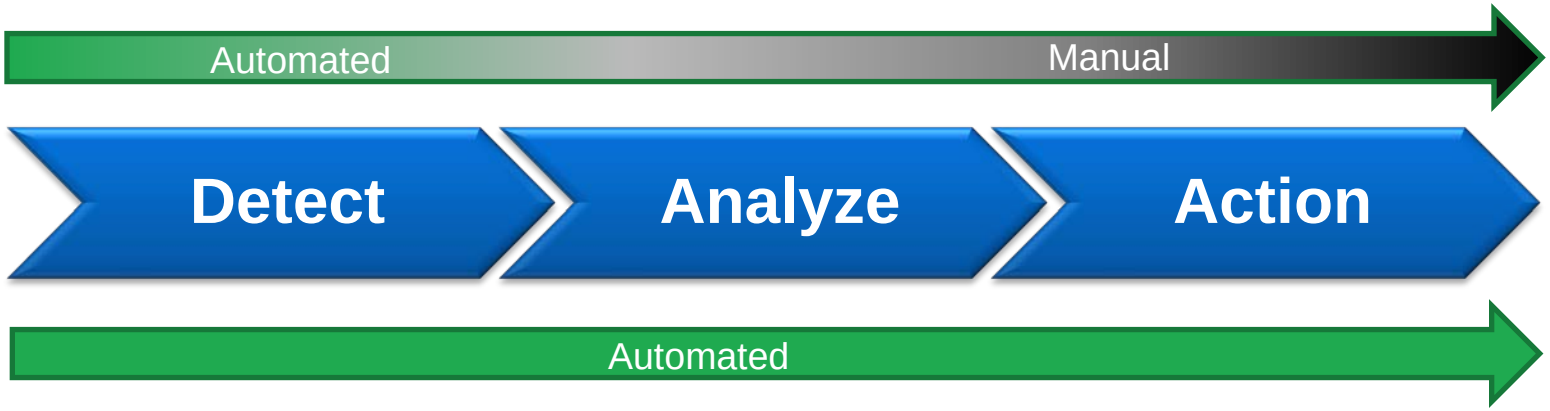
Security Automation Through Granular Change Detection

Jim Ivers, CMO and SVP, Product Management
Triumfant, Inc.

The Next Step in Security Automation

- Move from manual to automated processes
- Move from periodic to continuous activities
- Move from global to contextual requirements

Current solutions lack scan scope, contextual analysis, and fall well short of automating the process



Leveraging granular change detection enables full automation of the process, including the synthesis of a remediation in real-time

Triumfant

Problem Statement

Existing Security Solutions	Problems
Security posture is monitored periodically rather than continuously (periodic versus continuous)	Security posture will weaken every day it isn't checked and enforced. This includes status of other endpoint protection tools
Remediations are designed by highly skilled humans after the fact (manual versus automated)	Significant time lag between the emergence of a new attack and availability of an effective response
Remediations are not contextual (global versus contextual)	Insufficient knowledge to repair collateral damage
Detection of attacks relies on prior knowledge	Misses at least 50% of the unknown attacks and 2%-10% of known attacks

Triumfant

Introducing a New Approach

Existing Security Solutions	Automated Detection/Remediation
Security posture is monitored periodically rather than continuously (periodic versus continuous)	Security posture is monitored and enforced *continuously*. Every change goes through detect-analyze-action cycle.
Remediations are designed by highly skilled humans after the fact (manual versus automated)	Remediations are *synthesized automatically* on the fly. Full automation of the detect-analyze-action cycle.
Remediations are not contextual (global versus contextual)	Remediations are tailored to the situation and the environment, removing the malware and repairing collateral damage.
Detection of attacks relies on prior knowledge	Attacks detected and characterized based on *analytic methods*. Effective for targeted attacks and attacks that evade other tools

Triumfant

Context

Most tools view potential security events in the context of the affected machine only

Triumfant

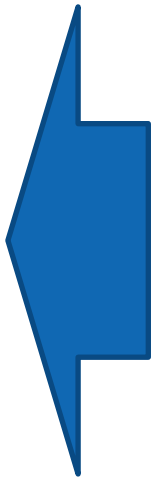
Context

Most tools view potential security events in the context of the affected machine only

Triumfant views potential events in the broader context of the endpoint population

Building Context Into the Equation

Adaptive Reference Model



Building Context Into the Equation

Adaptive Reference Model

We convert data into contextual knowledge

- A detailed model of what is normal in the endpoint population at a particular time
  - Creates a normative baseline and a normative whitelist
  - Automatically synthesized, refreshed weekly
  - Based on patented data mining algorithms
  - Broad context eliminates false positives
- Explicitly tuning the model
  - Policies - set specific rules within the model
  - Filters - excludes things from the model
  - Includes OVAL interpreter for SCAP content

Triumfant

The Data Behind The Context

Adaptive Reference Model

What is in the Model?

- Registry keys
- Files – MD5 hash of every file
- Processes
- Services
- Open ports
- Event Logs
- Performance counters
- Security settings
- Hardware attributes
- Memory tables

Triumfant

Continuous Scanning

Continuously scans every computer every day

- Scans for changes to the elemental attributes
  - 24 hour cycle by default
  - Includes scan of SCAP vulnerability data
- Scans for changes that are indicators of malicious activity
  - Approximately every 30 seconds
  - Triggers immediate analysis
- Scans when the machine is not connected to the network

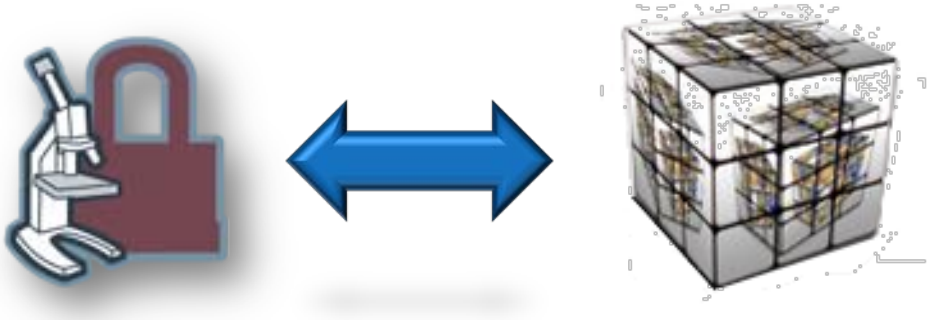
Triumfant

Analyzing Changes in Context

Changes are Analyzed in the Context of the Adaptive Reference Model

Is the change isolated to this machine?

Do other machines running the same software have the same set of associated files??



Is a new application running anywhere else in the population?

Does the change make the machine non-compliant with explicit configuration settings – i.e. a SCAP checklist?

Triumfant

Gathering Additional Context

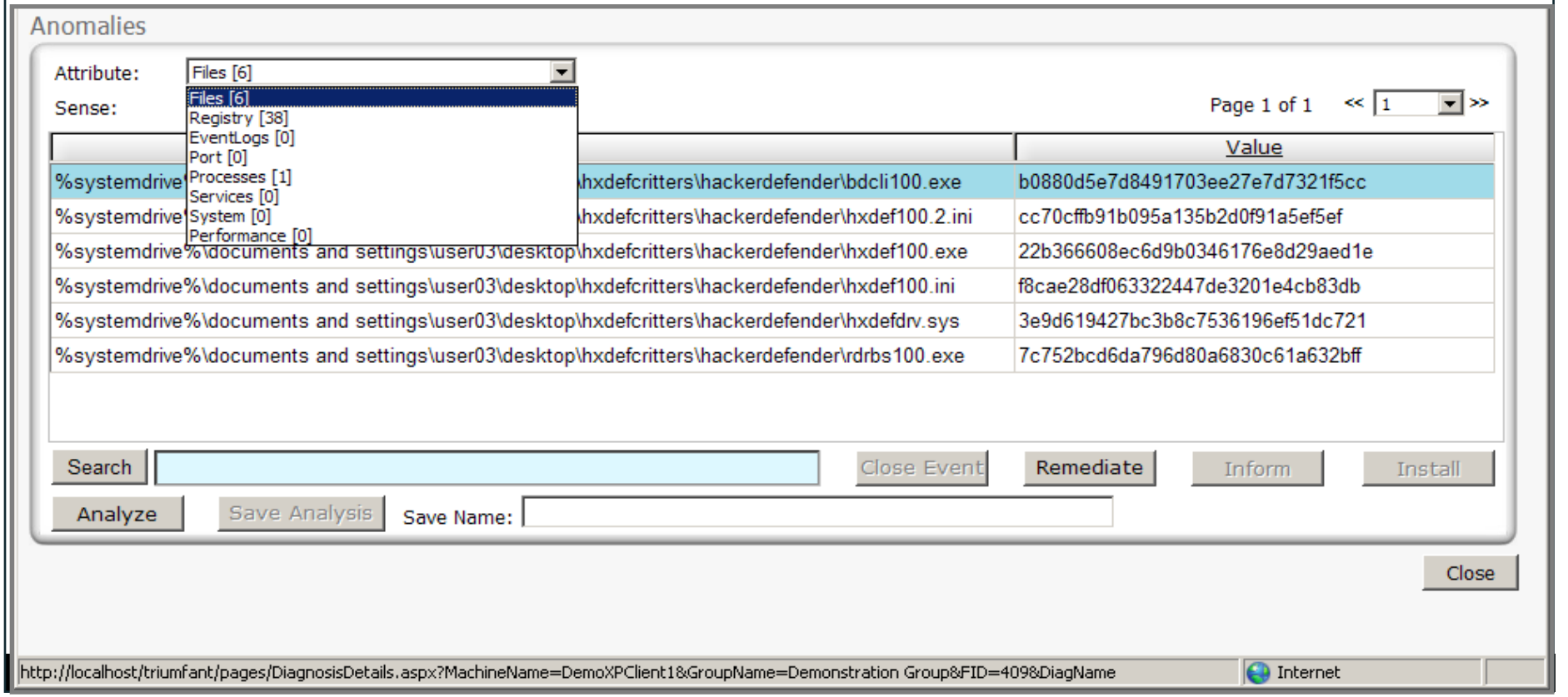
When a Potential Attack is Detected

- Agent contacts server immediately with data
- Server assesses and takes immediate action
  - Requests full scan
  - Begins to correlate changes into broader events
- Server may request additional data
  - Synthesizes a probe specific to the situation
  - Uses over 20 correlation algorithms

Triumfant

Every Change Analyzed and Correlated

- Every change is identified
- Changes are correlated/grouped into broader events
- The risk of the event is assessed



Knowledge Enables Precise Action

By detecting and correlating all of the changes associated with an event, it is now possible to automate remediation

Automatically synthesizes a remediation

- Custom, situational, contextual
- No human intervention
- Applied only to the affected machine

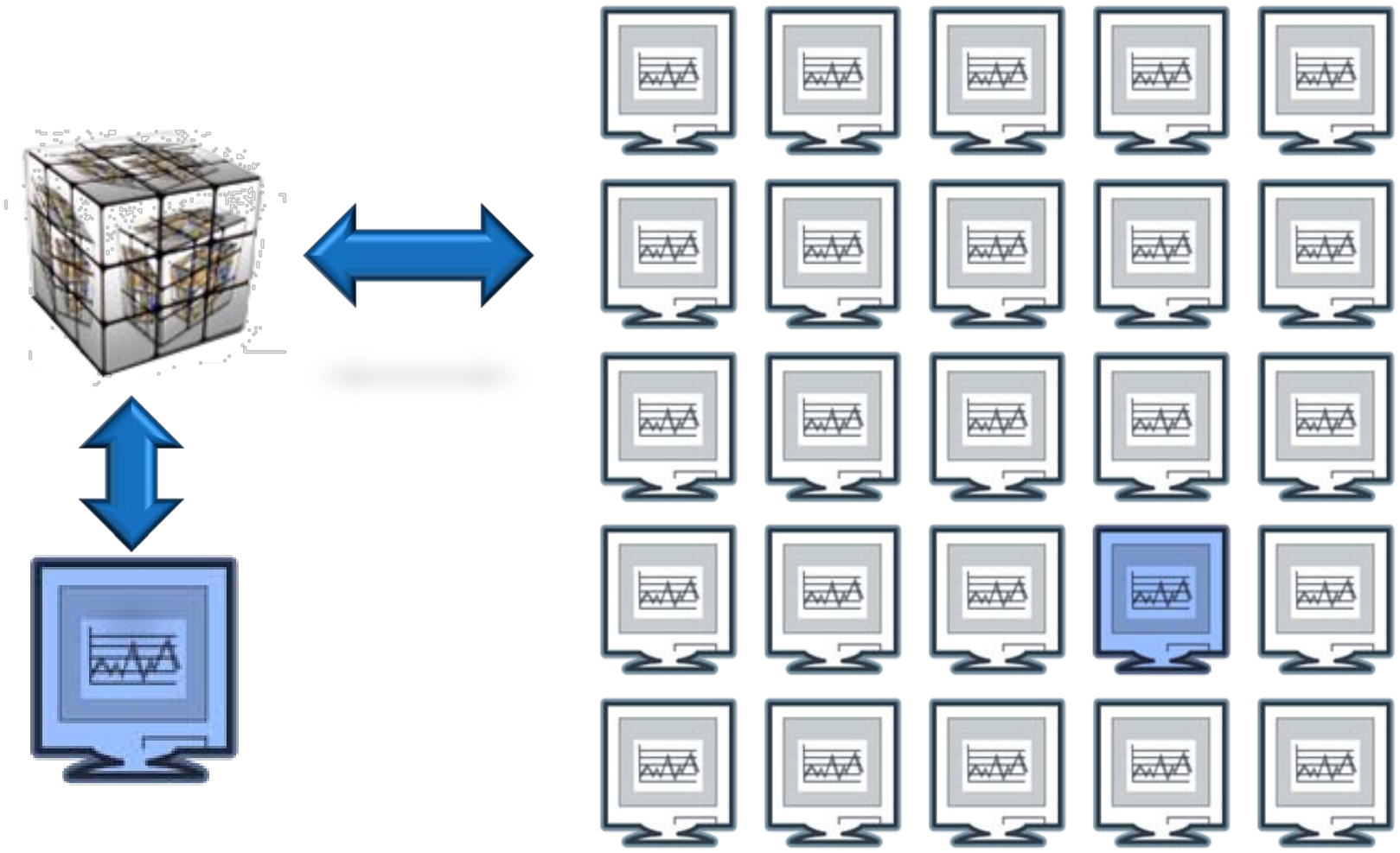
Removes malware and collateral damage

- Replaces corrupted or deleted attributes via Donor Technology
- Closes ports, restores config. settings, etc.

Surgical, unobtrusive, and real-time

- No rebooting
- No re-imaging
- Detection to remediation in five minutes or less

Leveraging the Context for Donor Technology



Automation Through Granular Change Detection

How We're Different	Why it Matters
We continuously gather and store more state information than anyone else	• Enables continuous awareness of the total threat environment • Enables automated knowledge creation and decision making
We provide unique analytic capabilities that learn from the environment	• Minimum administrative cost • Never-before-possible situational awareness • Automated granular control
We automatically synthesize precise responses based on acquired knowledge	• Continuously manages attack surface • No external dependencies • Repairs damage (70% of cost)

Triumfant

Security Automation Through Granular Change Detection

Jim Ivers, CMO and SVP, Product Management
Triumfant, Inc.