Security tools don’t buy security

Chris Van Den Abbeele
Global Solution Architect Datacenter & Cloud Security
Introduction: Trend Micro

- 30 years focused on making “A World Safe for Exchanging Digital Information”
- Headquartered in Japan, Tokyo Exchange Nikkei Index
- Annual sales of approximately $1.3B US, consistently profitable
- Customers include 45 of top 50 global corporations
- 6000+ employees in over 50 countries

500k commercial customers & 250M+ endpoints protected
The MARKET LEADER in server security for 7 straight years.

Source: IDC, Securing the Server Compute Evolution: Hybrid Cloud Has Transformed the Datacenter, January 2017 #US41867116
Best threat intelligence in the world

Discovered **66.3%** of verified vulnerabilities in 2017

**LEADER** in vulnerability discovery since 2007


Trend Micro Research
Security tools don’t buy security

So, what is (/can be) the benefit of security tools? What can we expect from (good) security tools?

- 
- 
- 
-
Security tools don’t buy security

So, what is (/can be) the benefit of security tools? What can we expect from (good) security tools?

- Provide visibility / insight / focus
- Provide decent security without much human intervention
- Provide a high degree of integration and automation

- **Tools should empower Security Personnel to provide great security**
- Tools should be easy to manage
- Tools should be **holistic (minimal toolset with maximum coverage)**
Holistic (workload) Protection
Holistic: protect different generations of workloads

- Public Cloud
- Virtual Servers
- Virtual Desktops
- Containers and Micro-services
- Physical Servers
- Security Automation

Infrastructure as code / security as code

Shifting left security
Holistic: multiple security controls

How many different agents are you running on your servers?
Holistic: multiple security controls

**Network Security**
- Intrusion Prevention
- Firewall
- Vulnerability Scanning

Stop network attacks, shield vulnerable applications & servers

**System Security**
- Application Control
- Integrity Monitoring
- Log Inspection

Lock down systems & detect suspicious activity

**Malware Prevention**
- Anti-Malware
- Behavioral Analysis & Machine Learning
  (requires DDAN)
- Sandbox Analysis

Stop malware & targeted attacks
Automation capabilities
What we hear from our customers

CUSTOMERS WANT TO

Go Automated: connected security that fits seamlessly into Dev and Ops processes to minimize friction & ensure adoption
The process of protecting new server workloads

Workload creation → Test phase → Production
The process of protecting new server workloads

- Workload creation
- Test phase
- Production
Provisioning Pipeline

Workload creation

Commit
Build Applications
Build
Dev instance

Test phase

Test
Base Image

Production

Run
Deploy/Runtime

Maintain

Blue-Green deployments
Security in the build pipeline
Security in the build pipeline

Workload creation

- Build
- Applications
- Dev instance

Test phase

- Test
- Base Image

Production

- Run
- Deploy/Runtime
- Blue-Green deployments

Commit

Maintain
Real live story
Real live story

I once delivered a presentation to prospect, talking about DevSecOps. The Security Officer said she had everything under control, they follow ISO standards, everybody follows procedures and she has a security dashboard where she can see all her protected machines and their security status. All was “fine”, there was no need for a new security product. We had no sales opportunity.

A few weeks later the Operations Manager of that company called me back and asked me to do the presentation again, but now his Operations team.

What had happened?
An unexpected audit had shown that several workloads were not adequately patched and others did not have basic Anti Malware installed.
They had identified 2 root causes:
1. The Operations team has to do more with less, every day. They create more new VMs than ever before. Manually adding the security controls, takes a lot of time and it is often postponed (and/or finally... “forgotten”)
2. The Dashboard of the security officer only showed computers which had been brought under the control of the Security Solution (where a security agent was installed). ... And this was a manual task.

So... Integration with the control plane of the workload orchestrator is required. The Security Tool should detected new VMs immediately without any manual intervention. Once a new computer is detected, all the next steps up to applying full protection, should preferably be automatable.
You can’t protect it if you don’t know it exists

- Are we sure that our security dashboard shows all the workloads?
- How can good security tools help us to provide full visibility?

**Security tool capability:**
Connect to the Control Plane of the Orchestration tool for the workloads

Detecting newly created workloads is an essential requirement, but also gracefully removing deleted workloads from the security solution is key (in stead of having to deal with “cannot connect errors”)
Workload orchestration

Server workload protection
Security is all about context
Workload orchestration

Server workload protection
Security is all about context

• Can you tell if you are looking at a server that is Internet facing or a server that is in the Datacenter behind multiple firewalls?
• Is it a Web server or a Database server?
• Is it a Server or Workstation VM?
• Is it a server with Marketing materials or is it a critical Finance system?
• Is it a Windows server, some Linux server, a Docker Host, a SAP system...

Security tool capability:
Provide rich context on the workloads (empowering security officers to make well informed decisions)
Security is all about perspective (or different perspectives)
Good security tools allow you to look at your workloads from different angles:
- OS
- Security Zone
- Asset Value
- Dev / Prod
- Unprotected VMs

Security tool capability: Allow to change perspective on the fly
Security in the build pipeline

Workload creation

Commit

Build

Applications

Dev instance

Auto-discovery with rich context

Test phase

Test

Base Image

Deploy/Runtime

Production

Run

Maintain

Blue-Green deployments

Auto-

discovery with rich context
Security in the build pipeline

Workload creation

Commit
Build Applications
Dev instance

Test phase

Build
Test
Base Image

Production
Run
Deploy/Runtime

Blue-Green deployments

Maintain
Determine the risk level

- Which OS (/version/patch level/..) is this?
- Which applications are running on this system?
- Which OS vulnerabilities exist on this system?
- Which Application vulnerabilities exist on this system?

-> Run a vulnerability scan (automatically)

Security tool capability:
Provide rich APIs that can be called e.g. from the provisioning pipeline. Preferably using the OpenAPI standard
Built-in Vulnerability Scan

Intrusion Prevention Rules

- 1007596 - Identified Possible Ransomware File Extension Rename Activity Over Network
- 1006017 - Restrict OpenSSL TLS/DTLS Heartbeat Message
- 1006016 - OpenSSL TLS/DTLS Heartbeat Message Information Disclosure Vulnerability
- 1006012 - Identified Suspicious OpenSSL TLS/DTLS Heartbeat Request

Last Scan for Recommendations: October 10, 2016 16:14

Unresolved Recommendations:
- Assign 991 additional rule(s)
- Unassign 5 currently assigned rule(s)

Automatically implement Intrusion Prevention Recommendations (when possible): Inherited (No)

Scan For Recommendations
Built-in Vulnerability Scan

Intrusion Prevention

Assign 991 additional rule(s). Unassign 5 currently assigned rule(s)

Automatically implement Intrusion Prevention Recommendations (when possible): Inherited (No)
Security in the build pipeline

Workload creation

- Commit
- Build Applications
- Dev instance

Test phase

- Build
- Test
- Base Image

Production

- Run
- Deploy/Runtime
- Blue-Green deployments
- Maintain

Applications
Commit
Dev instance
Base Image
Run
Deploy/Runtime
Blue-Green deployments
Maintain

33
Locking down the applications/modules/libraries/scripts

- Following the Blue-Green deployment method, we would not allow any changes to systems in Production.
- No more changes to any “executable” applications, modules, libraries and scripts.
- But also:
  No more changes to any sensitive (configuration) files.

**Security tool capability:**
- Application lockdown
- Integrity Monitoring
Computer: cdcdocker.greenhisc.net

Application Control

Configuration: On
State: Inherited (Off)
Enforcement: On

Maintenance Mode

While in Maintenance Mode, new or changed software will be automatically added to the list of Allowed software Ruleset.

Status: N/A

Ruleset

- Inherit settings

Local or shared ruleset:
Application Control

Configuration: On
State: Inherited (Off)
Enforcement: On
- Block unrecognized software until it is explicitly allowed
- Allow unrecognized software until it is explicitly blocked

Maintenance Mode
While in Maintenance Mode, new or changed software will be automatically added to the list of allowed software.
Status: N/A
- Turn On
- Indefinitely

Ruleset
- Inherit settings
- Local or shared ruleset:
Integrity Monitoring
Monitor sensitive files and sensitive registry keys for changes

Application Lockdown:
“Freezes” the server and blocks new executables and scripts from running

Protect against “drift”
Security in the build pipeline

- Workload creation
  - Commit
  - Build Applications
  - Dev instance

- Test phase
  - Build
  - Test
  - Base Image

- Production
  - Run
  - Blue-Green deployments
  - Deploy/Runtime
  - Maintain
New zero days are discovered almost daily

- How quickly *can* you patch?
- How quickly *do* you patch?
- Good security tools allow to quickly protect against newly discovered vulnerabilities

**Security tool capability:** automated, scheduled, vulnerability scans plus automatic assignment of new IPS rules “*Automated Virtual Patching*”
Vulnerability Scan

Scheduled Tasks

- **Name:** Daily Scan Computers for Recommendations
- **Type:** Scan Computers for Recommendations

Schedule Information:
- **Daily**: September 15, 2014, 23:35
- **Days:** Every Day
- **Every**: 2 days
Automated Vulnerability Scan

Computer: SAPNWgw

Intrusion Prevention

- Configuration: Inherited (On)
- State: On, Prevent, 16 rules
- Intrusion Prevention Behavior: Prevent

Assigned Intrusion Prevention Rules

<table>
<thead>
<tr>
<th>Name</th>
<th>Application Type</th>
<th>Severity</th>
<th>Microsoft</th>
</tr>
</thead>
<tbody>
<tr>
<td>1007596 - Identified Possible Ransomware File Extension Rename Activity Over Net...</td>
<td>DCERPC Services</td>
<td>Critical</td>
<td>N/A</td>
</tr>
<tr>
<td>1006817 - Restrict OpenSSL TLS/DTLS Heartbeat Message</td>
<td>OpenSSL Client</td>
<td>Medium</td>
<td>N/A</td>
</tr>
<tr>
<td>1006816 - OpenSSL TLS/DTLS Heartbeat Message Information Disclosure Vulnerability</td>
<td>OpenSSL Client</td>
<td>Medium</td>
<td>N/A</td>
</tr>
<tr>
<td>1006812 - Identified Suspicious OpenSSL TLS/DTLS Heartbeat Request</td>
<td>OpenSSL</td>
<td>Medium</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Recommendations

- Last Scan for Recommendations: October 10, 2016 16:14
- Unresolved Recommendations: Assign 991 additional rule(s). Unassign 5 currently assigned rule(s)
- Automatically implement Intrusion Prevention Recommendations (when possible): Yes

Save | Close
Automated Vulnerability Scan

**Intrusion Prevention**
- Configuration: Inherited (On)
- State: On, Prevent, 16 rules
- Intrusion Prevention Behavior:
  - Prevent
  - Detect

**Assigned Intrusion Prevention Rules**

<table>
<thead>
<tr>
<th>Name</th>
<th>Application Type</th>
<th>Severity</th>
<th>Microsoft</th>
</tr>
</thead>
<tbody>
<tr>
<td>1007596 - Identified Possible Ransomware File Extension Rename Activity Over Net...</td>
<td>DCERPC Services</td>
<td>Critical</td>
<td>N/A</td>
</tr>
<tr>
<td>1006017 - Restrict OpenSSL TLS/DTLS Heartbeat Message</td>
<td>OpenSSL Client</td>
<td>Medium</td>
<td>N/A</td>
</tr>
<tr>
<td>1006016 - OpenSSL TLS/DTLS Heartbeat Message Information Disclosure Vulnerability</td>
<td>OpenSSL Client</td>
<td>Medium</td>
<td>N/A</td>
</tr>
<tr>
<td>1006012 - Identified Suspicious OpenSSL TLS/DTLS Heartbeat Request</td>
<td>OpenSSL</td>
<td>Medium</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Recommendations**
- Current Status: 16 Intrusion Prevention Rule(s) assigned
- Last Scan for Recommendations: October 10, 2016 16:14
- Unresolved Recommendations: Assign 991 additional rule(s). Unassign 5 currently assigned rule(s)
- Automatically implement Intrusion Prevention Recommendations (when possible): Inherited (No)
Making the Business Case For Automated Virtual Patching
(a little segway)
Typical patch cycle without virtual patching

- **Monthly Security Patching**
- **Half-yearly Full Patching**

12 x patching /year
Scheduled Recommendation Scans
Computer: SAPNWgw

Intrusion Prevention
- Configuration: Inherited (On)
- State: On, Prevent, 16 rules

Intrusion Prevention Behavior
- Prevent
- Detect

Assigned Intrusion Prevention Rules
- 1007596 - Identified Possible Ransomware File Extension Rename Activity Over Network
- 1006017 - Restrict OpenSSL TLS/DTLS Heartbeat Message
- 1006016 - OpenSSL TLS/DTLS Heartbeat Message Information Disclosure Vulnerability
- 1006012 - Identified Suspicious OpenSSL TLS/DTLS Heartbeat Request

Recommendations
- Current Status: 16 Intrusion Prevention Rule(s) assigned
- Last Scan for Recommendations: October 10, 2016 16:14
- Unresolved Recommendations: Assign 991 additional rule(s). Unassign 5 currently assigned rule(s)
  - Automatically implement Intrusion Prevention Recommendations (when possible): Inherited (No)
  - Scan For Recommendations
  - Cancel Recommendation Scan

Setting: Yes
Typical patch cycle with virtual patching

- Automated Ongoing Security Patching
- Half-yearly Full Patching

2 x patching/year
5 days after ShellShock: 766 attacks blocked
(Customer example)

766 attacks blocked by Deep Security Automated Virtual Patching on Sept 30th, at a customer managing 100+ instances

If Emergency (physical) Patching takes 5 days...
Win-Win: increases security + reduces cost

Typical patch cycle without Virtual Patching

- $y_1$
- $y_2$
- $y_3$

12 x patching /year

- Monthly Security Patching
- Half-yearly Full Patching

Typical patch cycle with Virtual Patching

- $y_1$
- $y_2$
- $y_3$

2 x patching /year

- Automated Ongoing Security Patching
- Half-yearly Full Patching
Further Automation capabilities
Event system

Security tool capability:
Good security tools have an event-system that can be triggered by specific conditions and that can execute predefined tasks

<table>
<thead>
<tr>
<th>Dashboard</th>
<th>Alerts</th>
<th>Events &amp; Reports</th>
<th>Computers</th>
<th>Policies</th>
<th>Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Settings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scheduled Tasks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event-Based Tasks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manager Nodes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tenants</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Licenses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Roles</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contacts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Updates</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rules</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Event-Based Tasks**

Select the event that this task will be based on.

**Event:**
- Select Type
  - Computer Created (by System)
  - Computer Moved (by System)
  - Agent-Initiated Activation
  - IP Address Change
Event-based tasks to profile new systems

Select the event that this task will be based on.

Event: Computer Created (by System)

Select the action(s) to perform.

- Activate Computer Delay (in minutes): 5
- Assign Policy
- Assign to Computer
- Assign to Computed Name
- Platform

Specify any match condition(s). (All conditions have to be met before the task is carried out.)

Platform matches *Win.*
Summarizing
Automated protection for all types of server workloads

Best threat intelligence in the world
Market Leader, 7 years in a row

Protecting the supply chain / Shifting left security
Infrastructure as code / security as code

Security Automation  DevOps
The process of protecting new workloads

Visibility

Seeing new workloads on premise and in multiple clouds as soon as they become online

Context

Workload in Dev or in Prod? Internet facing? Is it a DB server or a webserver? Finance system or whitepaper server?

Risk assessment

What is the Attack-surface? Which exploitable vulnerabilities exist on this workload?

Protect

Anti-Malware, - Host-based Firewall - Intrusion Prevention - Integrity Monitoring - Web Reputation - Application control - Log Inspection

- Continuously:
  - Automated virtual patching
  - Integrity Monitoring
  - App Control
  ...

Maintain

APIs
Thoughts?