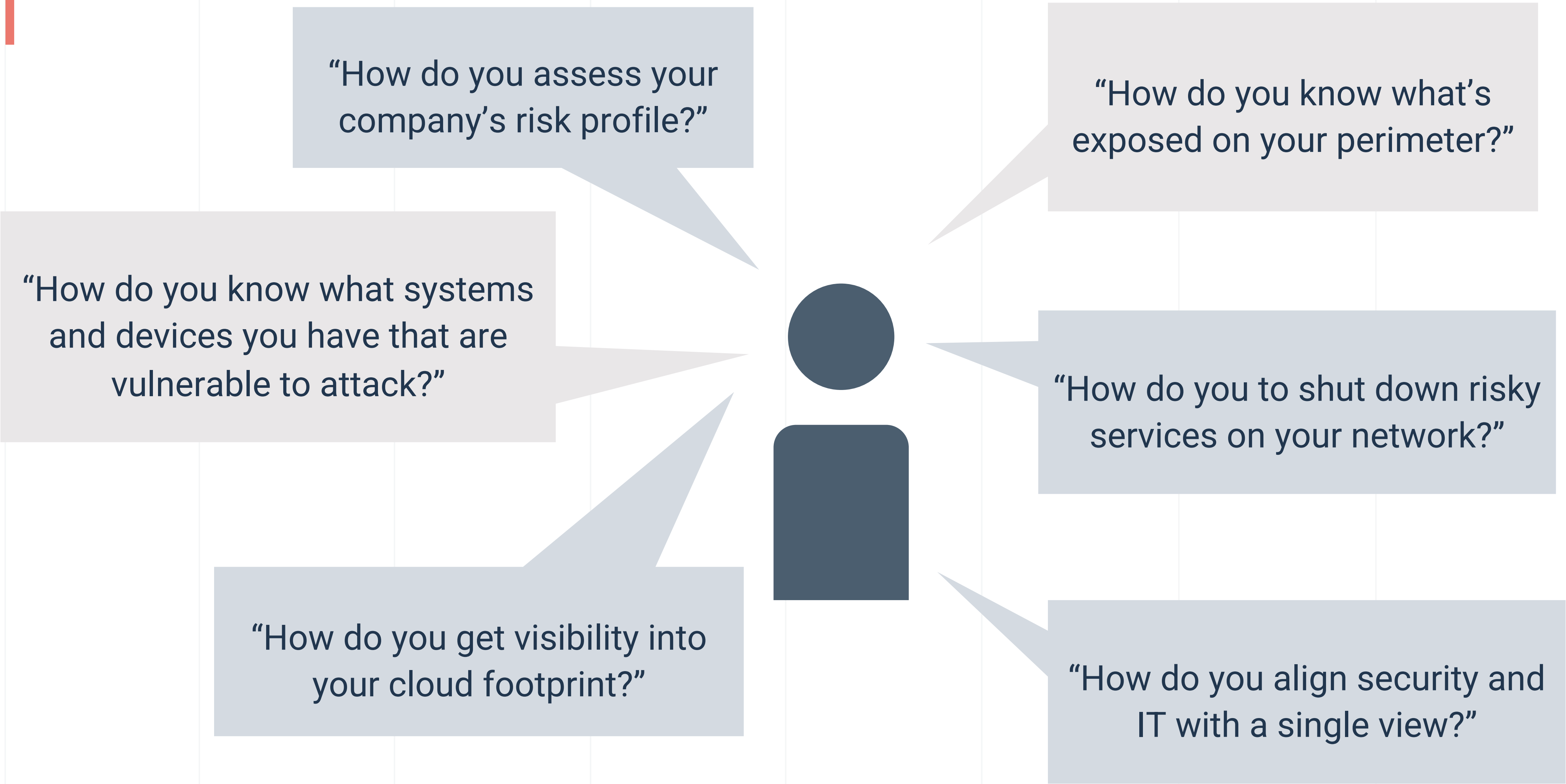
- Nothing
- Use siloed tools
- Self-reporting of assets
- Feed stale IP list through VRM
- Monitor known cloud assets

Part of Your Discovery Motion

After a Security Event

- Add security budget
- Use Expanse as a SOR
- Validate self-reporting of assets
- Feed accurate IP list through VRM
- Scan known + discovered cloud assets

ASR Discovery Questions



“How do you assess your company’s risk profile?”

“How do you know what’s exposed on your perimeter?”

“How do you know what systems and devices you have that are vulnerable to attack?”

“How do you to shut down risky services on your network?”

“How do you get visibility into your cloud footprint?”

“How do you align security and IT with a single view?”

Why We Will Win

Expanse Differentiators
Superior Asset Discovery & Attribution

Accenture

22 acquisition mappings completed

Expanse was used as a scanning source of truth in Vulnerability Management

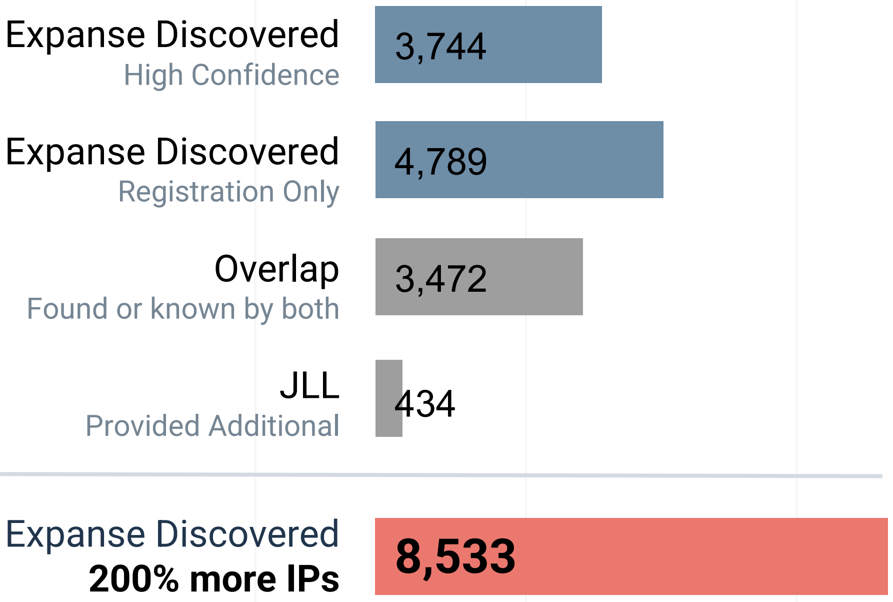
storm DIGITAL
INSITUM Part of Accenture Interactive
SILVEO
Apis
drosa
shackleton
PARKER FITZGERALD part of Accenture
Analytics8
Pragsis Bidoop
CLARITY INSIGHTS
?WHAT IF! part of accenture
HJALTELIN STAHL
ZIELPULS
Nytec
happen Part of Accenture
ep
CIRRUSEO Part of Accenture
sutter mills
maihiro
BRIDGE ENERGY GROUP
Northstream Part of Accenture
BCT Solutions

In all cases, we were told we **found more than provided**.

JLL

Over **200% more IPs** discovered

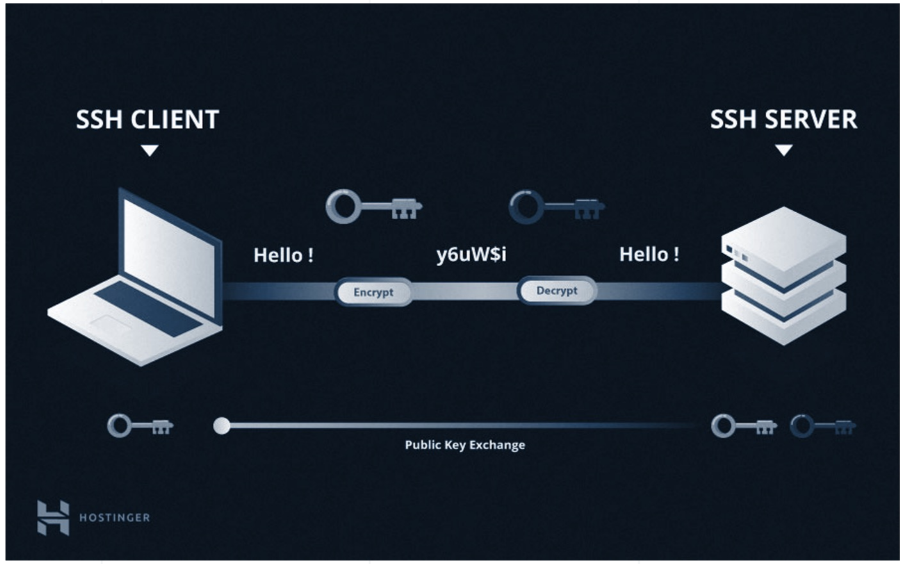
Provided visibility into the devices on their managed buildings which they never had before.



Expanse Differentiators
More Accurate Exposure Data

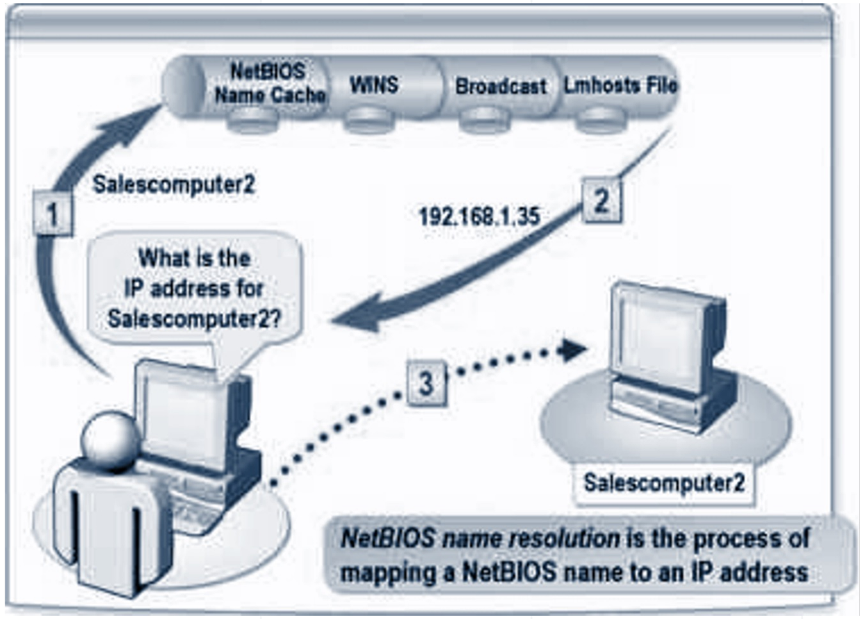
BDO

BDO's pentest identified an SSH server but after investigating in Expander, we found that the pentest was observing an open port and not a true SSH server.



JLL

JLL has attempted to take NetBIOS Name Servers offline for months, closing out the investigation as remediated despite Expanse still observing the exposures.


NetBIOS Name Cache
WINS
Broadcast
Lmhosts File
Salescomputer2
1
192.168.1.35
2
What is the IP address for Salescomputer2?
3
Salescomputer2
NetBIOS name resolution is the process of mapping a NetBIOS name to an IP address

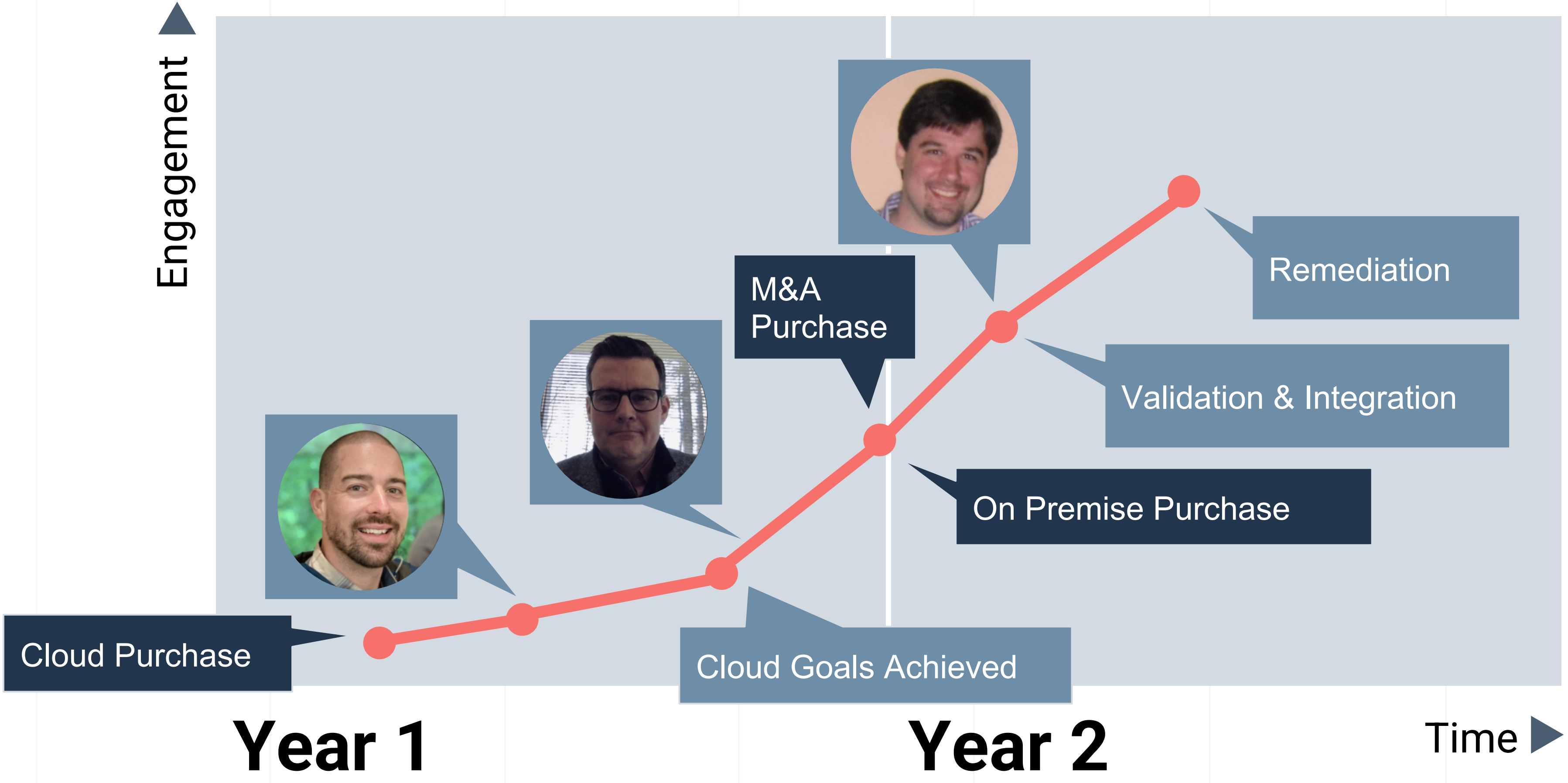
Expanse Differentiators
A Better Workflow Story

"We were told that **RiskIQ doesn't integrate well** into any of their systems so they had to manually move the data around or just don't bother so it remains a bit silo'd."

"When we were doing POV scoping, another member of the team spoke up that they use RiskIQ, and the manual management sucks. They continually have to re-mark ranges as stale month over month, and they keep having them re-surfaced. **If we can improve workflow management of ranges** (not sure if this is in the product, or fully via integrations), we can solve a lot of pain for them."

How to Sell (And Up-Sell)

CISCO



Delivering ASR Through the IOM Platform

What a Successful...
Attack Surface Reduction Program Looks Like With Expanse

1 **Inventory** public assets accurately

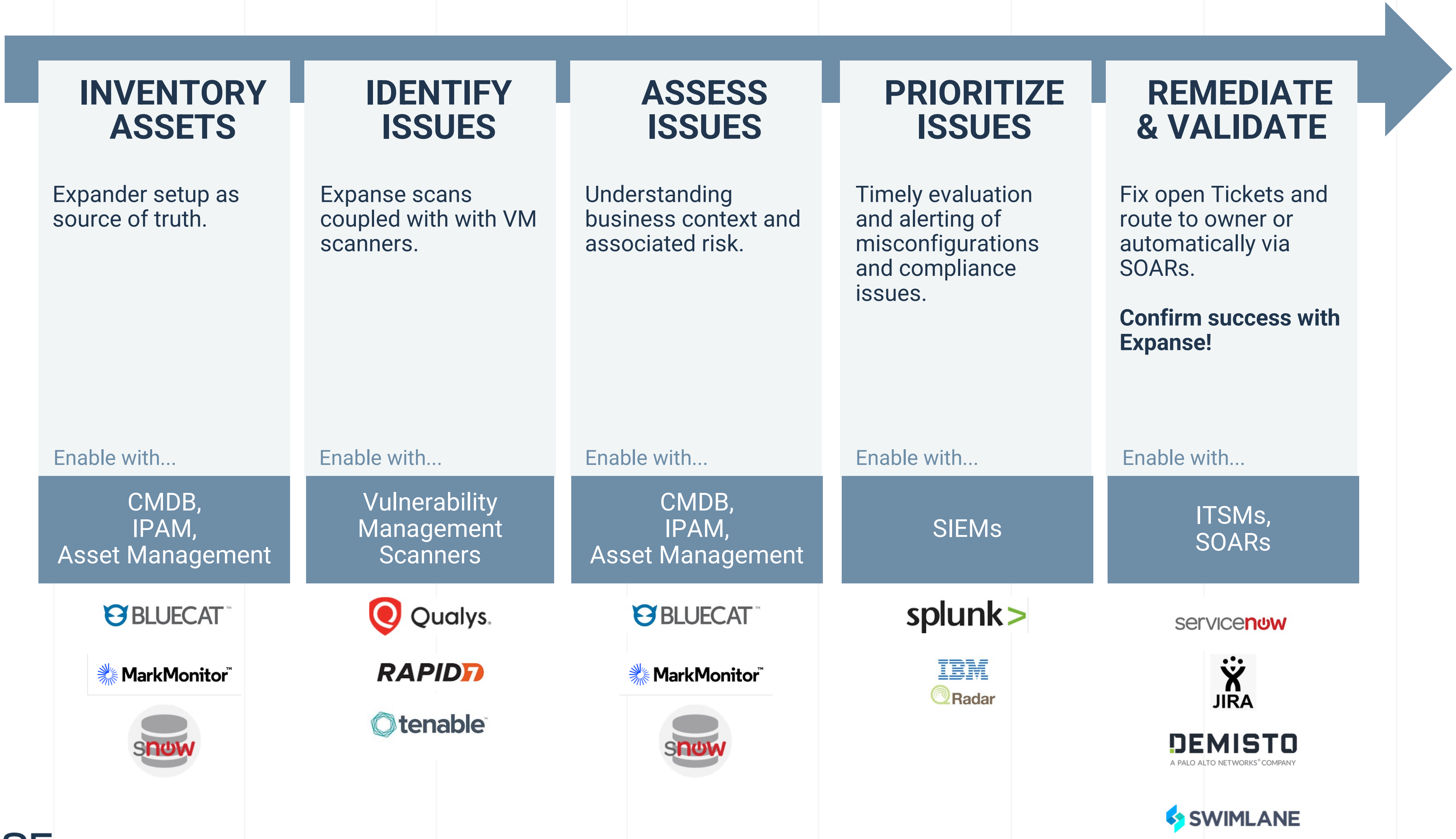
2 **Identify** security issues successfully

3 **Assess** security impact of issues

4 **Prioritize** issues using best practices

5 **Remediate** issues using a repeatable processes

ASR Operationalization Process



INVENTORY ASSETS

Expander setup as source of truth.

Enable with...

CMDB,
IPAM,
Asset Management

BLUECAT
MarkMonitor
snow

IDENTIFY ISSUES

Expanse scans coupled with with VM scanners.

Enable with...

Vulnerability
Management
Scanners

Qualys.
RAPID7
tenable

ASSESS ISSUES

Understanding business context and associated risk.

Enable with...

CMDB,
IPAM,
Asset Management

BLUECAT
MarkMonitor
snow

PRIORITIZE ISSUES

Timely evaluation and alerting of misconfigurations and compliance issues.

Enable with...

SIEMs

splunk>
IBM
QRadar

REMEDIATE & VALIDATE

Fix open Tickets and route to owner or automatically via SOARs.

Confirm success with Expanse!

Enable with...

ITSMs,
SOARs

servicenow
JIRA
DEMISTO
A PALO ALTO NETWORKS COMPANY
SWIMLANE

Stories From the Field

What Has Expanse Enabled Customers to Do for ASR?

- **Experian's Remediation Efficiency**
  - After a number of Telnet servers appeared in Expander, Experian was able to remediate them in 30 min compared to previously when it *"would've taken weeks to months or just not happened at all"*
- **BDO's Triage of New Exposures**
  - Maintaining 0 critical exposures, reliant on Expander recommendations for policies, turning email alerts into SNOW tickets
- **BP's Operationalization Strategy**
  - Using the first 90 days to lay the groundwork for the Asset Management and Vulnerability Management use cases - beginning asset validation and documenting future processes, tackling low hanging "exposure fruit" to showcase quick wins to upper leadership, and prioritizing highest impact integrations (SNOW [ITSM])

Demo
Attack Surface Reduction With Expanse

Competitive Landscape

TIER 1	ANKLE- BITERS	EMERGING	COMPLEMENTARY
RISKIQ™	CYCOGNITO	Censys	SecurityScorecard BITSIGHT

What to Sell and to Whom

PRODUCTS

- Expander
- Behavior
- Link

TARGET BUYERS

- CISO/VP of InfoSec
- Dir. of InfoSec
- Dir. of VM

TARGET INFLUENCERS

- Security Architect
- Director of Audit

How to Sell Tomorrow

PROSPECTING	DISCOVERY	DEMO	POV	CLOSE
ASR SalesLoft Cadence Expander datasheet Behavior datasheet Link datasheet Leverage existing Gong calls	Pitch Deck ASR WP 5 Common Perimeter Exposures WP Behavior WP Supply chain WP ASR discovery questions (in SalesHood early Feb.) Second meeting deck (ETA Q1)	Learn and do ASR demo video (in SalesHood early Feb.)	Bring in Jeremy or Haley as needed	Leverage pricing guidelines in SalesHood Bring in executives as needed

How Marketing Will Help

- **Jan 27: ASR demand-gen launch**
  - Campaign launch will drive over 1k leads to target accounts
- **Q1: VRM WP**
  - Expanse for Vulnerability Management white paper
- **Ongoing:**
  - Competitive training and enablement
  - ABM marketing efforts (when applicable)

In Summary...

- Most companies don’t have a good ASR program in place and don’t even know how to begin implementing one
- ASR is impossible without accurate discovery and visibility into exposures — this is what Expanse provides better than anyone else
- Learn the discovery questions, collateral, and demo to sell Expander, Behavior, and Link to security personas