tenable® network security

Eliminating Cybersecurity Blind Spots

Challenges for Business

April 15, 2015

Table of Contents

Introduction

An organization's ability to deliver value to its stakeholders directly correlates to its ability to manage risk. Simply stated, risk is any event that could positively or negatively affect the organization's ability to meet their business objectives. Risk management, a key responsibility of executive management, is not an exact science because identifying all possible outcomes, assigning probabilities to each and estimating the expected financial impact is often based on judgment and estimates, not on hard quantitative data. Fortunately, errors in estimates may average out and result in a reasonable risk model. However, if significant risk blind spots exist, the organization will be overexposed to risk and may suffer unexpected losses.

Risk Management

Businesses and governments are increasingly formalizing processes and procedures to identify, assess and manage risk, and many have adopted an enterprise risk management framework such as COSO's Enterprise Risk Management Integrated Framework, which was originally released in 2004 and is currently undergoing revision.

COSO defines enterprise risk management as follows:
Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.[1]

Risk management principles can help organizations plan for and manage cybersecurity risk. Once cyber risks have been identified, they are assessed according to the likelihood of occurrence, quantitative and qualitative impact, the organization's vulnerability to the risk and the speed of onset. The speed of onset is of particular interest for information security and compliance risks, because organizations often have little or no time between the event's occurrence, detection and effects; by the time the event has been detected, serious damage has been done. Therefore, any actions that can be taken to provide advanced warning regarding an organization's vulnerability to the risk have the potential to reduce or prevent the risk's effects.

After risks have been assessed, the organization must decide whether to avoid, accept, share and/or reduce the risk. In most cases, organizations must have an Internet presence, making complete avoidance of cyber risk impossible. Cybersecurity insurance is becoming increasingly popular as a tactic to share some financial risk of a security breach with an insurance carrier. Risk reduction is the most common course of action, and organizations typically implement controls to diminish the risk to a level they can accept. The most common control categories for information security and compliance risk, listed according to the time they act, are:

- **Preventive Controls** act before the event to prevent the threatening event or incident. For example, firewalls, intrusion protections systems and vulnerability management software work to prevent unauthorized access to the network and reduce systems' susceptibility to malware.

- **Detective Controls** act during or shortly after the event to identify and characterize the threat event or incident. Examples are intrusion detection systems and security information and event management systems, both of which raise alerts when suspicious activity is detected. Of course, bad actors often take one little step at a time to avoid detection.

- **Corrective Controls** act after the event to limit and recover from its impact. Examples include implementing network access control that blocks potentially compromised systems from the network, business continuity plans, and failover sites designed to quickly restore interrupted services.

[1] Enterprise Risk Management – Integrated Framework, COSO

The determination of which information security and compliance controls to implement is a business decision involving building a risk profile that trades off the residual risk that remains after the controls have been implemented with the cost of implementing and maintaining additional controls.

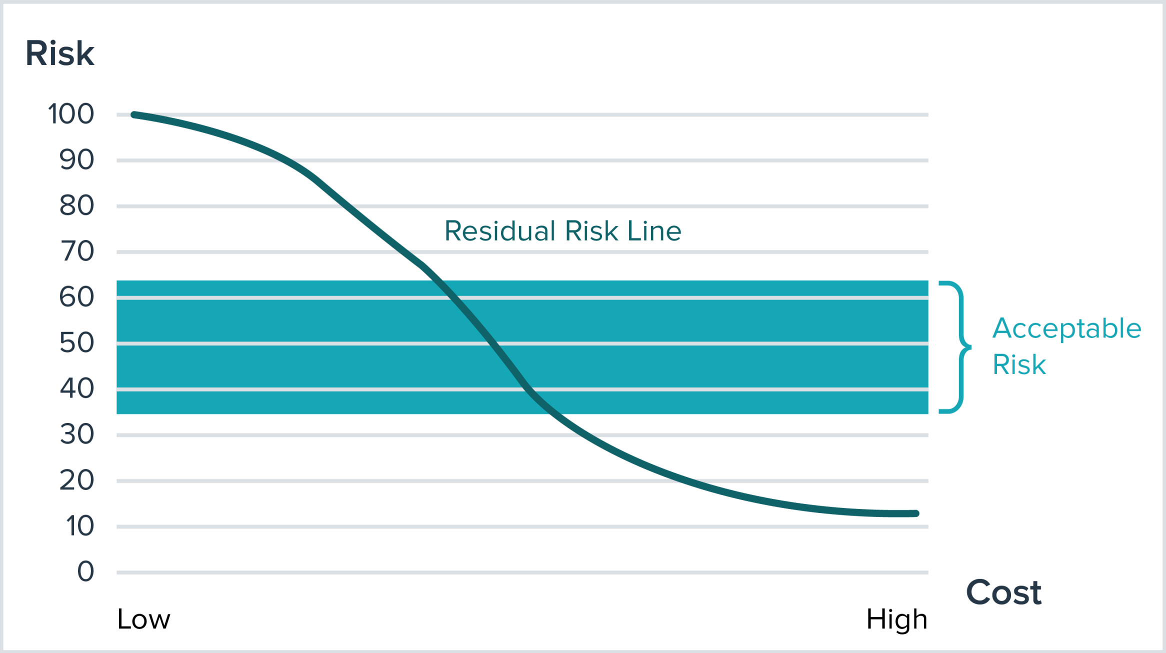


Figure 1. Acceptable Risk Range

However, even with an unlimited budget, 100% security is not achievable. Nor, in most cases, would attempting to achieve it be a sound business decision. The goal should be to operate in a range of acceptable risk by matching residual risk with an organization's risk appetite.

The Risk Blind Spot

Matching an organization's residual risk to its risk appetite assumes perfect or near-perfect knowledge of its risk profile. Unfortunately, the sobering truth is most organizations lack visibility into their actual risk profile, and the actual profile is often seriously underestimated. The realities of the mobile workforce, transient devices and cloud applications introduce an often unknown level of risk.

"Bring-your-own-device" laptops, tablets and smart phones frequently connect to the corporate network, often with minimal or no assurance that they are securely configured and uninfected by malware. Protected/proprietary data can be transferred to these insecure devices, removed from the premises and then exposed. Perhaps even more troubling is the recent trend for protected/proprietary data to move to the cloud, often without IT's knowledge, where it may be used with applications that offer minimal security. A *Frost & Sullivan*[2] study reported that more than 80% of survey respondents admitted to using non-approved SaaS applications in their job. Typical SaaS unsanctioned applications include publishing, business productivity, social media, file sharing, file storage and backup. *CipherCloud*[3] reported that the average global enterprise uses more than 1,100 cloud applications, and that 86% of the cloud applications are unsanctioned by IT.

[2] The Hidden Truth Behind Shadow IT, Frost & Sullivan
[3] Cloud Adoption and Risk Report for North America and Europe, CipherCloud

> If left ungoverned, decentralized, unknown and unmonitored activity presents a significant risk to any enterprise, particularly those companies operating in highly regulated sectors. These risks include issues with data security, transaction integrity, business continuity and regulatory compliance, all of which are often exacerbated by the presence of third-party vendors[4].

Blind spots not only increase security and compliance risk, they also can increase legal risk because information retention policies designed to limit legal liability are very unlikely to be applied to electronically stored information (ESI) contained on unauthorized cloud, mobile and virtual assets. The result is increased legal risk from retaining potentially unfavorable evidence and/or being sanctioned for not producing all potentially relevant ESI. Additionally, e-discovery costs increase as additional data sources must be searched during e-discovery and regulatory inquiries.

The net effect of blind spots resulting from bring-your-own-devices and use of unsanctioned SaaS applications is an undetected shift upward of an organization's actual risk profile, possibly into an unacceptable range.

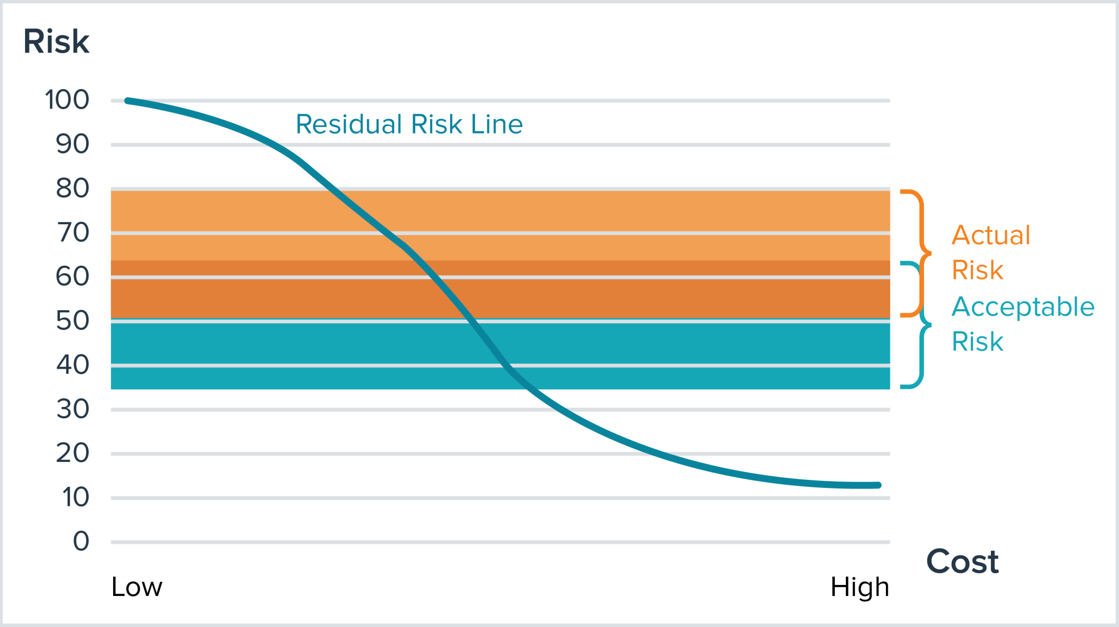


Figure 2. Unknown Assets Increase Actual Risk

Continuous Asset Visibility

Continuous visibility of network assets eliminates the risk blind spot and gives organizations visibility into their true risk profile, allowing them to make informed risk decisions. Asset discovery is so important that it is a foundational part of all popular information security frameworks including:

- **Council on CyberSecurity Critical Security Controls:** Creating an inventory of authorized and unauthorized devices is the first control in the prioritized list of Critical Security Controls, and creating an inventory of authorized and unauthorized software is the second control on the list. According to the Council on Cybersecurity, "Attackers, who can be located anywhere in the world, are continuously scanning the address space of target organizations, waiting for new and unprotected systems to be attached to the network. Attackers also look for devices (especially laptops) which come and go off of the enterprise's network, and so get out of synch with patches or security updates. Attacks can take advantage of new hardware that is installed on the network one evening but not configured and patched with appropriate security updates until the following day." Additionally, the council recommends organizations deploy an

[4] Managing the Shadow Cloud, PWC

automated asset discovery tool and use it to build a preliminary asset inventory of systems connected to an organization's public and private networks, and that both active tools that scan through address ranges and passive tools that identify hosts based on analyzing their traffic should be deployed.

- **NIST Information Security Continuous Monitoring for Federal Information Systems and Organizations – SP 800-137:** Information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities and threats to support organizational risk management decisions. NIST says that ISCM necessitates maintaining situational awareness of all systems across the organization.

- **NIST: Framework for Improving Critical Infrastructure Cybersecurity:** The framework advocates a risk-based approach in which "Identify" is a core function. Within the Identify function, asset management, including an inventory of physical devices, systems, software platforms, and applications within the organization, is the first category to be addressed.

- **ISO/IEC 27001 Information Management Security System Requirements:** The standard requires that all assets be clearly identified and an inventory of all important assets be drawn up and maintained.

- **Tenable's Critical Cybersecurity Controls:** The first control is "Track your authorized inventory of hardware and software." Discovery of all assets is a critical first step, including identification of all authorized or unauthorized hardware and software, transient devices and applications, unknown endpoints, BYOD devices, network devices, platforms, operating systems, virtual systems, cloud applications and services.

Other security frameworks and standards, including the PCI Data Security Standard, COBIT, SEC OCIE Cybersecurity Initiative and NERC/FERC Critical Infrastructure Protection, are consistent in the requirement to maintain an up-to-date inventory of hardware and software.

IT organizations often have asset management tools as part of their IT service management solutions. These asset management tools monitor the network to identify assets. However, they do not typically operate 24/7 and are optimized to detect depreciable assets, such as servers, load balancers and storage devices, used to deliver enterprise applications to the business. These tools are not sufficient for information security because they typically ignore assets not owned by the organization, such as the transient BYOD products that often introduce hidden risk to the enterprise.

Information security requires continuous asset discovery that uses passive, active and event-based technologies to ensure that all assets on the network are identified.

Passive Network Monitoring

Passive network monitoring continuously analyzes network traffic at the packet layer to build a model of active devices and applications on the network. Because passive detection operates 24/7, it will detect transitory assets that may only be occasionally and briefly connected to the network and can send alerts when new assets are detected.

Passive monitoring can frequently determine a device's operating system and version using OS fingerprinting techniques that can also identify protocols and protocol versions. More importantly, passive monitoring can identify client applications used on the network, such as email clients, web browsers and chat programs. It can also detect FTP peer-to-peer file sharing, and connections to cloud services such as DropBox, YouSendIt and Box.net. As described earlier, when protected/proprietary data is sent to unsanctioned cloud applications, organizations are frequently exposed to significant hidden risk. Sophisticated passive monitoring tools have the ability to examine unencrypted data sent to the cloud to determine if it contains protected/proprietary data that should not leave the premises.

Advanced passive monitoring tools can associate discovered operating systems, protocols and applications with known vulnerabilities, enabling organizations to prioritize remediation as vulnerabilities are discovered. These tools can also detect when systems are compromised based on application intrusion detection.

Advantages of passive network monitoring are: it identifies transient systems that may only be on the network a brief time; it does not perturb the network or devices on the network; it has visibility of Internet and cloud services being accessed from systems on the network; and it can identify vulnerabilities in real-time, 24/7, to eliminate gaps between active scans (described below) and accelerate threat remediation. The shortcoming of passive network monitoring is that passive detection sensors must be strategically deployed throughout the network so they can monitor all desired traffic, and if the network is reconfigured without reconfiguring or deploying additional passive sensors, devices and applications may not be detected.

Active Scanning

Active scanning periodically examines the network or a section of the network for devices that are connected to the network at the time of the scan. Many of these devices will have likely been detected by passive network monitoring. However, some may not have been active on the network or may be located on segments of the network not seen by passive monitoring. In this case, they will likely be detected by active scanning.

Because active scanning can interact with and interrogate the systems it discovers, it can obtain in-depth information about vulnerabilities, perform configuration and compliance auditing, and detect malware, backdoors and unknown processes. Additionally, active scanning can accurately identify operating systems and versions. Advanced active scanning products can also determine if devices are storing unencrypted protected/proprietary data on their filesystems.

Advantages of active scanning include in depth analysis of vulnerabilities, malware detection and configuration and compliance auditing. Its shortcomings are that because it is performed periodically, it may miss transient devices and vulnerabilities that arise between scheduled scans, and it cannot realistically scan for devices on IPv6 networks due to the large address space.

Event Log Analysis

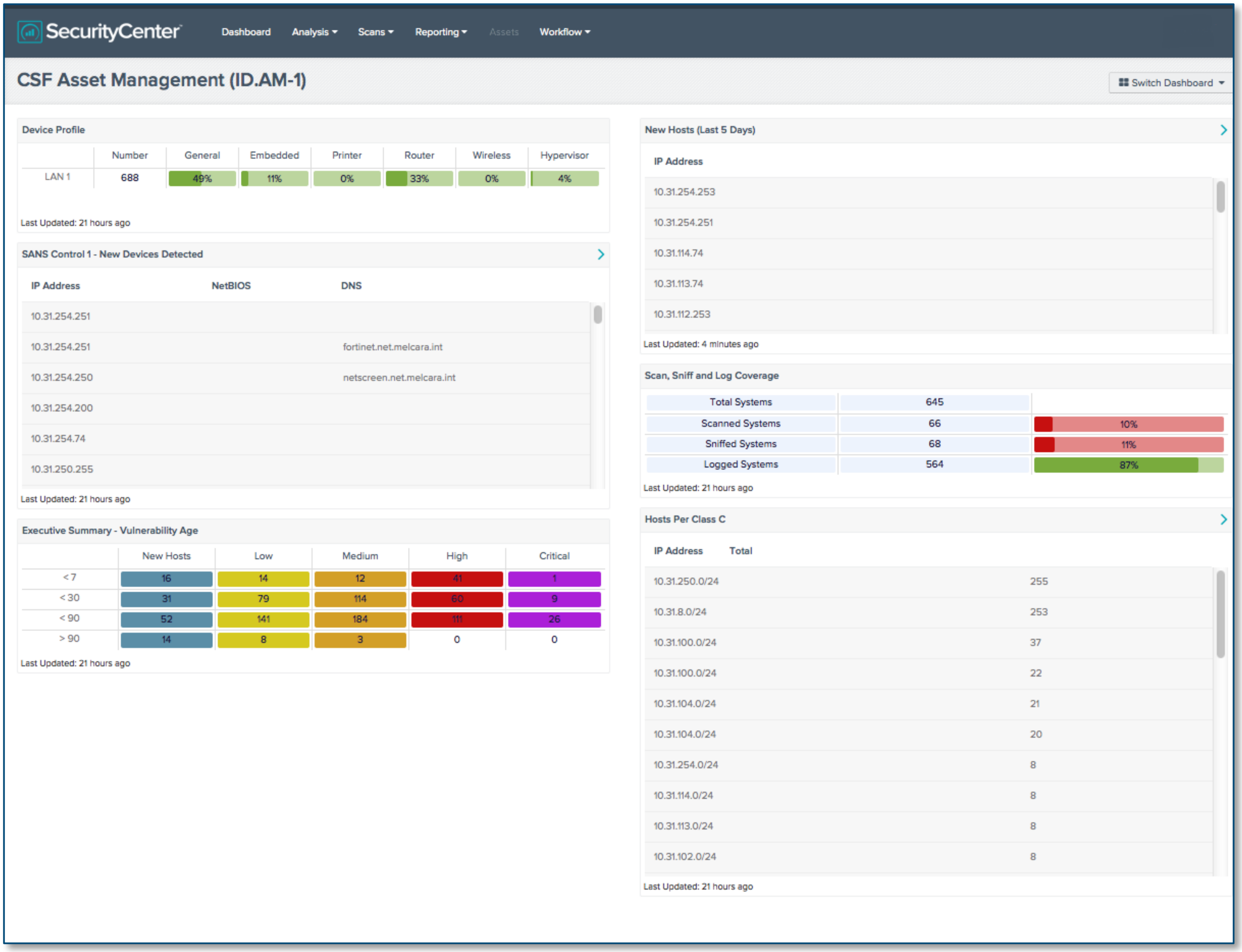
Event log analysis is the third technique for identifying assets on the network. It can detect systems on network segments that are neither passively monitored nor actively scanned. Log events generated by firewalls, switches and routers will capture the IP addresses of all assets on the network that send and/or receive traffic that reaches the devices. The advantage of event log analysis is that typically the logs are already being generated, so asset identification is as simple as extracting the pertinent information from the log stream. The challenge of using event logs to identify network assets is that it is like looking for a few needles in the proverbial haystack. Fortunately, log correlation rules can automate this process.

The Continuous Asset Visibility Solution

The primary benefit of continuous network monitoring is the elimination of unacceptable risk created by unknown, and therefore likely unmanaged, network assets. Multiple techniques: passive network monitoring, active scanning and event log analysis, are required to detect virtually all assets. However, it is not efficient to have different, unreconciled asset inventories from three different tools because extracting actionable information would be difficult and expensive.

A continuous asset discovery solution must deduplicate assets detected by different tools, highlight new assets on the network and provide a preliminary risk assessment, such as the number of known vulnerabilities, for each asset so risk-based corrective action can be taken. The dashboard below shows this information in a format consistent with NIST's Cybersecurity Framework[5]. It delineates assets discovered with passive network monitoring (sniffed systems), active scanning (scanned systems) and log event analysis (logged systems). It also shows vulnerability by age to help prioritize risk-based remediation.

[5] Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, February 12, 2014



CSF Asset Management (ID.AM-1)

Device Profile

	Number	General	Embedded	Printer	Router	Wireless	Hypervisor
LAN 1	688	49%	11%	0%	33%	0%	4%

Last Updated: 21 hours ago

SANS Control 1 - New Devices Detected

IP Address	NetBIOS	DNS
10.31.254.251		
10.31.254.251		fortinet.net.melcara.int
10.31.254.250		netscreen.net.melcara.int
10.31.254.200		
10.31.254.74		
10.31.250.255		

Last Updated: 21 hours ago

Executive Summary - Vulnerability Age

	New Hosts	Low	Medium	High	Critical
< 7	16	14	12	41	1
< 30	31	79	114	60	9
< 90	52	141	184	111	26
> 90	14	8	3	0	0

Last Updated: 21 hours ago

New Hosts (Last 5 Days)

IP Address
10.31.254.253
10.31.254.251
10.31.114.74
10.31.113.74
10.31.112.253

Last Updated: 4 minutes ago

Scan, Sniff and Log Coverage

Total Systems	645	
Scanned Systems	66	10%
Sniffed Systems	68	11%
Logged Systems	564	87%

Last Updated: 21 hours ago

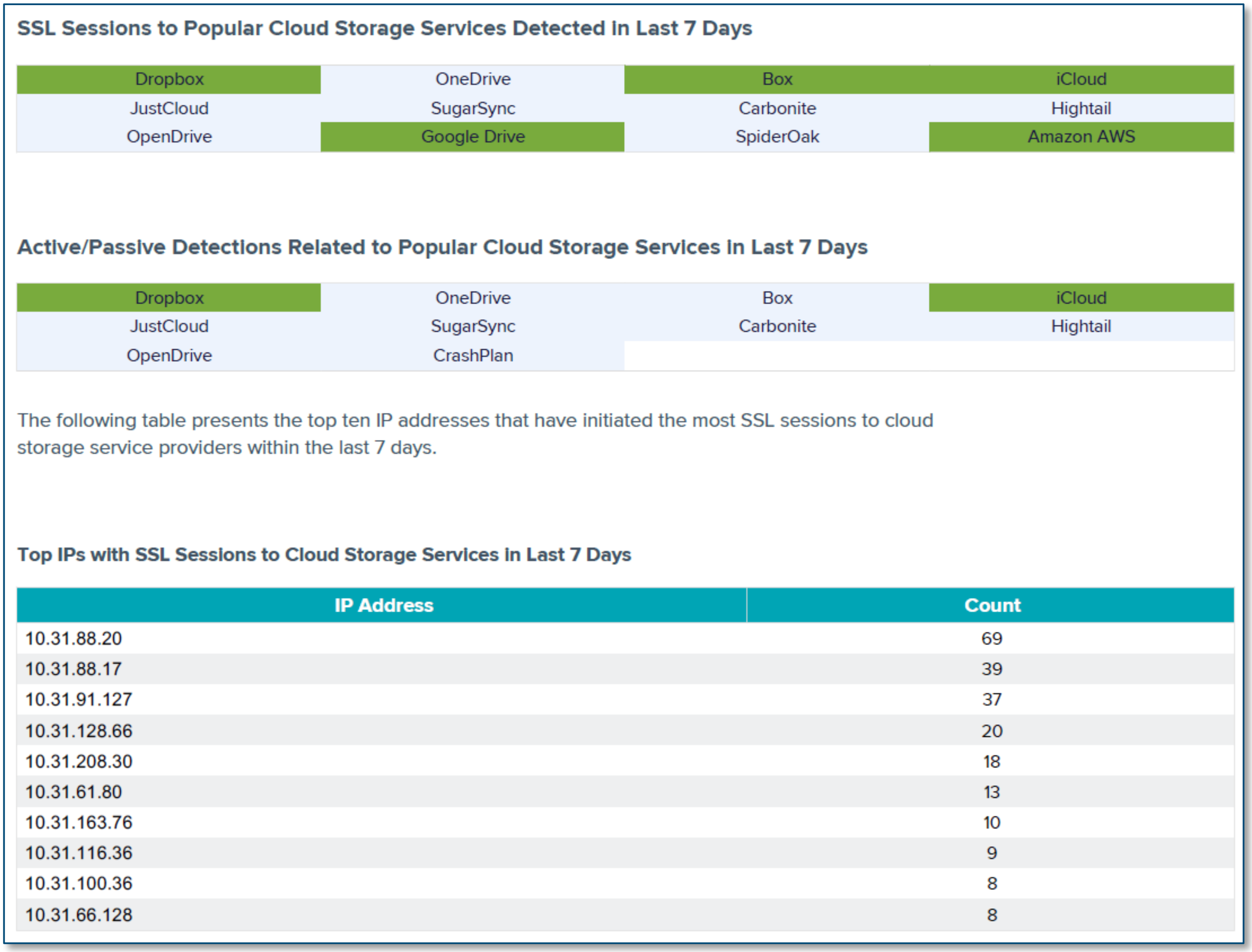
Hosts Per Class C

IP Address	Total
10.31.250.0/24	255
10.31.8.0/24	253
10.31.100.0/24	37
10.31.100.0/24	22
10.31.104.0/24	21
10.31.104.0/24	20
10.31.254.0/24	8
10.31.114.0/24	8
10.31.113.0/24	8
10.31.102.0/24	8

Last Updated: 21 hours ago

Figure 3. Critical Security Framework – Asset Management

Assets, such as laptops, tablets, smartphones and network devices which are on the network are important, but enterprise data is arguably even more important. As discussed above, data stored in potentially insecure "shadow IT" locations introduce data security, compliance and legal risk. A continuous asset discovery solution should provide visibility of which devices behind the firewall are communicating with potentially risky cloud storage services. Figure 4 is part of a report that shows which IP addresses have interacted with popular cloud storage services, such as Dropbox, in the past seven days.



SSL Sessions to Popular Cloud Storage Services Detected in Last 7 Days

Dropbox	OneDrive	Box	iCloud
JustCloud	SugarSync	Carbonite	Hightail
OpenDrive	Google Drive	SpiderOak	Amazon AWS

Active/Passive Detections Related to Popular Cloud Storage Services in Last 7 Days

Dropbox	OneDrive	Box	iCloud
JustCloud	SugarSync	Carbonite	Hightail
OpenDrive	CrashPlan		

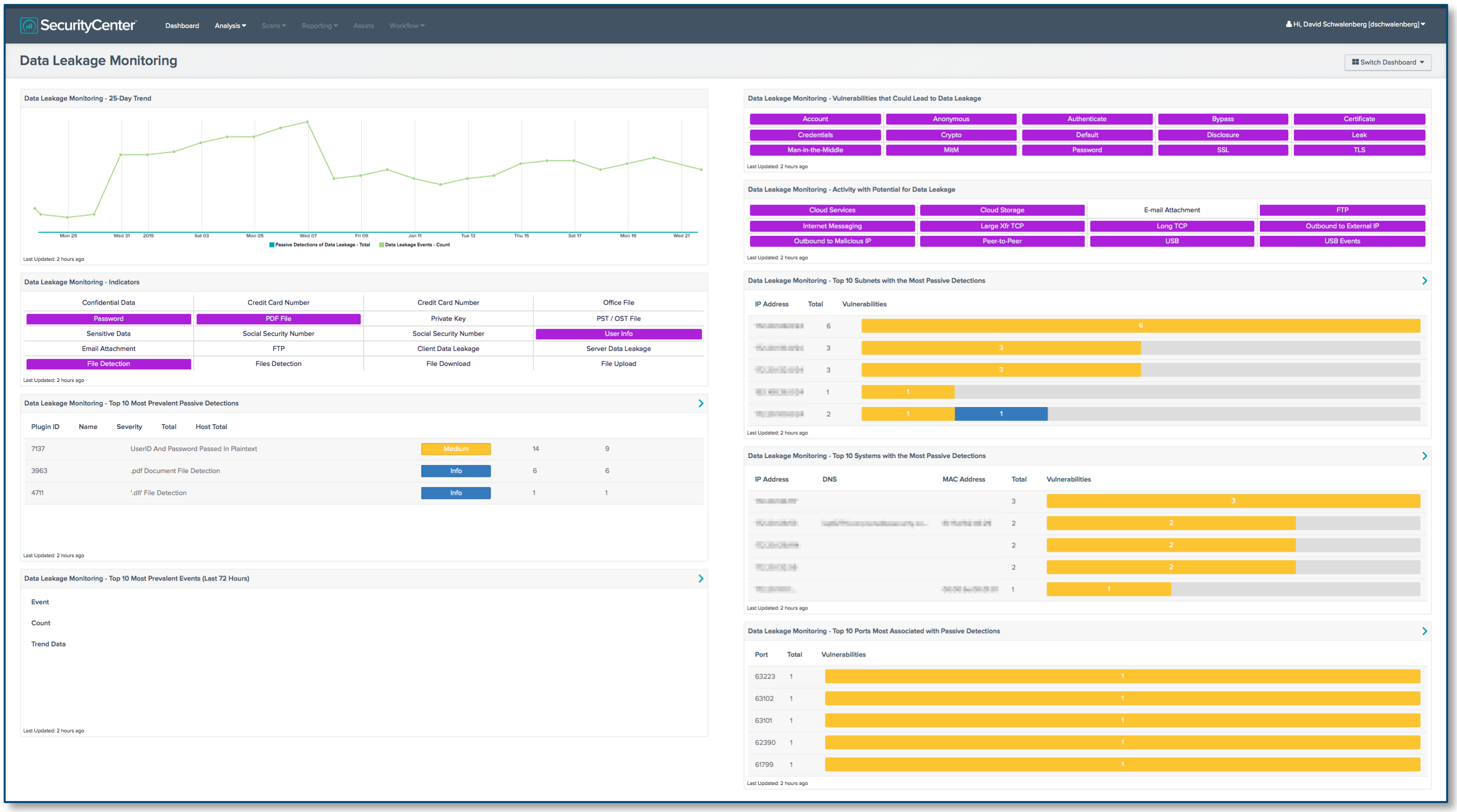
The following table presents the top ten IP addresses that have initiated the most SSL sessions to cloud storage service providers within the last 7 days.

Top IPs with SSL Sessions to Cloud Storage Services in Last 7 Days

IP Address	Count
10.31.88.20	69
10.31.88.17	39
10.31.91.127	37
10.31.128.66	20
10.31.208.30	18
10.31.61.80	13
10.31.163.76	10
10.31.116.36	9
10.31.100.36	8
10.31.66.128	8

Figure 4. Recent Cloud Storage Use

Knowing which devices (IP addresses) have been using popular cloud storage services is very useful. However, also having visibility into unencrypted protected/proprietary content being stored on devices and being transferred to or from the cloud, plus having visibility into the devices' vulnerabilities, provides much more insight into risk. The data leakage dashboard shown in Figure 5 provides insight into all three indicators of protected/proprietary data loss risk; presence of protected/proprietary data, vulnerabilities and activities such as usage of cloud storage.



Data Leakage Monitoring

Data Leakage Monitoring - 25-Day Trend

Last Updated: 2 hours ago

Data Leakage Monitoring - Indicators

Confidential Data	Credit Card Number	Credit Card Number	Office File
Password	PDF File	Private Key	PST / OST File
Sensitive Data	Social Security Number	Social Security Number	User Info
Email Attachment	FTP	Client Data Leakage	Server Data Leakage
File Detection	Files Detection	File Download	File Upload

Last Updated: 2 hours ago

Data Leakage Monitoring - Top 10 Most Prevalent Passive Detections

Plugin ID	Name	Severity	Total	Host Total
7137	UserID And Password Passed In Plaintext	Medium	14	9
3963	.pdf Document File Detection	Info	6	6
4711	'.dll' File Detection	Info	1	1

Last Updated: 2 hours ago

Data Leakage Monitoring - Top 10 Most Prevalent Events (Last 72 Hours)

Event

Count

Trend Data

Last Updated: 2 hours ago

Data Leakage Monitoring - Vulnerabilities that Could Lead to Data Leakage

Account	Anonymous	Authenticate	Bypass	Certificate
Credentials	Crypto	Default	Disclosure	Leak
Man-in-the-Middle	MitM	Password	SSL	TLS

Last Updated: 2 hours ago

Data Leakage Monitoring - Activity with Potential for Data Leakage

Cloud Services	Cloud Storage	E-mail Attachment	FTP
Internet Messaging	Large Xfr TCP	Long TCP	Outbound to External IP
Outbound to Malicious IP	Peer-to-Peer	USB	USB Events

Last Updated: 2 hours ago

Data Leakage Monitoring - Top 10 Subnets with the Most Passive Detections

IP Address	Total	Vulnerabilities
[redacted]	6	6
[redacted]	3	3
[redacted]	3	3
[redacted]	1	1
[redacted]	2	1 1

Last Updated: 2 hours ago

Data Leakage Monitoring - Top 10 Systems with the Most Passive Detections

IP Address	DNS	MAC Address	Total	Vulnerabilities
[redacted]			3	3
[redacted]	[redacted]	[redacted]	2	2
[redacted]			2	2
[redacted]			2	2
[redacted]		[redacted]	1	1

Last Updated: 2 hours ago

Data Leakage Monitoring - Top 10 Ports Most Associated with Passive Detections

Port	Total	Vulnerabilities
63223	1	1
63102	1	1
63101	1	1
62390	1	1
61799	1	1

Last Updated: 2 hours ago

Figure 5. Indicators of Protected/Proprietary Data Risk

Tenable's SecurityCenter Continuous View™

Tenable Network Security's SecurityCenter Continuous View (CV) is the market leading continuous network monitoring platform that, in addition to delivering continuous asset visibility, enables organizations to continuously identify all known vulnerabilities, continuously monitor networks for advanced threats, and gather contextual analytics to rapidly respond to security breaches. SecurityCenter CV incorporates passive network monitoring, active scanning and log analysis to eliminate blind spots caused by the ever-changing IT landscape.

Conclusion

Without accurate and up-to-date visibility of all network assets, a risk manager or security professional cannot possibly answer the questions, "What is our risk?" and "Are we secure?" The rapidly changing IT landscape with BYOD, shadow IT and mobile/guest workers is making it nearly impossible for security organizations to ensure that the network, related devices and protected/proprietary data are identified and secure.

Continuous asset discovery shines the light on the previously unseen wireless access points, laptops, tablets, mobile phones and virtual machines that, if left undetected, could easily expose networks to malware and data exfiltration. It relies on passive network monitoring, active network scanning and event log analysis to perform three real-time functions; asset detection, identification and risk triage.

Continuous asset discovery gives risk and security management insight into their network so they can direct security and operations staff to take the corrective action needed to reduce risk to meet the expectations of executive management.

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, please visit tenable.com.