



Including Shadow IT in Your Vulnerability Management Program

Diane Garey
Tenable Product Marketing
dgarey@tenable.com

Today's Discussion

- **What** is Shadow IT
- **Why** make it part of your vulnerability management program
- **How** to include it

What is Shadow IT

Shadow IT

Information-technology systems and solutions built and used inside organizations without explicit organizational approval.

What	Examples
Storage / files	Dropbox, Box, Google Apps
IaaS	Amazon, Azure, Google Compute Engine
SaaS / Subscription	Online chat, LMS Web survey, polling tools, Adobe

Shadow IT?



"Serving Humanity to Honor God"

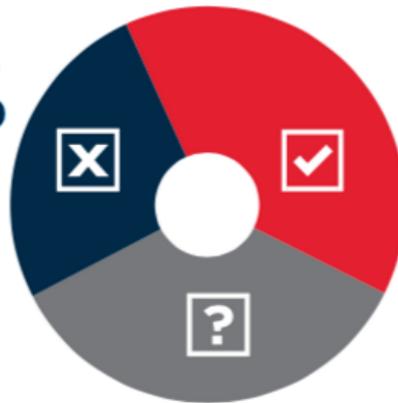
"You miss a lot of systems as you grow or if someone leaves. We had a web server that was set up by an outside vendor for our PR department. Web designers didn't manage the box; they just used the services on the machine."

Shadow IT?

Have any of your BYO or corporate-owned devices downloaded malware in the past?



26%
NO



39%
YES

35%
Not Sure

Shadow IT by the Numbers

80%

... of survey respondents admitted to using non-approved SaaS applications in their job per Frost & Sullivan.

8%

...companies that know the scope of shadow IT at their organizations, according to a survey by the Cloud Security Alliance.

37%

...Unsure if mobile devices were involved in security breaches in their organization in the past

742

...average number of cloud services used by government agencies in the USA and Canada; 10-20 times more than the IT department manages via a study of 800,000 by Skyhigh Networks

Why Make Shadow IT Part of Your Vulnerability Management Program

Security Frameworks

- The first step in most security frameworks is to **inventory assets**
 - CIS Critical Security Controls –
CSC 1: Inventory of Authorized and Unauthorized Devices

Framework Core Categories

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies & Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communication	Improvements
Governance	Data Security	Detection Process	Analysis	Communications
Risk Assessment	Information Protection & Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Freemium -> Cost

Microsoft Azure

[Why Azure](#) [Products](#) [Documentation](#) [Pricing](#) [Partners](#) [Blog](#) [Resources](#) [Support](#)

Create your free Azure account

Get started with \$200 in credit, and thousands of free options

[Start now >](#)

[Or buy now ▶](#)

 SurveyMonkey®

[Home](#) [How It Works](#) [Examples ▾](#) [Survey Services ▾](#) [Plans](#)

BASIC
Free

SELECT
\$26 / month

Billed month-to-month

[SAVE with an annual plan](#)

Get Started with AWS for Free

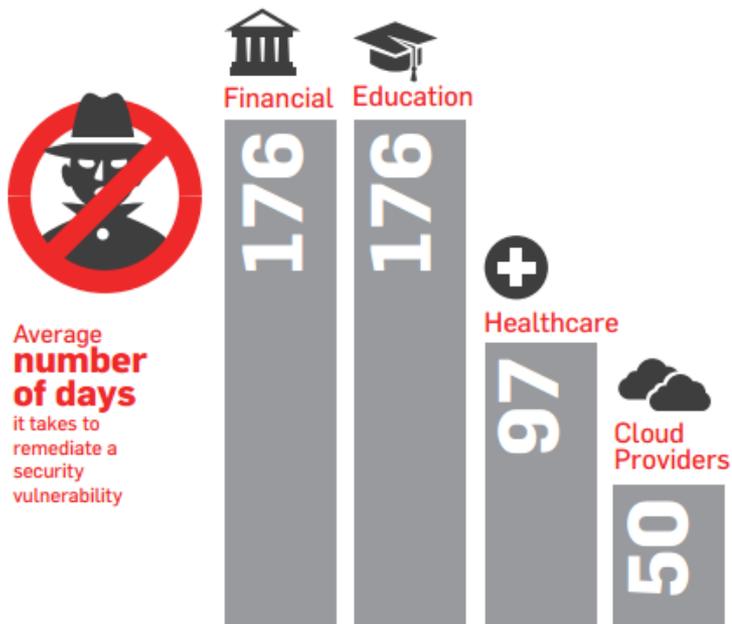
[Create a Free Account](#)

Amazon DynamoDB

25GB of storage and up to 20 million requests/month

[View AWS Free Tier Details »](#)

Cloud Shadow IT Risk

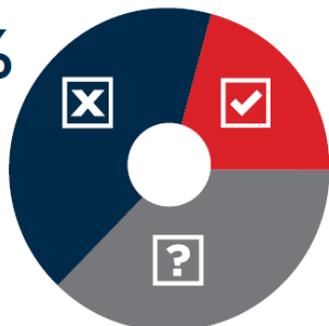


Mobile Shadow IT Risk

Q: Have mobile devices been involved in security breaches in your organization in the past?



42%
NO



21%
YES

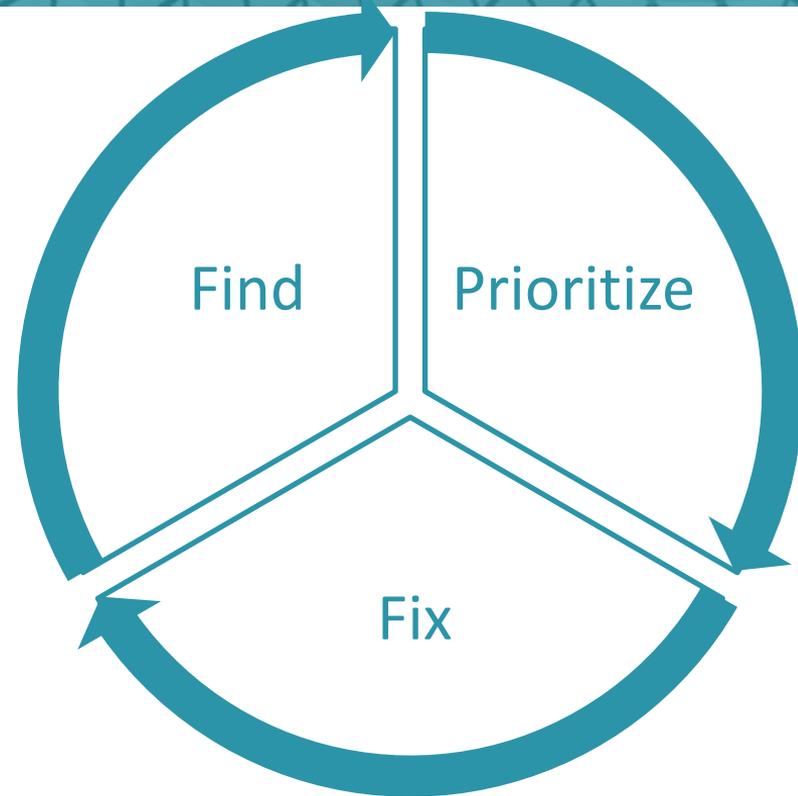
37%
Not Sure

A screenshot of an ExtremeTech article. The article title is "950M phones at risk for 'Stagefright' text exploit thanks to Android fragmentation". The author is Jamie Lendino, dated July 27, 2015. The article features a photo of the green Android robot mascot. Below the article, there are social media sharing options for Facebook (2.3K), Twitter (381), LinkedIn (64), Google+ (87), and a plus sign for other options.

How to Include Shadow IT in Vulnerability Management

Vulnerability Management

- More than vulnerability scanning
 - Process to find, rate, remediate, and track progress
 - Should be about context, context and more context
- Allows for the following:
 - Meeting compliance or regulator goals
 - Defined success factors
 - Measurable
 - Repeatable



Including Shadow IT in Vulnerability Management

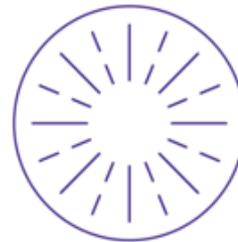
Continuous
Visibility



Critical
Context



Decisive
Action



Continuous Visibility

VM Visibility
Challenge:
Active scanning
alone misses
Shadow IT

Responses:

- Use multiple discovery techniques:
 - Active scanning
 - Passive network scanning
 - Log analysis
- Integrate
 - Mobile Device Management (MDM) integration

Example: Mobile Device Management

- With Mobile Device Management, you set policies for devices to follow:
 - Enable remote wipe
 - Turn on encryption
 - Set complex passcodes
- Integrate MDM auditing with your VM solution
 - Automatically audit MDM results
 - Flag devices that don't adhere to policy



Android Devices and Vulnerabilities

Switch Dashboard ▾

Options ▾

Android Devices and Vulnerabilities - Android Devices by Vulnerability

IP Address	Total	Vulnerabilities
192.168.1.100	220	107 High, 113 Info
192.168.1.101	101	83 Info
192.168.1.102	60	60 Info
192.168.1.103	54	53 Info
192.168.1.104	41	35 Info

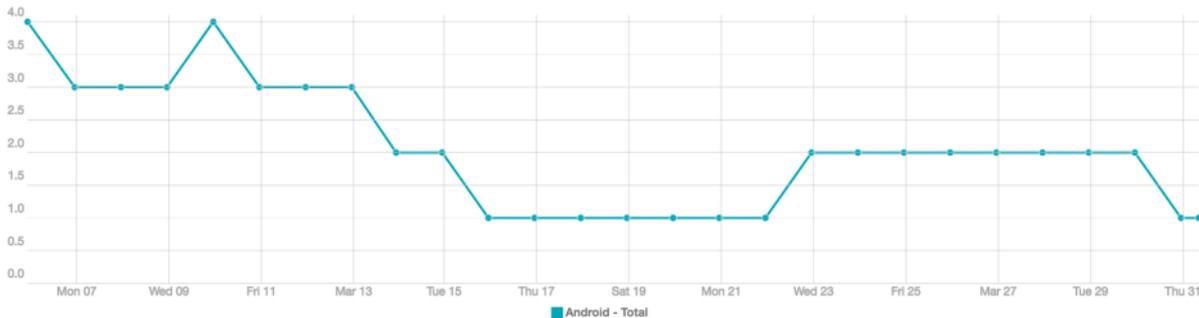
Last Updated: 2 minutes ago

Android Devices and Vulnerabilities - Android Vulnerabilities by Severity

Plugin ID	Name	Severity	To...
90195	Google Chrome < 49.0.2623.108 Multiple Vulnerabilities (Mac OS X)	High	1
4645	Google Chrome Version Detection	Info	3
8996	Google Public DNS Usage Detection	Info	3
8453	Google Drive Detection via DNS	Info	2
800100	Google Chrome Version Detection	Info	1

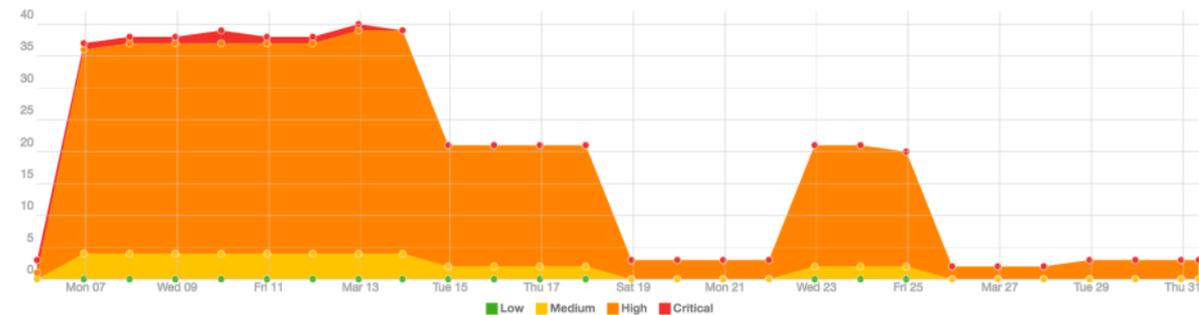
Last Updated: 1 minute ago

Android Devices and Vulnerabilities - Android Device Trend - Past 25 Days



Last Updated: 3 minutes ago

Android Devices and Vulnerabilities - Android Vulnerability Trend - Past 25 Days



Last Updated: Less than a minute ago

Critical Context

VM Context
Challenge:
Difficult to
know true risk

Meet the Challenge:

- Limit data access
 - DRMs
- Control who has access
 - ACLs
- Shadow IT <-> known asset relationships
 - Passive monitoring
 - Log data

Example: Using Google Drive for Sharing Files

- Risks:
 - No control over what data is shared
 - No control where shared data is going
 - No control over who is able to share
- Responses
 - Use DRM to limit access to data
 - Use ACL to limit where data can go
 - Evaluate alternatives. E.g., Google Enterprise
 - Monitor cloud services and relationships

Cloud Services - Services Detected

Plugin ID	Name	Total
8453	Google Drive Detection via DNS	4
8451	GMAIL Cloud Service Detection	4
801800	Gmail Detection	1
8535	YAHOO! MAIL Cloud Service Detection	1
8475	Microsoft OneDrive Detection via DNS	1

Last Updated: 35 minutes ago

Cloud Services - Service Types Detected

File Sharing	Note Sharing	E-mail	Webinar	Social
CRM	ERP	Resource Planning	HR	Infrastructure

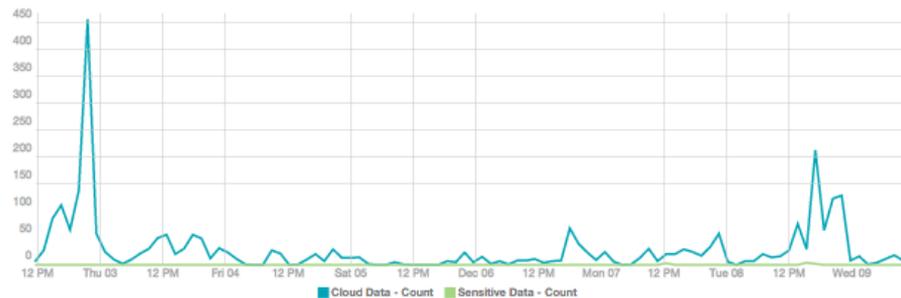
Last Updated: 49 minutes ago

Cloud Services - Popular Services

box.com	DocuSign	Dropbox	Evernote	GitHub
Google Apps	Google Drive	iCloud	Microsoft Dynamics	NetSuite
OneDrive	QuickBooks Online	Salesforce	WebEx	Workday

Last Updated: 49 minutes ago

Cloud Services - SSL Sessions Over Last 7 Days



Last Updated: 51 minutes ago

Cloud Services - Subnets Interacting with Cloud Services



Last Updated: 59 minutes ago

Decisive Action

VM Action
Challenge:
Using limited
resources most
effectively

Responses:

- Use all the data
 - Passive monitoring
 - Log data
 - Threat intelligence
- Track progress
 - Frameworks
 - Analytics

Example: Cybersecurity Framework

- Challenge: Want to follow best practice advice
 - How to evaluate and communicate?
 - How to improve CSF conformance posture?
 - How to use CSF to prioritize security investments?
- Responses:
 - Automate assessment of controls
 - Centralize data storage
 - Track and communicate progress

Assurance Report Cards

+ Add

Options ▾

✕ CSF IDENTIFY.Governance (ID.GV) ▾

Last Evaluated 33 minutes ago 🔄

- ✕ 1. At least 95% of actively and passively detected systems have been scanned for compliance in the past 90 days Non-Compliant
- ✓ 2. Less than 25% of compliance checks failed on Windows, Linux, Solaris and Mac OS machines Compliant
- ✕ 3. Less than 5% of secure configuration compliance checks failed Non-Compliant
- ✕ 4. Less than 5% of anti-malware compliance checks failed Non-Compliant
- ✕ 5. Less than 5% of data protection compliance checks failed Non-Compliant
- ✕ 6. Less than 5% of login configuration compliance checks failed Non-Compliant
- ✓ 7. Less than 5% of default account/password compliance checks failed Compliant
- ✕ 8. Less than 5% of least privilege compliance checks failed Non-Compliant
- ✕ 9. Less than 5% of database compliance checks failed Non-Compliant
- ✕ 10. Less than 5% of web server compliance checks failed Non-Compliant
- ✕ 11. Less than 5% of remote access compliance checks failed Non-Compliant
- ✕ 12. Less than 5% of removable media and USB compliance checks failed Non-Compliant
- ✕ 13. Less than 5% of wireless compliance checks failed Non-Compliant

Click to drill down



Vulnerability Summary ▾

3

Plugin ID	Name	Family	Severity ▾
1021147 ⓘ	Compliance Check Test Error	N/A	High
1015137 ⓘ	BSI-100-2: S 4.200: It is possible to prevent the device driver for USB storage media from starting up	N/A	High
1015248 ⓘ	BSI-100-2: S 4.21: Preventing unauthorised acquisition of administrator rights - Block ftp for administrative accesses.	N/A	High
1015239 ⓘ	BSI-100-2: S 4.13: Every GID must be unique - Careful allocation of identifiers	N/A	High
1015250 ⓘ	BSI-100-2: T 2.15: Finger service - Loss of confidentiality of sensitive data	N/A	High
1015257 ⓘ	BSI-100-2: S 4.18: Administrative and technical means to control access to the system-monitor and single-user mode	N/A	High
1015261 ⓘ	BSI-100-2: S 5.82: Secure Use of SAMBA - Use encrypted passwords	N/A	High
1015264 ⓘ	BSI-100-2: S 4.151: The Linux packet filter function iptables can be used.	N/A	High
1015286 ⓘ	BSI-100-2: S 4.105: ~/.Xclients - 'xhost +' should never be used.	N/A	High

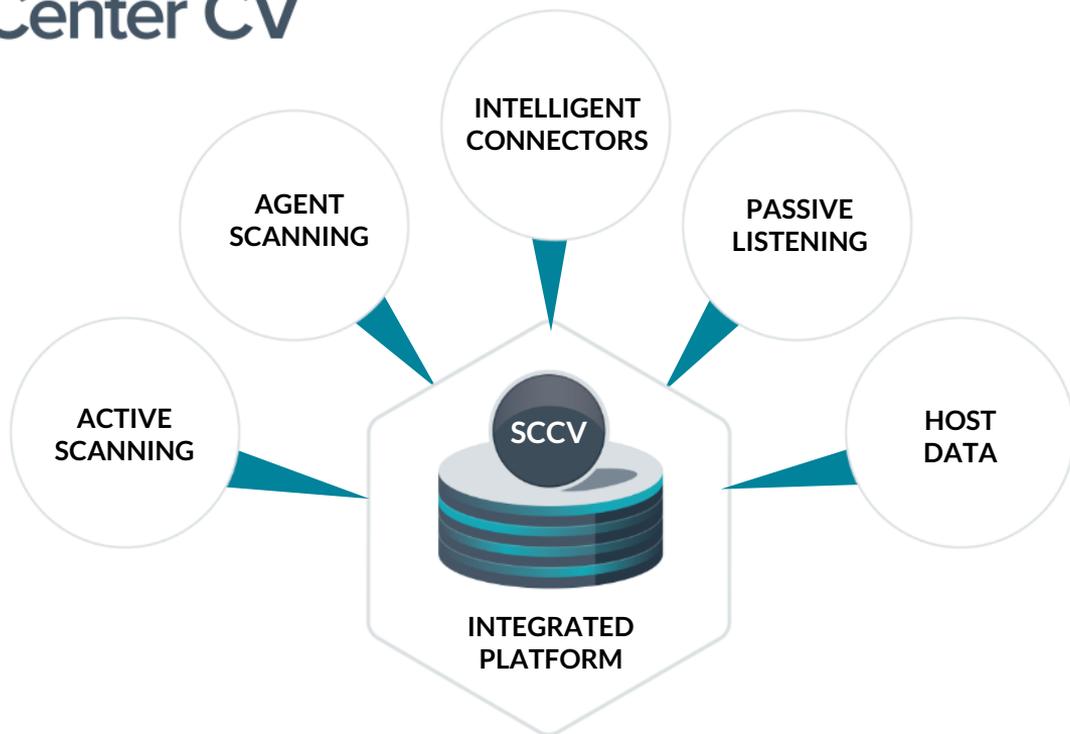
About Tenable Network Security

Founders of Nessus

The screenshot displays the Nessus Scan Library interface. At the top, the Nessus logo is on the left, and navigation links for 'Scans' (with a count of 3) and 'Policies' are in the center. On the right, the user email 'dgarey@tenable.com' is shown along with settings and notification icons. Below the navigation bar, the 'Scan Library' title is followed by a search bar labeled 'Search Library'. A secondary navigation bar includes 'All Templates', 'Scanner', and 'Agent' tabs. The main content area is titled 'Scanner Templates' and features a grid of 15 template cards, each with an icon, a title, and a brief description.

Icon	Template Name	Description
	Advanced Scan	Configure a scan without using any recommendations.
	Audit Cloud Infrastructure	Audit the configuration of third-party cloud services.
	Bash Shellshock Detection	Remote and local checks for CVE-2014-6271 and CVE-2014-7169.
	Basic Network Scan	A full system scan suitable for any host.
	Credentialed Patch Audit	Authenticate to hosts and enumerate missing updates.
	DROWN Detection	Remote checks for CVE-2016-0800.
	Host Discovery	A simple scan to discover live hosts and open ports.
	MDM Config Audit	Audit the configuration of mobile device managers.
	Mobile Device Scan	Assess mobile devices via Microsoft Exchange or an MDM.
	Offline Config Audit	Audit the configuration of network devices.
	PCI Quarterly External Scan	Approved for quarterly external scanning as required by PCI.
	Policy Compliance Auditing	Audit system configurations against a known baseline.
	SCAP and OVAL Auditing	Audit systems using SCAP and OVAL definitions.
	Web Application Tests	Scan for published and unknown web vulnerabilities.
	Windows Malware Scan	Scan for malware on Windows systems.

Pioneers of Continuous Monitoring



Tenable by the Numbers

Greater than
\$100M
Revenue

650+
Employees

Global Distribution
20 Countries
(vs. <6 in 2014)

20,000
Customers

Major
Investments in
Field, Sales,
Channel

\$300M
Invested

15-20%
of Business is
Federal
Government

Thank You!

More Info

- <https://www.tenable.com/solutions/shadow-assets>



Thank You!
dgarey@tenable.com
@dianegarey



tenable[®]
network security