# Mission Ready Attack Surface Management

**Tyler Jaeger**
**Sr. ATS Sales Engineer – Public Sector**

**Max Reitnauer**
**Principal Sales Account Director**

**Tyler Jaeger**

Sr. ATS Sales Engineer Public Sector

**Max Reitnauer**

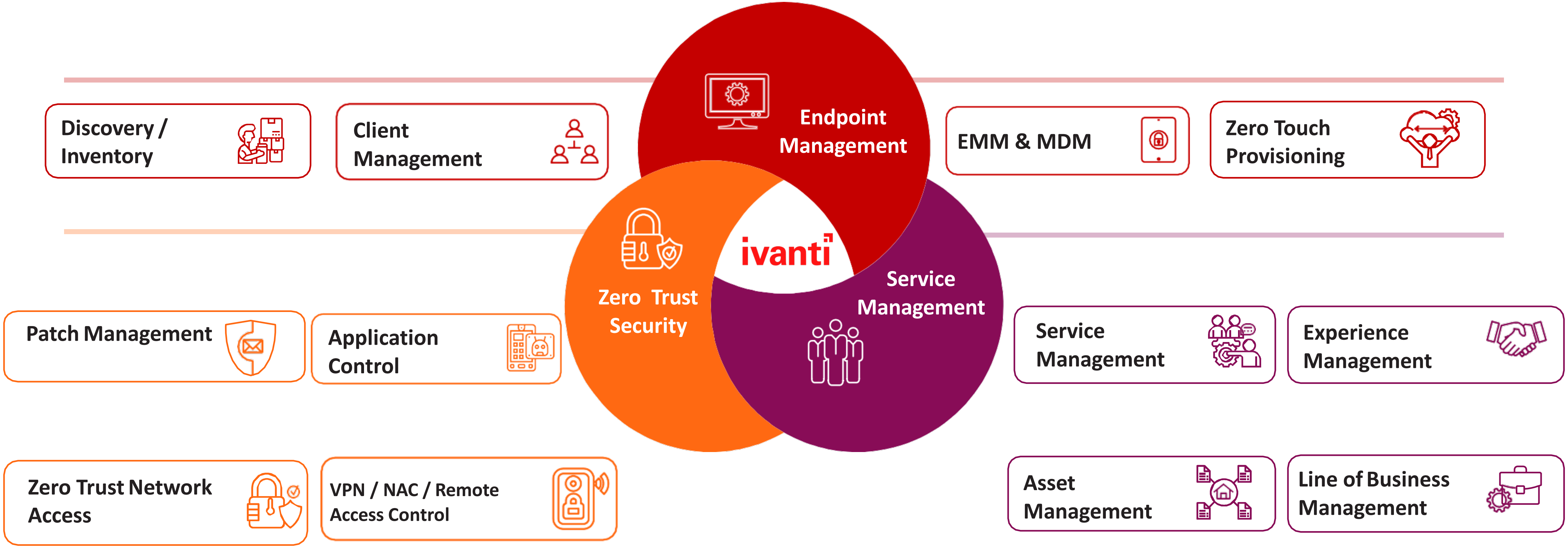
Principal Sales Account Director

# Agenda

- **About Ivanti**
- **What is Attack Surface Management?**
- **Attack Surface Management:**
  - Discovery
  - Privilege & Application Management
  - Risk-Based Vulnerability Management
  - Vulnerability Remediation
- **Question / Recap**

# Unmatched End-to-End Platform

Ivanti's Platform Enables IT Organizations to Discover, Manage, Secure, Service, and Automate Critical Workflows Across all Device Types



ivanti

Endpoint Management

Discovery / Inventory

Client Management

EMM & MDM

Zero Touch Provisioning

Zero Trust Security

Patch Management

Application Control

Zero Trust Network Access

VPN / NAC / Remote Access Control

Service Management

Service Management

Experience Management

Asset Management

Line of Business Management

# Zero Trust | Capability Model

ZERO TRUST

## CORE PILLARS

CORE CAPABILITIES

### Data

- Data Loss Prevention
- Data Classification
- Metadata Mgmt.
- Data Encryption
- Data Segmentation
- Dynamic Data Masking (DDM)
- Fully-automated Data Tagging via ML/AI
- Data Rights Management (DRM)

### Device & Endpoint

- Device Authorization
- HW & SW Inventory
- Cloud-based Baseline Enforcement
- Compliance Enforcement
- Device Authentication
- Cloud-based Software Deployment & Mgmt.
- Intelligence for Endpoint Response
- Asset Management

### Network & Environment

- API Integration
- Fully Encrypted Traffic
- Common Service Access
- Network Segmentation
- Cloud Access Security Broker (CASB)
- Software Defined Networking (SDN)
- Software Defined Perimeter *(Access to Apps and Data)*
- Application Proxy
- Management and Monitoring

### Application & Workload

- DevSecOps
- Application Delivery
- Micro Segmentation
- Application Segmentation
- Software Chain Supply
- Software Defined Compute
- Application Approved/ Prohibited List
- Application Visibility & Access *(Anytime, Anywhere)*

### User

- User Authentication
- User Authorization
- Cybersecurity Access Policy
- Privilege Access Mgmt.
- Single Identity Platform
- MFA
- In-session Monitoring
- ABAC
- Device based PKI – PIV-D/Derived
- Transparent Authentication

### Visibility & Analytics

- Discovery & Baselining
- Machine Learning
- Advanced Threat Protection
- Monitoring and Auditing
- Risk Evaluation & Dynamic Risk Scoring
- Security and Information Event Management (SIEM)

### Automation & Orchestration

- API Standards
- Incident Response
- Artificial Intelligence
- Security Orchestration, Automation & Response (SOAR)

Threat Score, Risk Score, Target Valuation, Triage Priority, and Compliance Score (snapshots & trend)

FCEB Framework (when available); Periodic review updates within 360 days; system wide data/system/software/user/log provenance (origin)

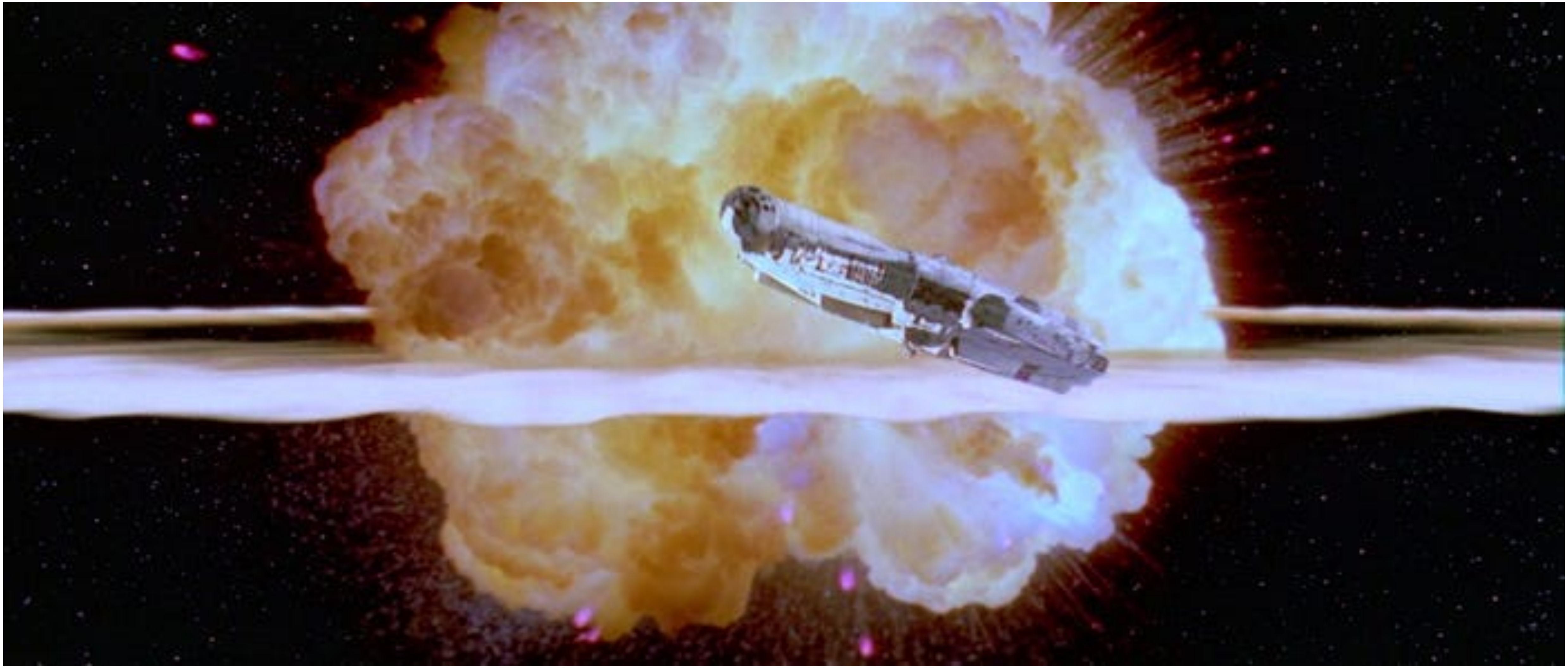
**GOVERNANCE**

# What is Attack Surface Management?

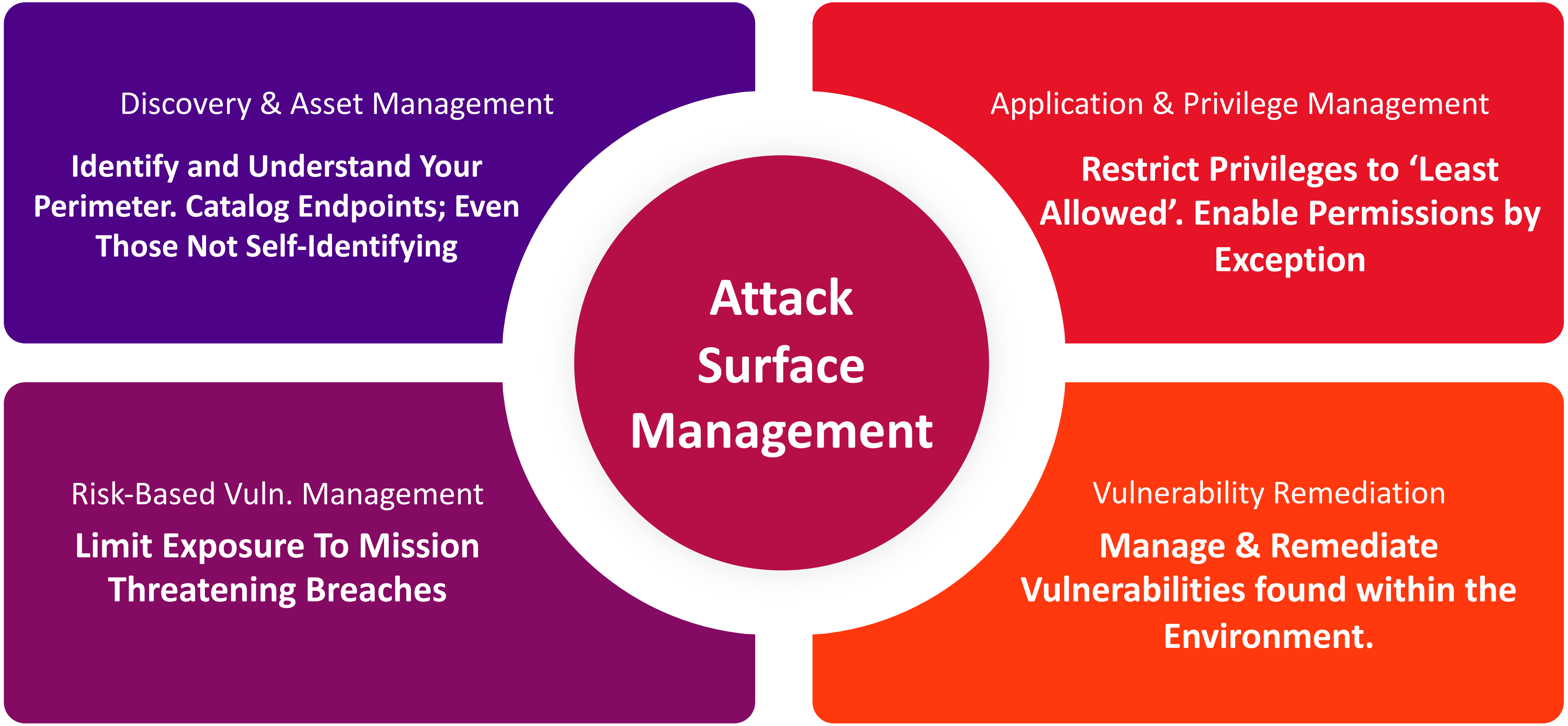
Mapping Solutions to Attack Surface Management

## Attack surface management is the continuous process of discovering, classifying and assessing the security of an organization's assets in it’s entirety.

# Attack Surface Management - Visualized



# Overview: Mapping Attack Surface Management



Discovery & Asset Management

**Identify and Understand Your Perimeter. Catalog Endpoints; Even Those Not Self-Identifying**

Application & Privilege Management

**Restrict Privileges to 'Least Allowed'. Enable Permissions by Exception**

**Attack Surface Management**

Risk-Based Vuln. Management

**Limit Exposure To Mission Threatening Breaches**

Vulnerability Remediation

**Manage & Remediate Vulnerabilities found within the Environment.**

# Canvassing Your Environment

Discovery
Asset Management
Application Whitelisting
Privilege Management
Risk Based Vulnerability Management
Vulnerability Remediation

Discover

# Discover your Environment

### Ivanti Discovery

Simplifies security with unified and automated prevention, detection, and response techniques that target your biggest attack vectors.

## Strengths

Ideal Discovery tools determine inventory, whether physical servers, VMs, and templates, regardless of power state or if they are on or offline.

Identify Windows, Mac, and Linux endpoints within the environment. Detect and remediate OS and third-party app vulnerabilities on systems running Windows, Red Hat Linux, Alma Linux, and CentOS.

Agentless scanning for rapid startup and zero footprint.

**Discover & Manage off-network devices.**

Integrate & automate with other products.

## Use Case

- Leverage discovery tools to canvas or map endpoints within your environment, whether they are self-declared or not.
- Discovers both workstations and servers to patch, mix of online and offline workstations and servers.
- Agentless technology supports assessment and deployment to workstations and servers connected to your network while minimizing the impact on both your team and system workloads.
- Common Industries: DoD, Department of Energy, Civilian Agencies, & Federal Service Integrators.

# Catalog Discovered & Managed Assets

Asset

## Strengths

Catalog the endpoints in your environment and establish a lifecycle for those devices. Alert admins of any issues from within a Centralized Console / Report.

Establish your Assets into your organizations CMDB. Begin to build a record that ties vulnerabilities & potential breaches to specific assets. Build your organizations technology into a centralized CMDB.

Export Asset information to reporting tools such as Splunk, etc.

Manage the entire Device Lifecycle from Procurement to Retiring

Sources include: Discovery Tools, & Contract Information.

## Use Case

- Deploy ITAM infrastructure to both Cloud-Based and On-Prem based environments to establish ITIL-based Asset Lifecycle Management.
- Allow ITAM to act as the Point of Record for any Assets within the environment and leverage that to
- Establish ITAM as a backbone for other Attack Surface Management Tools (Discovery, Privilege / Application Management, Risk-Based Vulnerability Management, & Vulnerability Remediation)
- Common Industries: DoD, Department of Energy, Civilian Agencies, & Federal Service Integrators

## Asset Management

Manage IT assets throughout their entire lifecycle—from purchase through disposal.

# How to Protect Your Endpoints (and Data)

Discovery
Asset Management
Privilege Management
Application Management & Whitelisting
Risk Based Vulnerability Management
Vulnerability Remediation

# Privilege Management Degradation

**Challenge:** *“I don’t want any local administrators in my environment however, there are some applications that require higher than standard rights and I don’t want to impact user productivity”*

**Description:** *Local administrative rights have been removed from all users. However, if an application is identified that requires additional rights, the user is given full administrative rights in their workspace again.*

## The Privilege Degradation Lifecycle

The user is working happily with standard user rights. >

After some time, the user attempts to use an application (or function in an application). >

The user receives a message implying that privileges are incorrect. >

The Support team are contacted to inform of the issue. >

Local administrative rights are given to resolve the issue. >

Security Posture has been worsened - Potentially permanently

# Controlling Privilege Degradation

**How leveraging Application Control tools like Ivanti & other 3$^{rd}$ Parties assist against Privilege Degradation**

### Granular Privilege Management

Enables you to implement **'least privilege' access** and eliminate local admin accounts while still giving users the privileges that they need to do their job.

### Maintain Productivity

Delivers security without impacting productivity with minimal performance impact to end users.

### Minimal Administrative Overhead

Manage application access and privilege management across your desktop and server estate in an automated fashion.

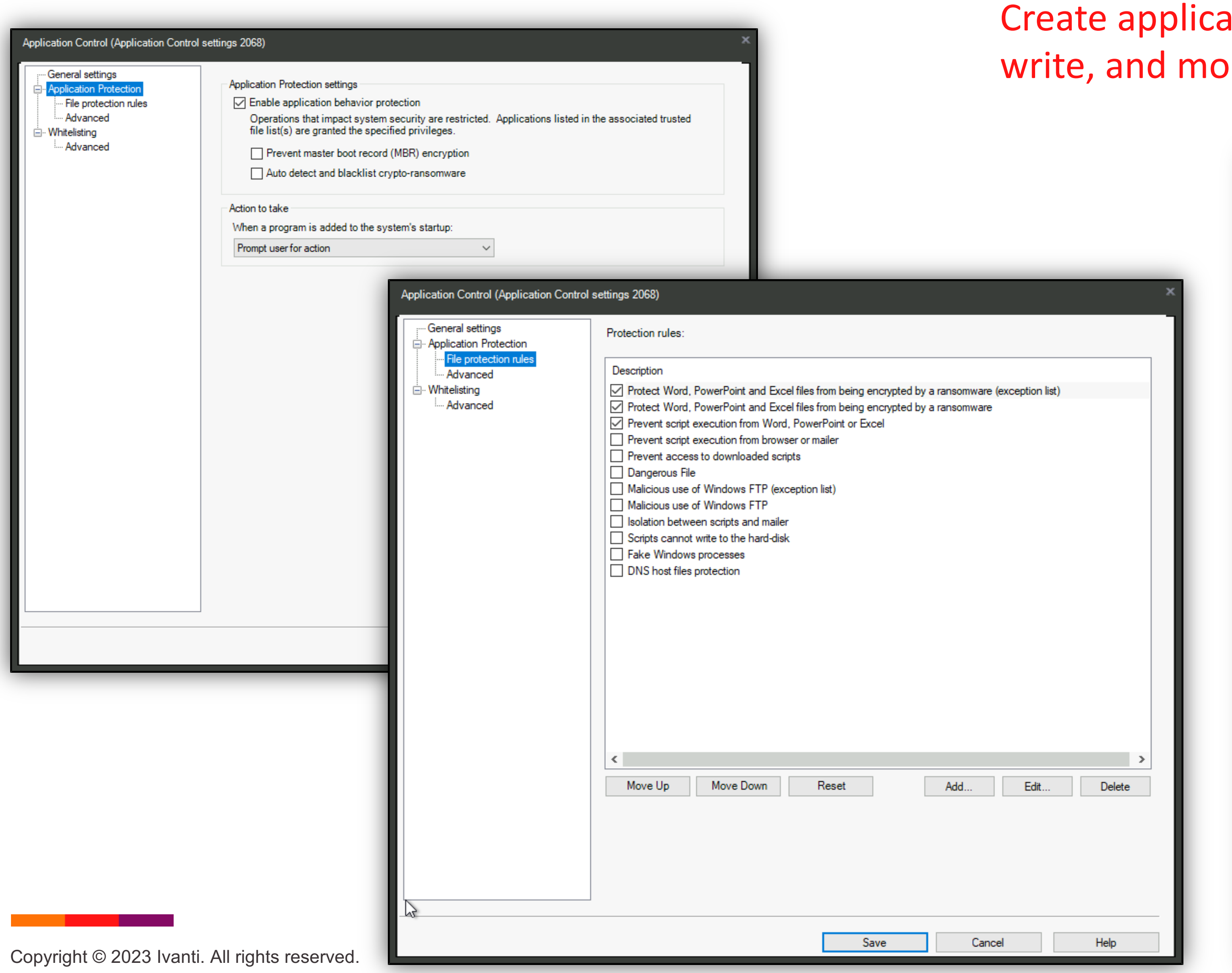
### Resource Redirection

Automatically redirect users when they attempt to access a specified URL. Setup a 'Whitelist' or a set of Categories of approved sites.

**Use Case:** According to Microsoft, over **80%** of critical Windows 10 vulnerabilities reported in 2019 required a level of privileged access. Allow Application Control tools to reduce your risk while maintaining optimum productivity.

# Application Distribution & Control

Create application policies to limit app's ability to read, write, and modify files in the appropriate locations.



Application Control (Application Control settings 2068)

Application Protection settings

☑ Enable application behavior protection

Operations that impact system security are restricted. Applications listed in the associated trusted file list(s) are granted the specified privileges.

□ Prevent master boot record (MBR) encryption

□ Auto detect and blacklist crypto-ransomware

Action to take

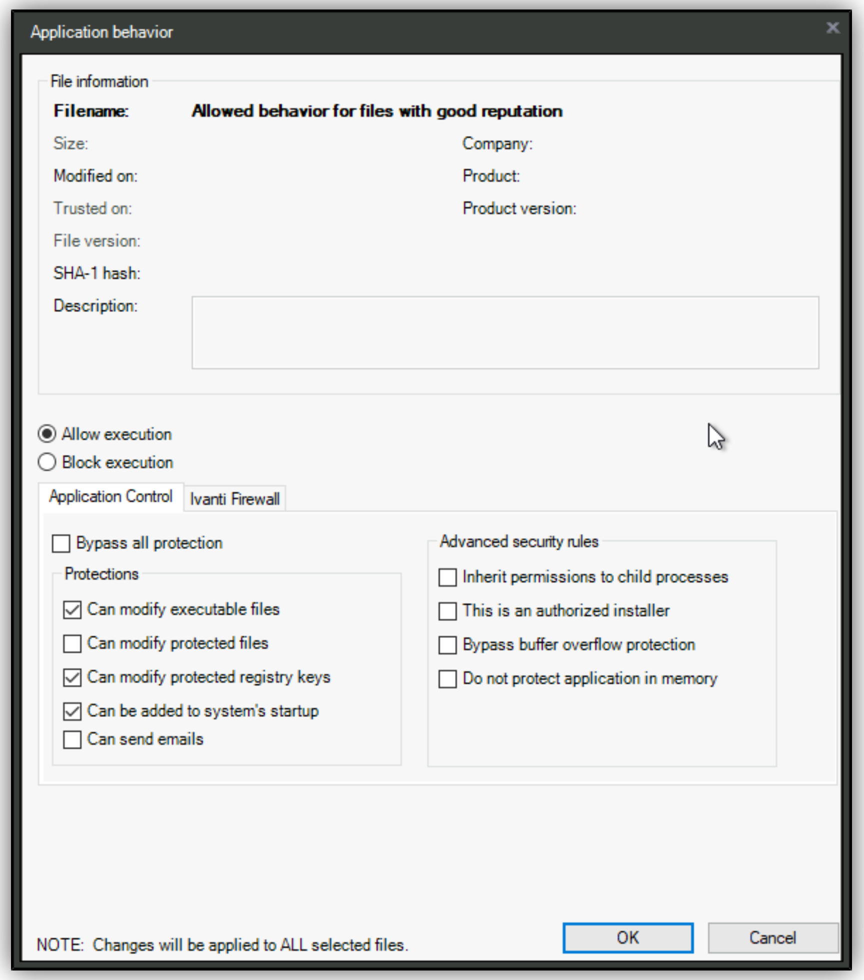
When a program is added to the system's startup: Prompt user for action

Application Control (Application Control settings 2068)

Protection rules:

Description

☑ Protect Word, PowerPoint and Excel files from being encrypted by a ransomware (exception list)
☑ Protect Word, PowerPoint and Excel files from being encrypted by a ransomware
☑ Prevent script execution from Word, PowerPoint or Excel
□ Prevent script execution from browser or mailer
□ Prevent access to downloaded scripts
□ Dangerous File
□ Malicious use of Windows FTP (exception list)
□ Malicious use of Windows FTP
□ Isolation between scripts and mailer
□ Scripts cannot write to the hard-disk
□ Fake Windows processes
□ DNS host files protection



Application behavior

File information

**Filename:** **Allowed behavior for files with good reputation**

Size:
Company:
Modified on:
Product:
Trusted on:
Product version:
File version:
SHA-1 hash:
Description:

● Allow execution
○ Block execution

□ Bypass all protection

Protections

☑ Can modify executable files
□ Can modify protected files
☑ Can modify protected registry keys
☑ Can be added to system's startup
□ Can send emails

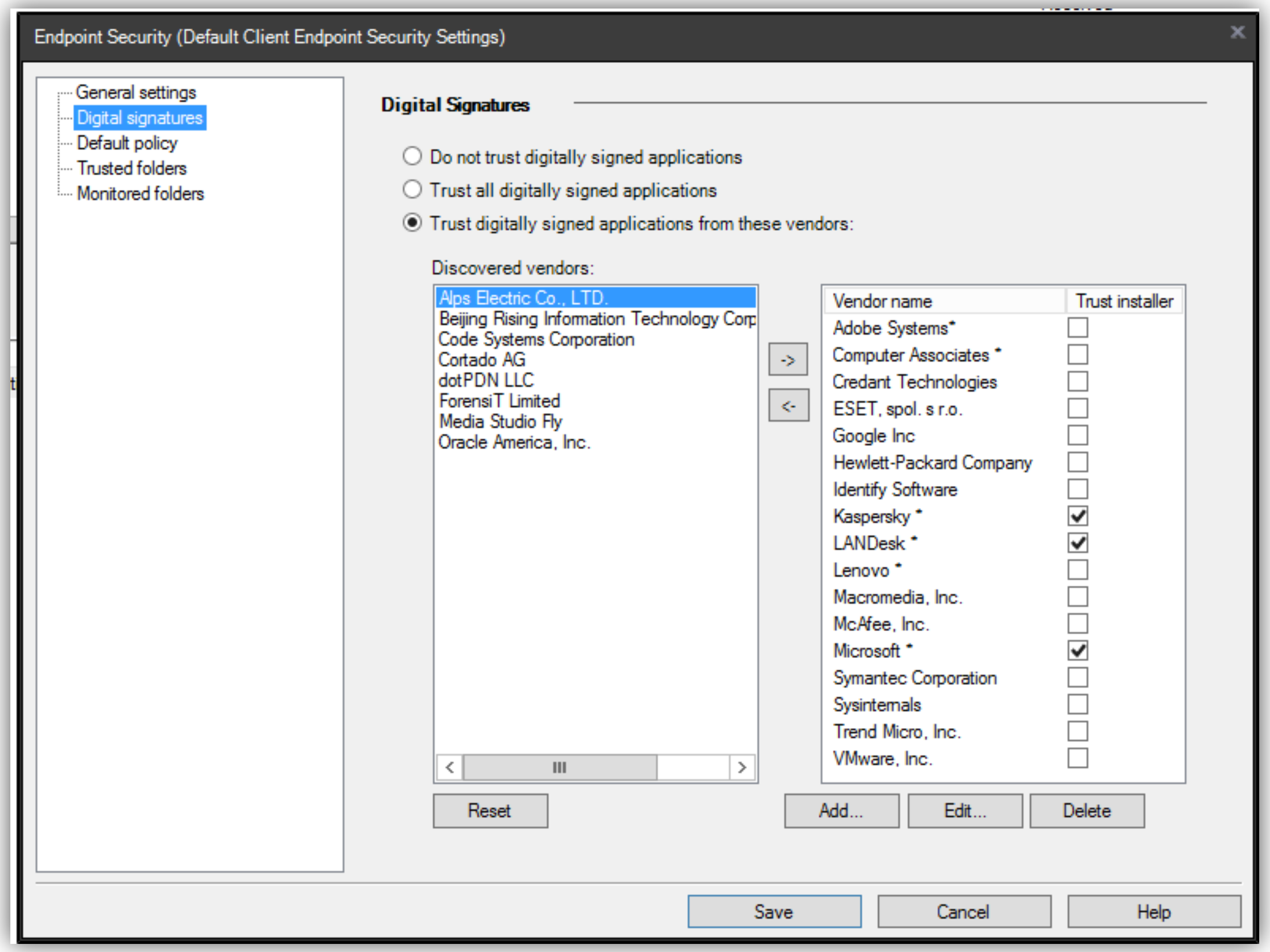
Advanced security rules

□ Inherit permissions to child processes
□ This is an authorized installer
□ Bypass buffer overflow protection
□ Do not protect application in memory

NOTE: Changes will be applied to ALL selected files.

# Trusted Ownership / Digital Signatures

**Set trust *only* for application that are digitally signed and specified by Administrators.**



Endpoint Security (Default Client Endpoint Security Settings)

- General settings
- Digital signatures
- Default policy
- Trusted folders
- Monitored folders

**Digital Signatures**

○ Do not trust digitally signed applications

○ Trust all digitally signed applications

● Trust digitally signed applications from these vendors:

Discovered vendors:

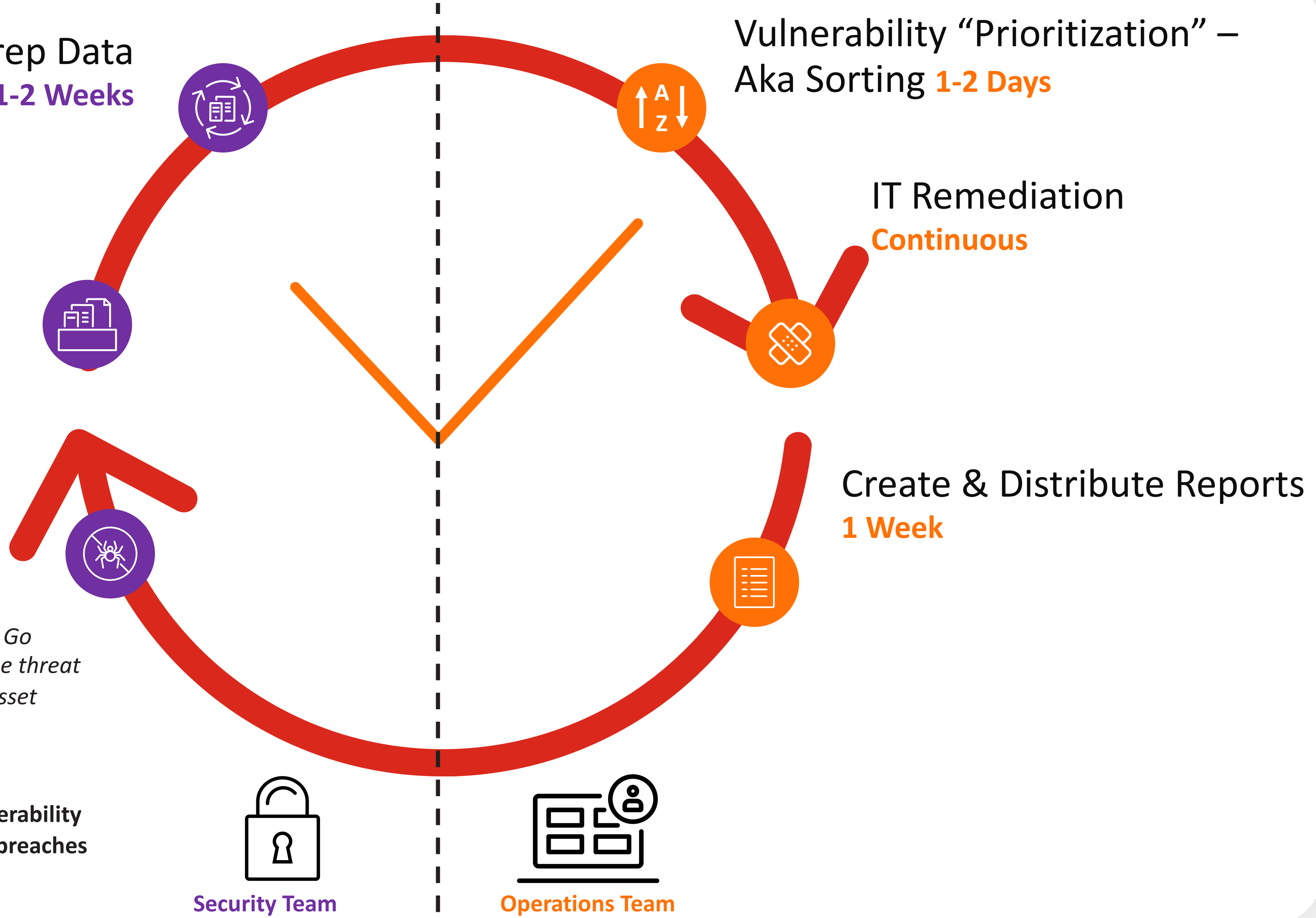
Alps Electric Co., LTD.
Beijing Rising Information Technology Corp
Code Systems Corporation
Cortado AG
dotPDN LLC
ForensiT Limited
Media Studio Fly
Oracle America, Inc.

| Vendor name | Trust installer |
|---|---|
| Adobe Systems* | ☐ |
| Computer Associates * | ☐ |
| Credant Technologies | ☐ |
| ESET, spol. s r.o. | ☐ |
| Google Inc | ☐ |
| Hewlett-Packard Company | ☐ |
| Identify Software | ☐ |
| Kaspersky * | ☑ |
| LANDesk * | ☑ |
| Lenovo * | ☐ |
| Macromedia, Inc. | ☐ |
| McAfee, Inc. | ☐ |
| Microsoft * | ☑ |
| Symantec Corporation | ☐ |
| Sysinternals | ☐ |
| Trend Micro, Inc. | ☐ |
| VMware, Inc. | ☐ |

# Using Intelligence to Decrease Exposure Risk

Discovery
Asset Management
Privilege Management
Application Management & Whitelisting
**Risk Based Vulnerability Management**
**Vulnerability Remediation**

# The Legacy Vulnerability Management Lifecycle



Normalize & Prep Data
1-2 Weeks

Data Gathering
2-4 Days

Vulnerability Scanning
2-5 Days

Vulnerability "Prioritization" –
Aka Sorting 1-2 Days

IT Remediation
Continuous

Create & Distribute Reports
1 Week

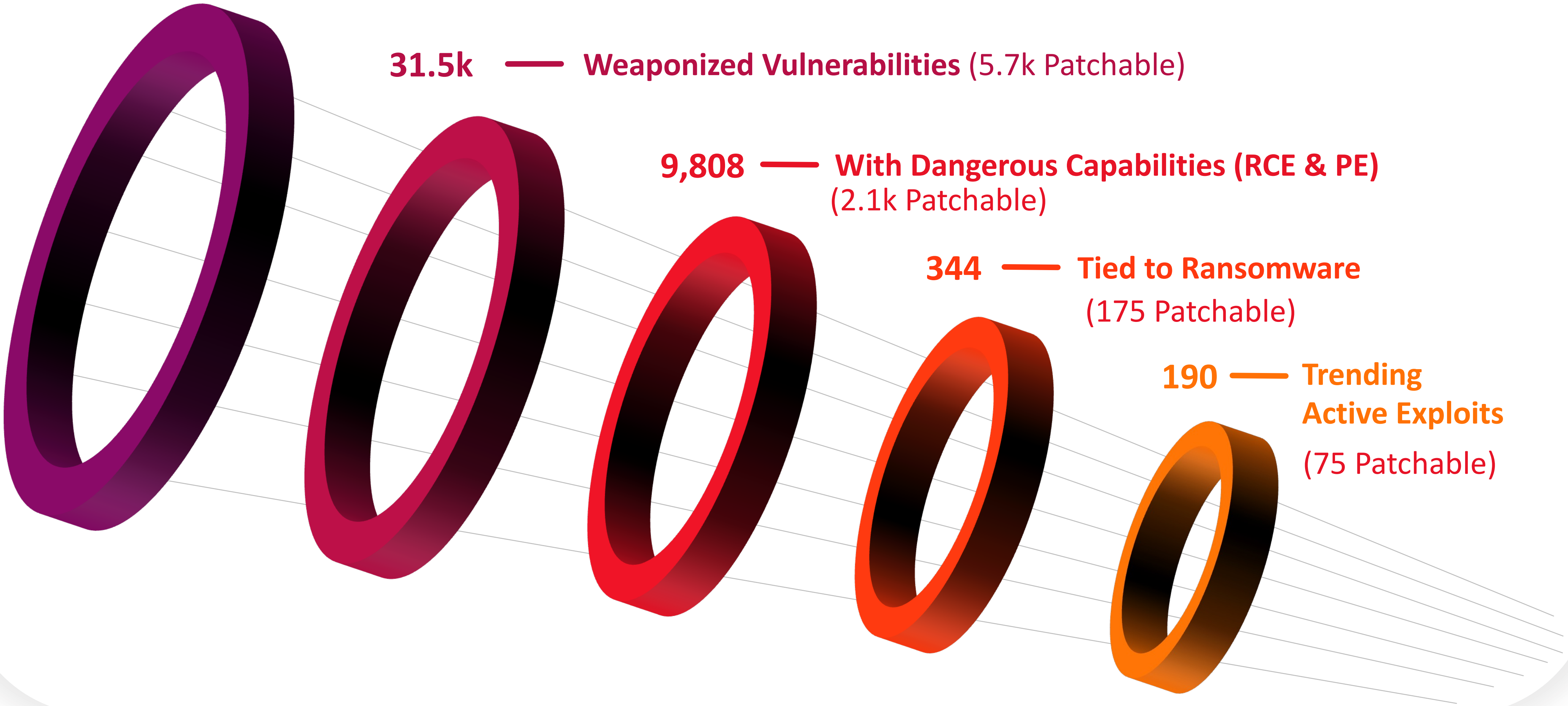
**Gartner on RBVM :**

*"Don't try to patch everything; focus on vulnerabilities that are actually exploitable. Go beyond a bulk assessment of threats and use threat intelligence, attacker activity and internal asset criticality to provide a better view of real organizational risk."*

**Organizations that use the risk-based vulnerability management method will suffer 80% less breaches**

# Leveraging Weaponization Funnels

Prioritize



250k — **Total Vulnerabilities** (60.4k Patchable)

31.5k — **Weaponized Vulnerabilities** (5.7k Patchable)

9,808 — **With Dangerous Capabilities (RCE & PE)** (2.1k Patchable)

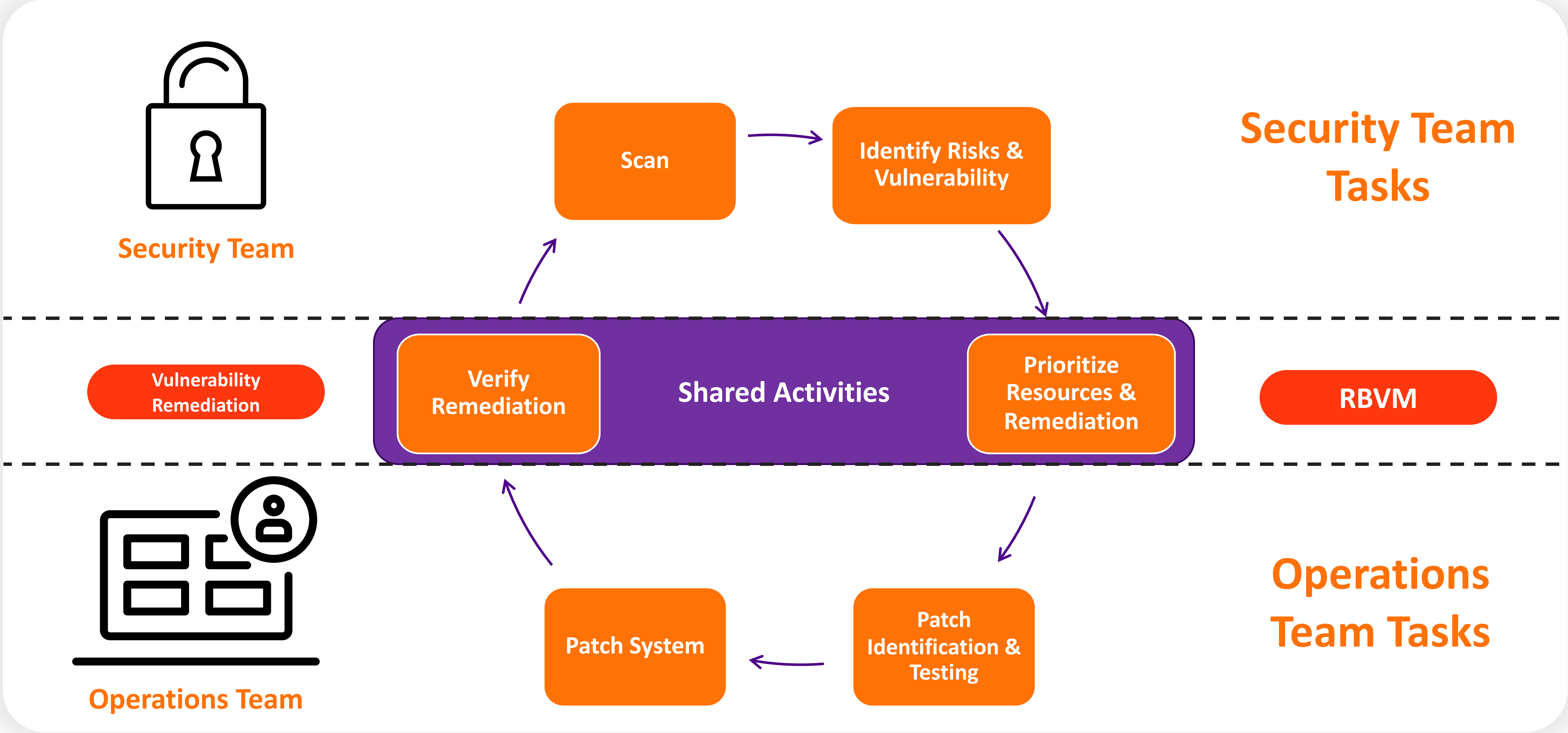
344 — **Tied to Ransomware** (175 Patchable)

190 — **Trending Active Exploits** (75 Patchable)

*Oct. 21, 2022

Source: Cyber Security Works, Cyware, Ivanti, Securin, "2023 Spotlight Report – Ransomware Through the Lens of Threat and Vulnerability Management"

# The Vulnerability Management Lifecycle - Optimized



Remediation

# Ivanti Vulnerability Remediation

## Ivanti EPM & Security Controls

Simplifies security with unified and automated prevention, detection, and response techniques that target your biggest attack vectors.

## Strengths

Patch your virtual servers – Discover, inventory, and patch physical servers, VMs, and templates, regardless of power state or if they are on or offline.

Patch your Windows and Linux machines – Detect and remediate OS and third-party app vulnerabilities on systems running Windows, Red Hat Linux, and CentOS.

Agentless scanning for rapid startup and zero footprint.

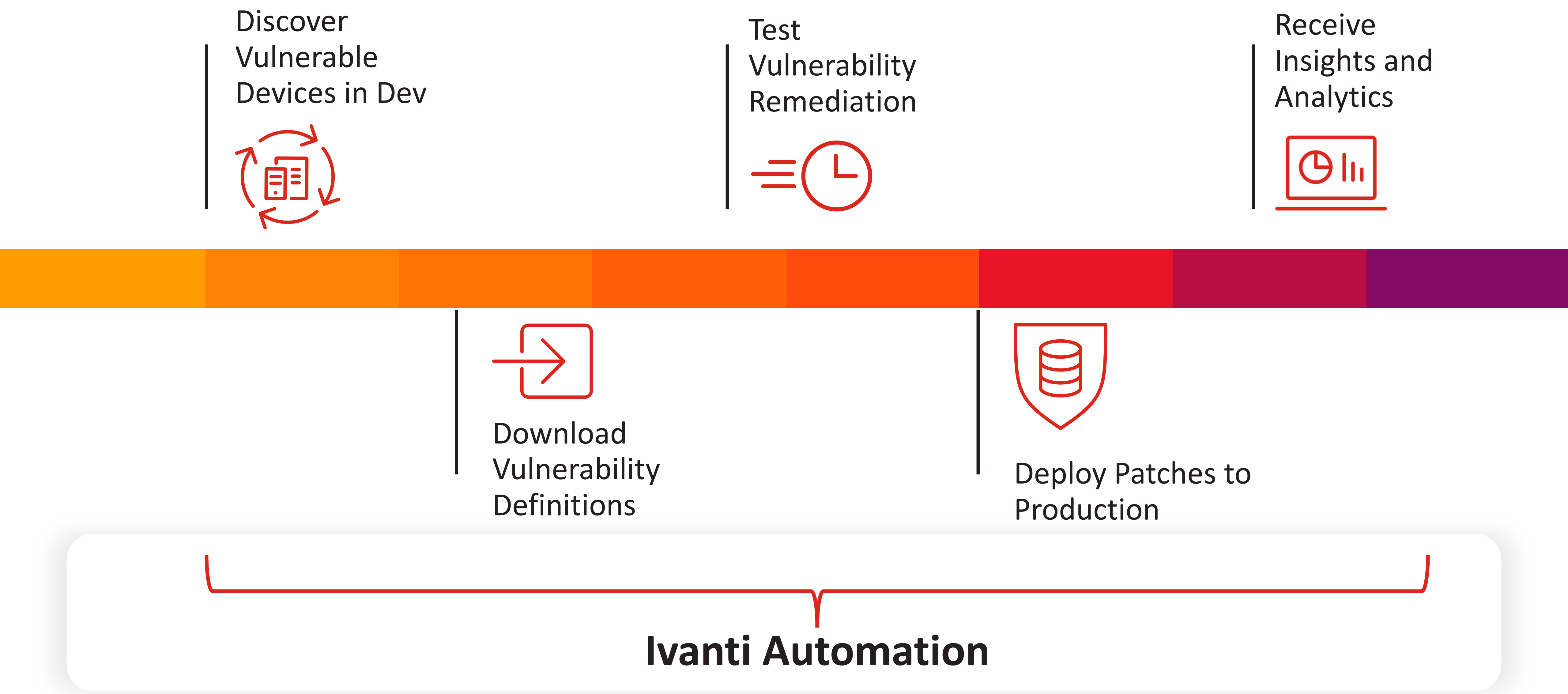
Manage off-network devices.

Integrate & automate with other products.

## Use Case

- Mix of workstations and servers to patch, mix of online and offline workstations and servers
- Agentless technology supports assessment and deployment to workstations and servers connected to your network while minimizing the impact on both your team and system workloads
- Agent policies provide a higher degree of accuracy in environments where devices are not continuously connected to the network
- Common Industries: DoD, Department of Energy, Civilian Agencies, & Federal Service Integrators

# Ivanti's Disconnected Vulnerability Remediation Process



Discover Vulnerable Devices in Dev

Download Vulnerability Definitions

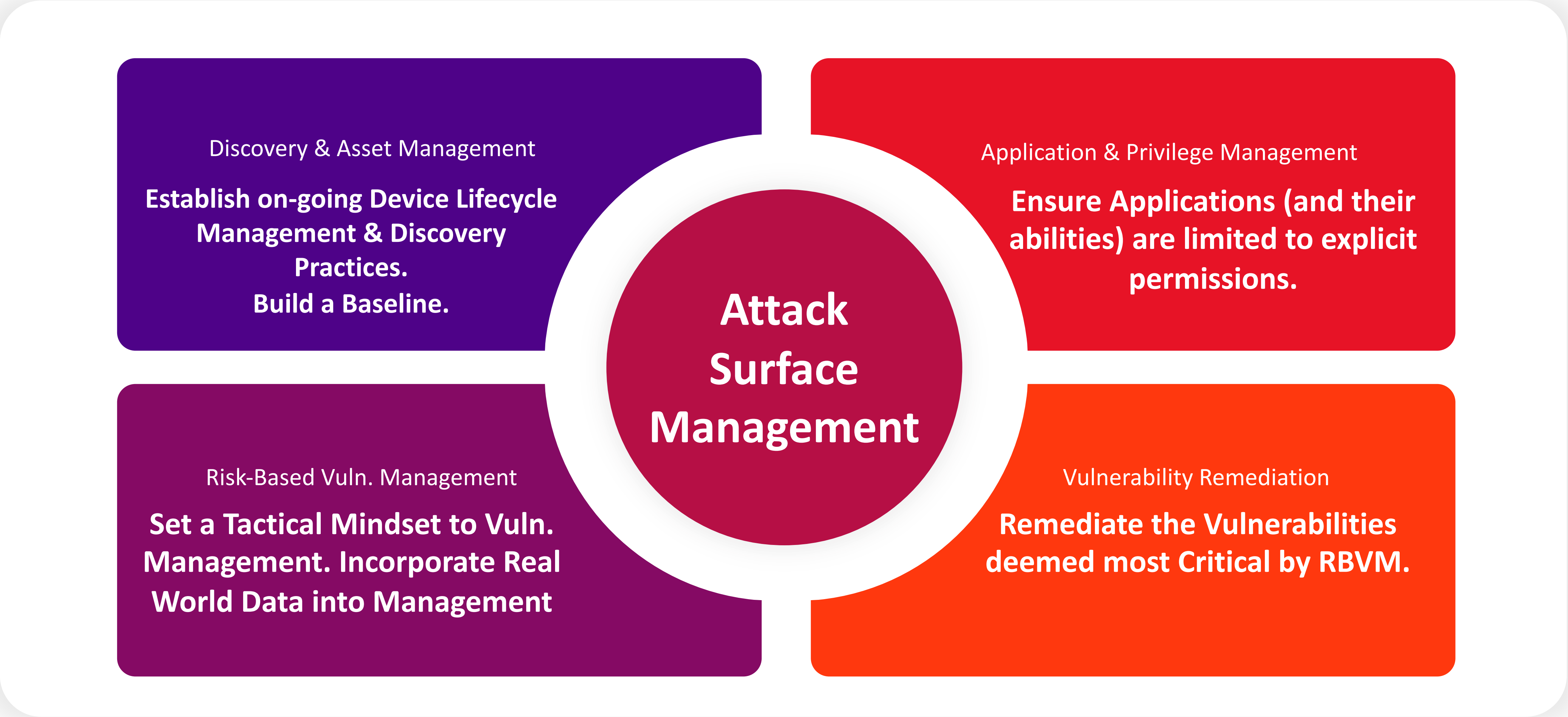
Test Vulnerability Remediation

Deploy Patches to Production

Receive Insights and Analytics

**Ivanti Automation**

# Recap: The Elements of Attack Surface Management



Discovery & Asset Management

Establish on-going Device Lifecycle Management & Discovery Practices.
Build a Baseline.

Application & Privilege Management

Ensure Applications (and their abilities) are limited to explicit permissions.

Attack Surface Management

Risk-Based Vuln. Management

Set a Tactical Mindset to Vuln. Management. Incorporate Real World Data into Management

Vulnerability Remediation

Remediate the Vulnerabilities deemed most Critical by RBVM.

# Questions?

ivanti

**Tyler Jaeger**
**Sr. Account Technical Strategist - Sales Engineer**
**C:(410) 417-8448**

**Max Reitnauer**
**Principal Sales Account Director**
**C:(240) 751-3295**