Transforming Security from Defense in Depth to Comprehensive Security Assurance

February 28, 2016

Revision #3

Table of Contents

Introduction

The information security field is robust and growing. Hundreds of security solutions are available, and organizations worldwide are investing more in security. But something else is happening—attackers are still penetrating systems, major breaches are occurring, and newer technologies are not well protected against today's threats. It appears that defense in depth—the layering of multiple information security tools to protect networks—is no longer working. No matter how many security solutions you deploy, if they don't work together, your organization is at risk.

Comprehensive security assurance requires unity. It's critical to ascertain if your security solutions are effective. Replacing existing investments is not always necessary, but the components must work together to achieve holistic security.
It's time to transform security from defense in depth to comprehensive security. Achieving unity requires three pillars of security assurance:

- Continuous **Visibility** into all assets, to meet the challenge of eliminating blind spots
- Critical **Context** to prioritize threats and weaknesses for response
- Decisive **Action** to reduce exposure and loss

This paper explains the principles behind comprehensive security assurance and how to achieve comprehensive protection.

The problem: defense in depth is not working

Over the past 20 years, we have witnessed steady growth in the development and marketing of security solutions. But despite the fact that organizations all over the world are investing in sophisticated security solutions and information security professionals, major data breaches are still occurring at an alarming rate.

Investing in layers of defense in depth is no longer working as a complete solution. The industry started out with prevention tools, like anti-virus software and firewalls. Then we moved to detection capabilities, such as anti-malware and intrusion detection systems. Now we have response tools such as SIEMs, threat intelligence, and forensics. All these tools may give the appearance of security, but in reality, attackers know how to circumvent the defenses.

Layering these solutions in a security program is no longer effective. Defense in depth is not preventing attackers from penetrating our systems. Deploying multiple tools and redundant solutions may feel like you are covering all the bases, but in reality, that strategy leaves gaps in security programs rather than providing a multifaceted solution. Once attackers are in a network, they often lurk in the shadows for months at a time, planning the next breach. While attackers lay low in a network, they often remain undetected because security professionals are too busy responding to known threats and alerts. When an attacker finally starts exfiltrating data, often slowly and in pieces, the breach may not be noticed for months on end. This is why experts now say that it's not a question of *if* you will be breached, but *when;* attackers have honed their skills, and they know how to go unnoticed on a busy network.

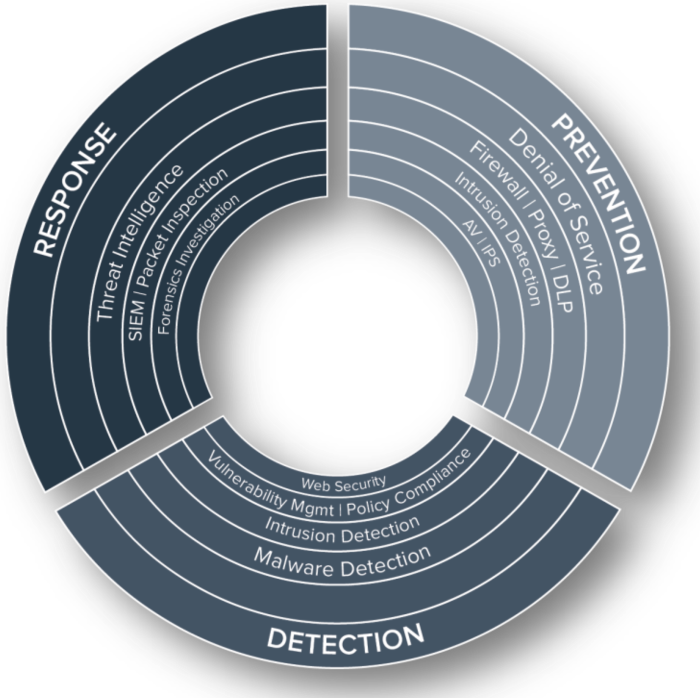

Figure 1: Defense in Depth

Why are so many compromises going unnoticed? Because the traditional defense in depth security is an outdated model. You can buy all the security solutions out there in the market, but if they are not integrated, gaps will open up for attackers to exploit. This strategy is also not effective at protecting newer technologies against threats. Today's digital enterprise runs borderless technologies—in the cloud, on virtual systems, and with mobile devices—in highly distributed and ever-changing systems.

Another problem for defense in depth is that the perimeter is gone. While different types of devices and applications across different environments—on-premises or in the cloud—help productivity and communications in an organization, it has become difficult to manage and secure the assets. Shadow IT—unknown devices, applications and services functioning outside the official scope of the IT department—is fast becoming the majority stake in digital assets. When unknown assets, services, and applications go unidentified, unmaintained, and unmonitored, your infrastructure can be compromised, exposing the company to major risk.

This environment also makes an integrated, holistic security program challenging to build.

The new strategy: comprehensive security assurance

To achieve security assurance, you need unity. This doesn't necessarily mean you have to remove and replace your existing investments; you need to focus on the basic building blocks of a good security program, and you need to have those components working together for comprehensive, holistic security.

You don't need another point solution. You need to transform security, to look at it holistically. You need assurance that your security investments are effective and that they are working together, not fragmented and silo'ed. You don't necessarily need 100 different solutions, but you do need assurance that the capabilities of the solutions that you own are integrated.

Transforming security

It's time to lay a new foundation for the future of security. But how do you achieve unity? With the three pillars of security assurance:

- **Visibility**
- **Context**
- **Action**

These three core pillars serve as the foundation for six basic domains of a sound security program. To achieve comprehensive security, these six domains must be present in your security program, unifying your defenses and providing continual assurance.

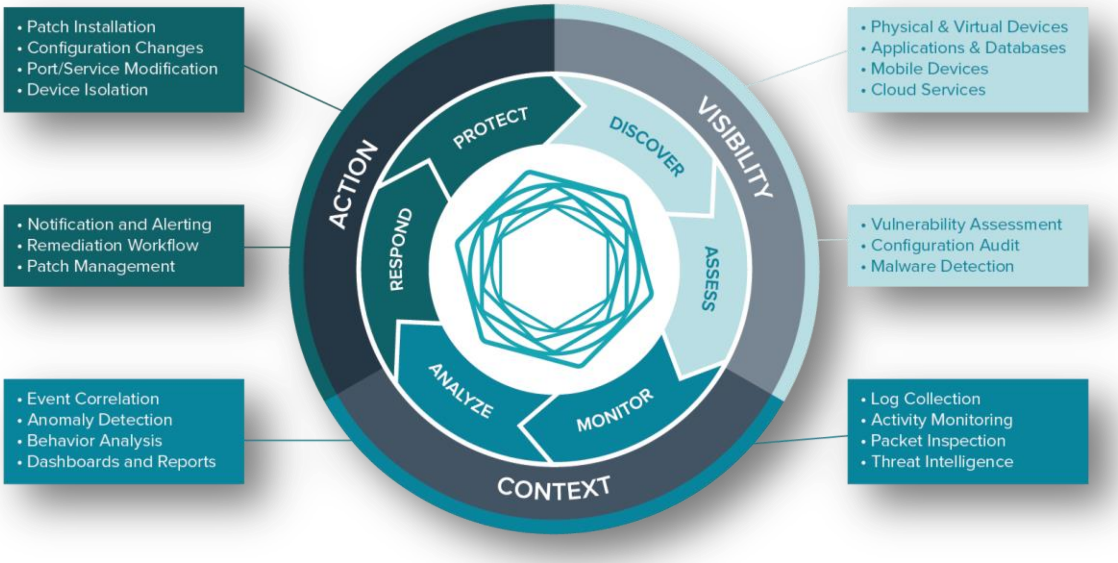

Figure 2: The Six Domains of Security

Achieve visibility

You can't be sure if your network has been compromised without comprehensive and continuous visibility across all systems and devices. Visibility is not just about a periodic scan; it's a full-time endeavor. Attackers are attempting to penetrate networks all the time; you need to find the threats and eliminate the blind spots. While you need a baseline to establish a pattern of normal behavior across all devices and applications—including rogue devices, shadow IT, and virtual systems—you also need continual surveillance to identify anomalous behavior that could indicate a compromise in your environment. Once you identify a potential problem, you can take immediate action before critical data is stolen. In short, you can't achieve security without complete visibility. Knowing what you have is paramount to building a strategy to protect it.

Visibility is achieved with a comprehensive inventory, a baseline of normal activity, and an assessment of the security state of each asset. Visibility encompasses two key domains:

- **Discovery**: You can't protect your network if you don't know what's on your network, both physical and virtual devices, applications, and services–the entire hybrid infrastructure. You must identify and inventory everything, not just the most visible devices and systems. Blind spots such as mobile devices, IoT, and personal cloud services evade point-in-time security scans, and the problem gets more challenging every day.
- **Assessment**: Once you have identified all assets, you must then understand the security state of each asset. You must assess each device for local vulnerabilities, misconfigurations, and malicious activity, baselining each device, system, and application. Attackers know that your weakest links are the entry points that you are unaware of—the open doors that can lead to data breaches. You need to build on a secure foundation to protect your organization's digital future.

Put context to work

With constant intelligence generated from logs, scans and events, you can quickly become overloaded with data. How can you make sense of it all? You need tools that prioritize threats and weaknesses, to identify the needles in the haystack, to distinguish malicious activity from non-events. By placing data *in context*, you can prioritize anomalies, identify the true threats, and shorten the time to respond and remediate. Instead of trying to respond to every alert and notification, you can concentrate your efforts on the most critical threats to thwart a major breach and to assure security. Contextual information is key.

Contextual information helps prioritize threats and weaknesses that require timely responses. Context is achieved through two primary activities:

- **Monitoring**: Monitoring the security activity of your assets is much more than collecting log data. It's about continual vigilance; leveraging actionable threat intelligence, packet inspection and activity monitoring. Attackers are persistent; security must be persistent, too.
- **Analysis**: Once you have collected data from the Discovery, Assessment, and Monitoring domains, you need to analyze that data to determine if a compromise or breach is in progress. Anomaly detection, event correlation, and behavior analysis provide contextual information and identify potential malicious activity. Data is more easily analyzed in reports and dashboards, which prioritize the risks that must be addressed first.

Facilitate action

While "action" may imply remediation of compromises, it also includes being proactive. Threat hunting is the process of proactively looking for potential compromises on your network before they become actual data breaches. Periodic scans are not good enough to identify new threats and never-before-seen events. Once you run a baseline scan of all your assets—both physical and virtual—you need to follow up with continuous vigilance. Attackers are learning new tricks all the time; network monitoring must be a constant activity to stay one step ahead of the attackers. By proactively monitoring your network for anomalous activity against your baseline, you can spot a potential compromise, learn from it, and quickly respond to stop a breach and cripple the attackers.

Many IT security departments are overwhelmed with the task of reacting to log data and notifications. Rather than investigating all anomalous events, security can be improved by proactively hunting for critical threats, collecting contextual data, and prioritizing actions in response to automatic alerts.

Taking action requires triggered alerts and targeted intelligence:

- **Rapid response**: With actionable intelligence from dashboards and reports, you can prioritize threats and develop a plan of action to respond and shut down breaches before they happen. Tools such as triggered alerts, notifications, patch management and remediation workflows provide the ammunition for responding to attacks.
- **Protection**: Protection is the ultimate goal, not easily achieved. Protection results from the automation of patch management, configuration changes, service modifications, device isolation, and ongoing intelligence gathering to remediate problems and reduce exposure and loss.

By analyzing this framework of the six security domains and mapping it to your operations, you can identify gaps in your security investments and capabilities that must be filled to achieve a unified security program. All your defenses must be aligned with each other, integrated and sharing data to achieve seamless protection.

Putting it all together: the Tenable solution

Tenable secures the future of organizations by delivering comprehensive security solutions that provide continuous visibility and critical context so you can take decisive actions and achieve security assurance.

SecurityCenter Continuous View™ (SecurityCenter CV™) is a comprehensive solution to continuously monitor for and identify vulnerabilities, to detect and identify shadow IT assets, and to provide contextual information that helps prioritize threats and inform actions. It provides assurance that you have the right security investments and that those investments are performing as expected.

To achieve comprehensive security, SecurityCenter CV includes five core components in one integrated solution:

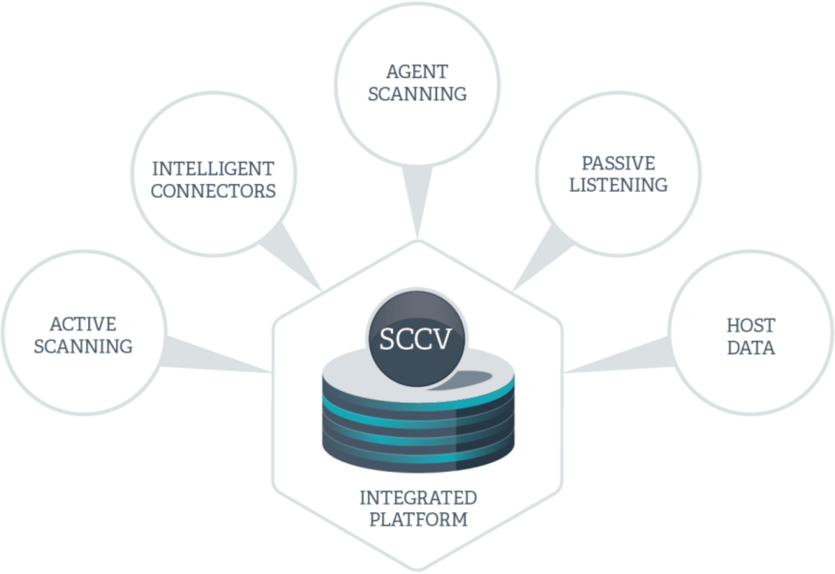

Figure 3: The Five Core Components of SecurityCenter Continuous View

- **Active scanning**: Periodically examines assets to determine their level of risk to the organization
- **Intelligent connectors**: Leveraging your other security investments, integrates additional security data to improve context and analysis
- **Agent scanning**: Instantly audits assets without the need for credentials
- **Continuous listening**: Monitors network traffic in real-time to provide information on which assets are connected to the network and how they are communicating
- **Host data**: Actively monitors host activities and events, including who is accessing them and what is changing

Tenable collects data from these five sensors, analyzes contextual information to prioritize threats, produces dashboards and pre-defined reports, and triggers alerts for decisive action against the most critical threats. Rather than having you sort through endless data, Tenable provides targeted intelligence and alerts for the most important events. You have assurance that you are taking appropriate action to protect your most critical assets against significant threats.

Conclusion

Defense in depth is no longer a total solution. Today's hybrid environments and mobile devices require comprehensive security assurance. By transforming to a comprehensive security program, you can achieve significant business benefits for your organization:

- Eliminate blind spots to reduce your overall attack surface
- Prioritize threats and weaknesses for your limited security resources
- Reduce exposure and loss to minimize overall risk

By concentrating on visibility, context, and action, you can achieve comprehensive security assurance and peace of mind.

For more information

Consult our library of use cases that apply the principles of comprehensive security to Tenable solutions:

Secure the Shadows & Unknown Assets Shadow IT—unknown devices, applications, and services outside of IT—is a major problem when not monitored or maintained. You can't protect what you don't see. In today's environment, you need continuous visibility to achieve comprehensive security. Tenable SecurityCenter CV delivers complete visibility.

Cybersecurity Framework & Tenable A framework such as the NIST Cybersecurity Framework (CSF) can help you build a defensible security program. Its technical controls provide the foundation for a strong security program to better manage and reduce security risk. Tenable automates CSF operation and assessment with CSF-specific Assurance Report Cards and Dashboards.

Threat Hunting Do you know if your network has been compromised? To answer that question confidently, you need a solution like SecurityCenter CV with precision tools for threat hunting. Threat hunting helps you proactively look for compromises and resolve problems before they become breaches.

About Tenable Network Security

Tenable delivers comprehensive security solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. For more information, visit tenable.com.

Transform security with Tenable, the creators of Nessus® and the leaders in continuous monitoring.