Five Essentials for Improving
Endpoint Security
# Table of Contents

- Introduction
- Find Hidden Endpoints
- Identify Security Weaknesses
- Prioritize Known Vulnerabilities on Endpoints
- Identify Advanced Threats on Endpoints
- Measure Security Effectiveness
The next major battle in IT security is focused on endpoints. Mobility and BYOD have made it possible for users to remotely access just about any business resource and data. Cloud-delivered services, directly accessible by mobile workers, are shifting computing to shared environments that bypass on-premises layered defenses. Attackers are targeting remote clients that are no longer confined behind the perimeter and which are not protected by layered defenses. As a result, many organizations are facing the following challenges:

**Endpoints are a hotbed for breaches!**

Traditional signature-based protection is bypassed by modern malware. Mobile devices add fuel to the fire because they are difficult to secure and assess for risk due to limited connectivity and lack of visibility.

**Compromised devices become a springboard for advanced attacks.**

This leads to further infiltration when they connect to internal networks. If infected, identifying the full impact requires both network and endpoint analysis.
Incomplete security view that combines threat assessment with configuration and compliance auditing.
To reduce the attack surface and prevent malware propagation, fixing the underlying problem is just as important as threat detection.

Existing endpoint security solutions can no longer work in isolation.
When solutions are deployed and managed by separate parts of the IT organization security effectiveness suffers. Endpoint security needs to work with network security, compliance, network infrastructure, and operations teams to provide consistent policies, identify and prioritize security issues and remediation actions, and clearly communicate the results.

But, you can get your endpoint security program on track...
By reading this eBook, you’ll be equipped with five essential strategies for achieving endpoint security assurance.

To get started, your endpoint security strategy should completely answer the following questions:

- How many and what types of endpoints are deployed on-premises and in the cloud? Are there endpoints not captured by my security program?
- Are my endpoints free of misconfigurations or security weaknesses that could allow attackers access to critical resources?
- How many endpoints are vulnerable, exploitable, and un-patched?
- How many endpoints are possibly compromised by advanced threats and new malware? Which are propagating malware to other critical endpoints and resources?
- Are my security policies and goals consistently implemented, analyzed, and validated throughout my organization?

Endpoint Security Assurance is a strategic approach that includes identifying weaknesses, finding unprotected endpoints, remediating vulnerabilities, detecting advanced threats, continuously monitoring for indications of compromise, and measuring effectiveness.
Find Hidden Endpoints

Challenges

Today's mobile workforce enabled by BYOD has resulted in a loss of IT control and an influx of unmanaged devices that frequently connect to and disconnect from internal networks. Consider that limited connectivity can cause devices to not always be visible, that many devices may not have the resources to run full versions of security software, and that ownership of the device lies with the user, IT teams are struggling to understand how many and where their endpoints are. Furthermore, deployment of endpoints and applications in the cloud, along with the use of hosted services, has created blind spots for security teams.

80% use unapproved SaaS applications
IT security teams need visibility into all endpoints and the applications running on them. Taking this a step further, security teams also need to identify whether endpoints are vulnerable, correctly configured or exploitable by malware. A Frost & Sullivan study reported that more than 80% of survey respondents admitted to using non-approved SaaS applications in their jobs. In some situations, the IT team is not aware that unauthorized applications are being used. If IT personnel do not have visibility into applications and endpoints, how can they ensure their environment is not compromised or at risk?

What can you do?

- **Scan**: Vulnerability scanners can identify endpoints as well as applications, services, active ports, and more on those endpoints. They can also be useful in discovering and auditing endpoints deployed in the cloud.

- **Traffic Monitoring**: Traffic monitoring technologies continuously analyze network traffic in-between scans to identify endpoints that communicate with other systems within your network as well as with systems that reside outside of your perimeter.

- **Analyze Logs**: Logs from your network infrastructure can be very useful in detecting devices that can’t be scanned. Event data from deployed security infrastructure (Firewall, IPS or other network security devices) can identify unmanaged devices. Events from your network infrastructure including DNS or DHCP servers can provide further insight.

- **Deploy Agents**: Endpoint agents are also useful for identifying applications, services, and changes on endpoints when those systems are disconnected from the network.

- **Integrate Your Strategy**: Integrating all of the above can provide a complete endpoint monitoring solution offering a composite view of endpoints deployed across your organization and in the cloud.
How Tenable Helps

- Regular scanning of your environment can identify endpoints in your network as well as detect operating systems, applications, and services that run on top. For continuous visibility of endpoints and applications connecting to your environment, you must deploy an integrated solution that includes periodic scanning as well as continuous network traffic monitoring and log analysis to provide a composite view of all endpoints.

- Tenable’s Vulnerability Management solutions offer flexible scanning with Nessus® that remotely or locally scans your environment to discover endpoints. Using Nessus, you can also audit cloud accounts to detect virtual machines running in the cloud. You can even deploy Nessus agents on virtual machines to locally scan your cloud assets and applications. Tenable solutions also integrate with your existing endpoint management investments including mobile device management solutions (MDMs) to detect mobile devices that are difficult to scan and identify endpoints managed by patch management systems.

- Tenable’s Continuous Monitoring solution SecurityCenter Continuous View™ expands visibility, filling the assessment gaps between active scans by incorporating:
  
  - **Network Traffic Monitoring:** Tenable’s network traffic monitoring solution, Passive Vulnerability Scanner™ (PVS), can continuously identify endpoints that are not detected by active scanning or that can’t be scanned. It detects and profiles endpoints that communicate externally as well as with other internal hosts.

  - **Log Analysis:** Tenable’s Log Correlation Engine™ (LCE) lets you aggregate, normalize, correlate, and analyze event log data from raw network traffic, intrusion detection data, system and application logs, and user activity within your infrastructure.
Identify Security Weaknesses

Challenges

Deploying a secure network is essential in preventing access to your critical endpoints. According to the 2015 Verizon DBIR, errors made by internal staff, including system administrators were the prime actors in over 60% of incidents. These types of errors can be due to configuration errors that introduce security weaknesses or due to not hardening server operating systems, middleware, databases, enterprise applications, and endpoint management systems.

60% of incidents attributed to errors by system administrators
What can you do?

- **Harden Endpoints:** Harden your endpoints to reduce your exposure. Identify misconfigurations such as open ports that allow attackers access to critical servers and remove default passwords and settings. Ensure security software is updated and enabled.

- **Identify Weaknesses:** Look for critical weaknesses such as admin access, insecure services, unencrypted transactions containing payment card or POS transactions, Social Security Numbers, and other PII information specific to your industry, such as patient identifiers for healthcare.

- **Establish a Baseline:** Establish gold images or profiles to ensure consistent deployments throughout your organization. Continuously monitor for critical deviations.

- **Monitor Change:** Continuously monitor for critical changes to endpoints, applications, databases, network devices, and be vigilant for systems that drift out of compliance.

- **Implement Authorization:** Establish a change authorization process and monitor for unauthorized configuration changes.

How Tenable Helps

- Auditing your environment for misconfigured endpoints can thwart attackers from taking advantage of security weaknesses. Continuous monitoring can help track changes from baseline configurations. This lets you proactively identify changes that can enable an attack or represent a compliance issue.
• Tenable’s vulnerability management solutions can audit on-premises and cloud deployments, and identify whether your endpoints – including operating systems, applications, databases, and network devices – are configured correctly based on vendor best practices, CIS benchmarks or industry regulations including HIPAA, PCI, NIST, and more. Tenable provides more than 450 audit policies for a wide range of assets and standards including operating system audits, application audits, database audits, content auditing, network infrastructure audits, and standards-based audits. Nessus can help you maintain gold images of your endpoints by scanning and reporting on critical changes that introduce security weaknesses.

• Tenable’s Continuous Monitoring solution offers real-time monitoring of configurations from the integration of Nessus scans, real-time monitoring using Tenable’s unique Passive Vulnerability Scanner (PVS), and the Log Correlation Engine (LCE). It detects system change events in real-time and automatically performs a configuration audit on new or changed systems. Continuous monitoring ensures that logging is configured correctly for Windows and Unix hosts, and audits the configurations of web application operating systems, applications, and SQL databases. For example, Tenable continuously monitors your endpoints to identify if SSL is enabled, but also monitors traffic from endpoints to verify if there is unencrypted traffic sent out due to misconfiguration or even malware. In addition, it identifies and prioritizes endpoints that access cloud applications such as Salesforce and checks security setting such as authorization configurations, network settings, permissions, password policies, logins, and more.
Prioritize Known Vulnerabilities on Endpoints

Challenges

According to the Verizon DBIR, more than 70% of attacks exploited known vulnerabilities with available patches. Ten CVEs accounted for almost 97% of the exploits observed in 2014. Organizations can vastly reduce exposure and prevent breaches by promptly removing vulnerabilities on endpoints. A common problem, however, is that the sheer number of vulnerabilities and threats can be overwhelming, making timely remediation a challenge. Organizations can focus on identifying those vulnerabilities that are critical; however, determining what to focus on first requires sufficient context about the endpoint and a clear understanding of not only what’s critically vulnerable, but also what is exploitable.
What can you do?

- **Identify Vulnerable Endpoints:** Regularly scan for vulnerable endpoints and implement a patch management program to knock out top vulnerabilities.

- **Use CVSS Scoring:** Use endpoint context and prioritize remediation by using CVSS scores as a first step to resolve severe vulnerabilities.

- **Pinpoint Exploitable Vulnerabilities:** Narrow your focus by identifying exploits that are added to popular exploit frameworks such as Metasploit.

- **Update Software:** Identify software that is not updated and ensure that patches are regularly applied.

- **Monitor Continuously:** Implement a continuous monitoring process to identify and track vulnerabilities in-between active scans.

How Tenable Helps
• Identifying vulnerabilities is a good start toward a proactive security program, but prioritizing critical vulnerabilities across all endpoints is where organizations face major challenges. Focusing on the most pressing issues first can reduce exposure and help enable your limited resources to take decisive and impactful remediation actions.

• Tenable’s Nessus vulnerability management solutions help identify risk in your environment by scanning operating systems, databases, and applications on your endpoints to identify vulnerabilities and then prioritize threats based on a variety of factors, including severity, exploitability, by asset groups, by remediation and risk reduction. Nessus prioritizes vulnerabilities based on industry standards such as CVSS scores and SCAP severity levels.

• Tenable solutions further prioritize vulnerabilities that can be exploited by commercial testing tools including Metasploit, Core Impact, Canvas, and more to help prioritize remediation. Attackers often use such tools for compromising endpoints, so remediating exploitable vulnerabilities quickly can help organizations reduce significant amount of risk.

• Tenable’s SecurityCenter continuous monitoring solution expands security analysis by tracking and trending endpoint vulnerabilities by continuously monitoring endpoints as they are updated and patched. It includes powerful dashboards and reports that help visualize vulnerabilities based on a variety of factors such as asset type, operating system, application type, exploitability, and more.
Identify Advanced Threats on Endpoints

Challenges

More than 90% of organizations have traditional endpoint anti-virus software deployed. While anti-virus provides a good start for detecting known malware, detecting advanced malware requires monitoring and tracking of normal endpoint behavior and then identifying endpoint activities that are indicative of compromise.
There are a variety of technologies that organizations may have implemented to detect advanced threats, however, organizations need a composite view of threats correlated with endpoint context such as prioritized vulnerabilities, abnormal endpoint behavior correlated with indicators of compromise, detection of malicious processes as well as identifying malware propagation from compromised endpoints.

What can you do?

- **Use Malware Hashes**: Complement vulnerability scanning by using multiple threat intelligence feeds and malware hashes from reputable sources to scan your environment for compromised endpoints.

- **Look for Malicious Processes**: Improve incident response by prioritizing endpoints that are running malicious processes or that are actively communicating with known command and control servers or botnet sites.

- **Look for Malware Propagation**: Identify malware propagation by analyzing network traffic and log analysis – for example, detect malicious file downloads or compromised hosts hosting malware.

- **Spot Abnormal Activities**: Monitor for unusual activities such as scanning from endpoints that have exploitable vulnerabilities. Identify unencrypted PII data sent to suspicious external sites. Use existing defenses such as firewalls, IPS, Network Access Control Frameworks to block active connections or data exfiltration.

- **Reduce Noise**: Share vulnerability scan results with threat management teams to establish threat relevancy with targeted endpoint and reduce the noise from threat monitoring products.
How Tenable Helps

- Endpoint security solutions must not only detect endpoints with exploitable vulnerabilities, but also identify and prioritize those that have malicious processes on the endpoint as well as identify new threats by correlating abnormal and malicious activities on endpoints.

- Tenable solutions not only scan endpoints to identify vulnerabilities, but also detect rapidly changing malware by checking endpoint processes against dozens of virus feeds to identify malware not detected by single engine anti-virus deployments.

- Tenable solutions can check endpoints for malware patterns that are detected by your existing security solutions such as Network IPS or NGFW. When you provide detected malware hashes to Tenable solutions, they can scan your endpoints for those patterns and confirm whether the malware has actually detonated and whether it successfully compromised the endpoint. It also tracks malware propagation inside your network as infected endpoints connect and communicate with other internal resources. You can also reduce false positives on your network security solutions by using vulnerability data to establish alert relevancy and implement blocking actions on active connections communicating with dangerous sites.

- Tenable’s Continuous Monitoring solution can also identify advanced attacks by profiling unusual activities from endpoints such as scanning of other endpoints or unencrypted PII data sent to external servers or botnet sites.
Measure Security Effectiveness

Challenges

Security, network infrastructure, and compliance solutions may be deployed and managed by separate parts of the organization. Often the objectives of each team are independent, but sharing goals and information from security activities and assessments can help provide a closed-loop view of how quickly security and compliance issues are detected, prioritized, remediated, and validated. In a 2015 ISACA report, a majority of infosec professionals surveyed believed they were able to secure their information effectively, yet only 22 percent of them believed so with a high degree of confidence. Moreover, the survey showed that more than a third did not believe that their organization effectively secures its data. Part of the problem is due to lack of consistent policies, goals, and visibility and measurement of key performance indicators across the organization.
What can you do?

- **Create Consistent Policies**: Start by building consistent security policies and then grade your endpoint security effectiveness against them.

- **Use Existing Frameworks**: Implementing an endpoint security program based on defined frameworks (such as the Critical Cyber Controls) that can help create a comprehensive, closed-loop processes to bring consistency to how security is implemented and measured across the entire organization.

- **Verify Patching**: Form a remediation plan that includes immediate blocking of active threats and compromised endpoints, but also long-term remediation strategy that is integrated, correlated, and validated against patch management results and software updates.

- **Measure Results**: Build dashboards and reports that continuously measure and visualize how quickly critically vulnerable, compromised, or non-compliant endpoints are detected and remediated.

- **Close Gaps**: Identify any gaps where endpoint security policies are failing to meet business objectives and employ a strategy to close them.

How Tenable Helps

- Organizations may have deployed a variety of network and security products to address security objectives and corporate and industry compliance goals. However,
security leaders need solutions that can clearly and concisely analyze and communicate the effectiveness of their security investments to key stakeholders throughout the organization.

- Tenable’s continuous monitoring solution measures, analyzes, and trends the security and compliance posture of your endpoints. It provides pre-built and customizable dashboards and reports to meet the needs of multiple teams throughout the organization. Tenable provides visibility into not only the current status, but also the actions that would reduce the most risk, enabling you to effectively remediate and provide measureable results to key stakeholders.

- Tenable offers many types of policies that are build around security frameworks including Tenable’s Critical Cyber Controls, Center for Internet Security’s Critical Security Controls, NIST Information Security Continuous Monitoring - SP 800-137, or ISO/IEC 27001 Information Management Security System Requirements, and more. Such policies provide consistency and offer a closed-loop security program that can be measured and graded.

- Tenable’s Assurance Report Cards (ARC)s communicate security program objectives and results in clear and concise terms. They let you identify and close potential security gaps and communicate the effectiveness of security investments to C-level executives, board members, and business managers.

Conclusion

Endpoint security assurance is more than just detecting threats. It provides a more effective approach to endpoint security by:

- Proactively detecting known and unknown endpoints
- Identifying weaknesses existing in your environment
- Identifying endpoints critically vulnerable to attacks
- Determining how effective you are at identifying and remediating threats

If you are clearly able to answer the question, “How secure are we?” and demonstrate this throughout the organization, you are already on your way to having a successful endpoint security program, and knowing your endpoints are not the weakest link in your security strategy.
About Tenable Network Security
Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk, and ensure compliance. Our family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data. Tenable is relied upon by many of the world’s largest corporations, not-for-profit organizations and public sector agencies, including the entire U.S. Department of Defense. For more information, visit tenable.com.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc. SecurityCenter Continuous View, Passive Vulnerability Scanner, and Log Correlation Engine are trademarks of Tenable Network Security, Inc. All other products or services are trademarks of their respective owners.