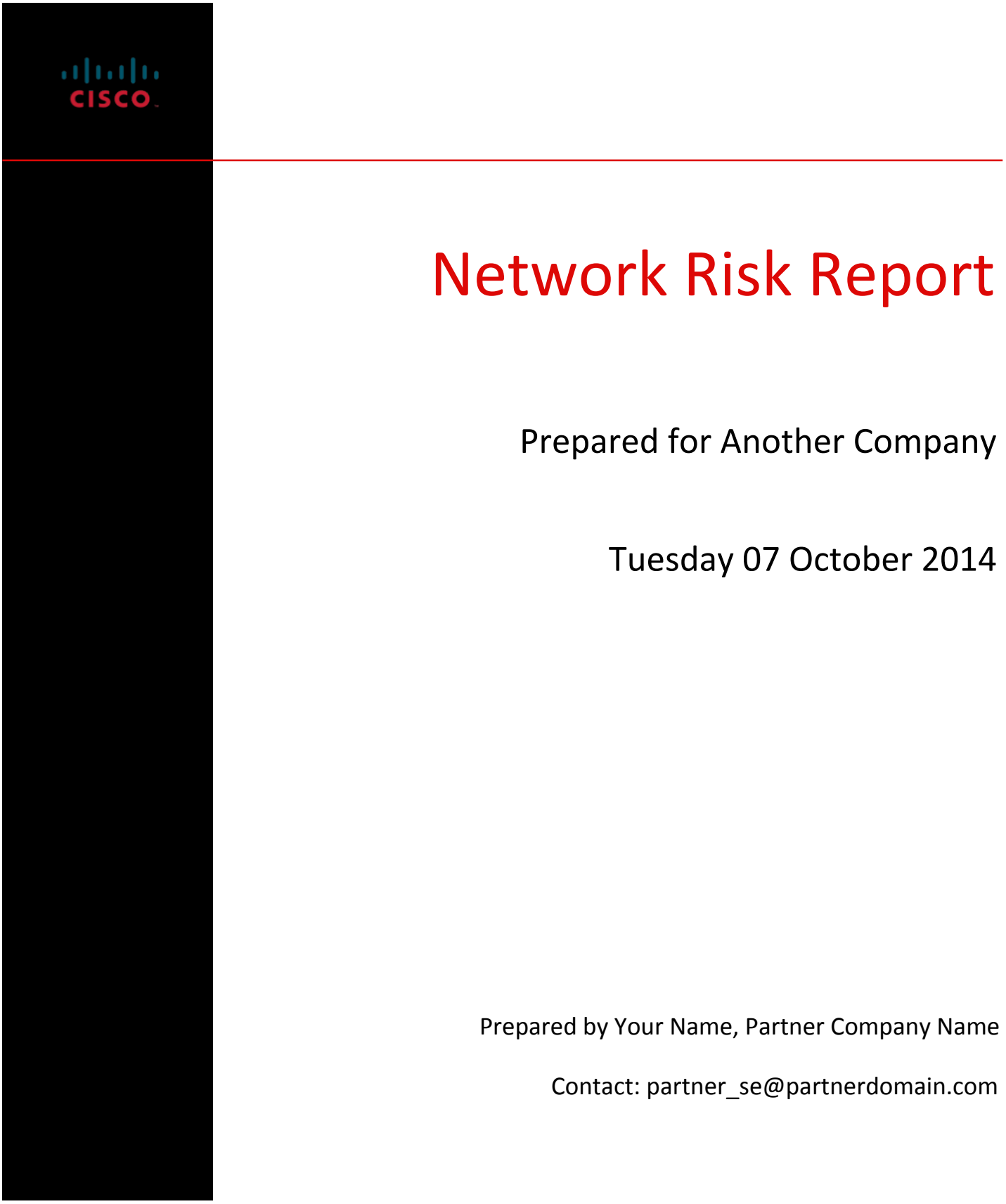


Network Risk Report

Prepared for Another Company

Tuesday 07 October 2014

Prepared by Your Name, Partner Company Name

Contact: partner_se@partnerdomain.com

I. EXECUTIVE SUMMARY

Cisco has determined that Another Company is at a High risk due to the use of applications that are potentially dangerous to the enterprise yet have low business relevance. These applications may leave your network vulnerable to attack, carry malware, or waste bandwidth.

Assessment Period: Wed Jul 9 09:34:36 2014 to Tue Oct 7 09:34:36 2014

Risky Apps	Risky Users	High Bandwidth Apps
11	*	24

* AD Integration disabled

Encrypted Apps	Evasive Apps	Dangerous Web Browsers
46	8	1

(A summary of the assessment results starts on page 3)

YOUR NETWORK PROFILE

14	0	515	14
Operating Systems	Mobile Devices	Applications In Use	File types transferred

RECOMMENDATIONS

Cisco recommends Another Company deploy Cisco FirePOWER Appliances (NGIPS/NGFW) with App Control and URL Filtering to:

1. Reduce your application attack surface
2. Granularly control applications, bandwidth, URL access and acceptable use policies
3. Get visibility into network risks and usage, including mobile devices and BYOD risk

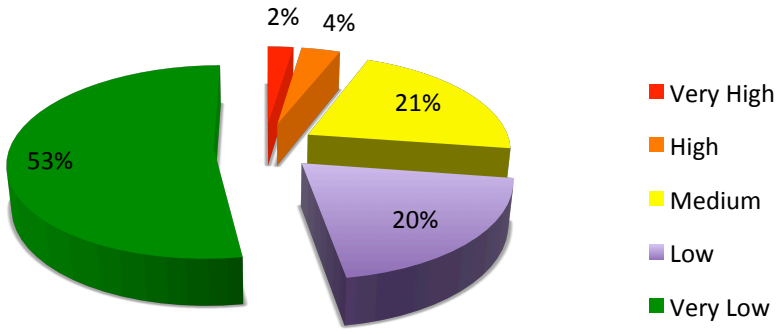
II. APPLICATION RISK

APPLICATIONS WITH HIGH RISK AND LOW BUSINESS RELEVANCE

Some applications carry high risk because they can be vectors for malware into the organization, possess recent vulnerabilities, use substantial network resources, or hide the activities of attackers. Other applications have low business relevance: they are not relevant to the activities of a typical organization. When an application has high risk and low business relevance, it is a good candidate for application control to reduce your application risk. You should investigate these applications to determine whether they are important to control.

APPLICATION	TIMES ACCESSED	APPLICATION RISK	PRODUCTIVITY RATING	DATA TRANSFERRED (MBYTES)
MySpace	9	Very High	Very Low	0.04
Facebook	24,818	Very High	Low	153.24
YouTube	4,393	High	Very Low	4,046.35
The Independent	700	High	Very Low	15.27
				0.00

SUMMARY OF ALL NETWORK CONNECTIONS BY APPLICATION RISK



HIGH BANDWIDTH APPLICATIONS

Some applications use a substantial amount of network bandwidth. This bandwidth usage can be costly to your organization and can negatively impact overall network performance. You may want to restrict the usage of these applications to particular networks: for instance, a wireless network may not be well suited for video streaming. Or, you can shut down these applications entirely or simply get visibility into how your bandwidth is being used.

APPLICATION	TIMES ACCESSED	APPLICATION RISK	PRODUCTIVITY RATING	DATA TRANSFERRED (MBYTES)
Netflix stream	2,690	Very Low	Very Low	53,529.34
Steam browser	2,436	Very Low	Very Low	14,181.55
YouTube	4,393	High	Very Low	4,046.35
Netflix	4,584	Medium	Very Low	253.23
Ubuntu Update Manager	41	Medium	Low	143.98

ENCRYPTED APPLICATIONS

Some applications encrypt data they process, causing security administrators to be blind to attacks and usage patterns. With SSL decryption, administrators can look inside these applications and observe their use. An SSL decryption appliance, such as a Cisco SSL Appliance, can decrypt SSL traffic inbound and outbound: inbound by storing the certificates of private web servers, and outbound by acting as an intermediary in browsers' connections to the Internet. It is important to use SSL decryption to obtain visibility into encrypted applications to help mitigate this potential attack vector.

APPLICATION	TIMES ACCESSED	APPLICATION RISK	PRODUCTIVITY RATING	DATA TRANSFERRED (MBYTES)
Facebook	24,818	Very High	Low	153.24
Akamai	10,082	Very Low	Low	8,482.89
SSH	5,833	High	Medium	77.66
Gmail	4,626	Low	Medium	19.80
SFTP	2,398	Medium	Medium	56.71

EVASIVE APPLICATIONS

Evasive applications try to bypass your security by tunneling over common ports and trying multiple communication methods. Only solutions that reliably identify applications are effective at blocking evasive applications. You should evaluate the risks of these applications and see if they are good candidates for blocking.

APPLICATION	TIMES ACCESSED	APPLICATION RISK	PRODUCTIVITY RATING	DATA TRANSFERRED (MBYTES)
Skype	10	Very High	Medium	0.02
SSL client	173,346	Medium	Medium	968.20
cURL	10	Medium	Medium	1.08
TURN Channel	3	Medium	Very High	0.00

OTHER APPLICATIONS OF INTEREST

Other applications were observed that may be of interest and possibly candidates for control. Users may use anonymizers and proxies to bypass your network security or cloak their identities. Gaming applications may be distractions to productivity and use excessive bandwidth. Peer-to peer applications are often malware vectors. And remote administration applications may allow malicious users to control machines in your environment.

Anonymizers and Proxies (accesses):

Tor(263) , Freenet(123) , Squid(23)

Games and Recreation (accesses):

Facebook(2097) , Google+(206), Twitter(195), Scorecard Research(156), LinkedIn(80), Game Center(76), LinkedIn(80), Game Center(76),

Peer-to-Peer and Sharing (accesses):

MSN(134), Windows Live(67), Pinterest(61), Photo Stream(31), Google Talk Gadget(17), Vimeo(10), Instagram(10), Vimeo(10),

Remote Administration and Storage (accesses):

HTTPS(730) , HTTP(730) , iCloud(470) , SSH(180) , WebEx(74) , Windows Live SkyDrive(66) , Wordpress(60) , Wordpress(60) ,

DANGEROUS WEB BROWSER VERSIONS

A profile of your network revealed the following old web browsers in use. Outdated web browsers are a major vector for network malware and it is important to update them (or encourage users to). These browsers often have unpatched vulnerabilities or carry other risks.

BROWSER	VERSION	NUMBER OF HOSTS
Internet Explorer	6	1
Chrome		0
Safari		0
Firefox		0

RISKY WEB BROWSING

The following web communications were identified that correspond to risky activity. Malware sites, open proxies and anonymizers, keyloggers, phishing sites, and spam sources are all Web activities that can put your networks at risk. It is wise to evaluate the use of URL filtering technologies to detect and control communications to risky sites.

URL CATEGORY	CONNECTIONS	BLOCKED	DATA INBOUND (BYTES)	DATA OUTBOUND (BYTES)
Spyware and Adware	247		385,297	834,328
Proxy Avoid and Anonymizers	6		2,800,397	62,111
Phishing and Other Frauds	5		94,924	7,165
Malware Sites	231		3,614,337	985,750
Social Network	27,496		158,553,198	52,942,788

THE APPLICATIONS ON YOUR NETWORK

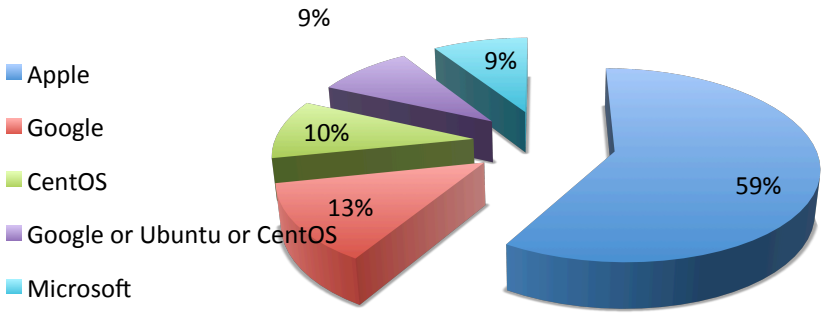
This is a list of the top applications discovered in use on your network. Three types of applications are identified and listed here: client applications (including web browsers), web applications (which run over HTTP), and server applications (for example, web servers). Full visibility over all application types enables you to get better perspective on how your networks are currently utilized.

CLIENT APPLICATIONS	WEB APPLICATIONS	SERVER APPLICATIONS
Client applications include web browsers and other desktop applications that access the network	Web applications are carried over Web-related protocols like HTTP and HTTPS. Many Web applications operate on port 80.	Server applications include web servers such as IIS and Apache
Total: 131	**Total: 387**	**Total: 38**
whois client, UPnP, Facebook, Skype…	WebSocket, SurveyMonkey, Facebook, WebDAV…	TFTP, whois, Jabber, SSH…

III. ASSET PROFILE

THE OPERATING SYSTEMS ON YOUR NETWORK

The operating systems below were observed on your network. You should identify any operating systems that fall outside your IT policy and investigate them further as to whether they should be permitted.



THE MOBILE DEVICES ON YOUR NETWORK

The following mobile devices were profiled on your network. Mobile devices may be vulnerable, especially older or jailbroken versions. It is important to be aware of how mobile devices are used and set appropriate security policies.

DEVICE TYPE	VERSION	COUNT

THE FILES TRAVERSING YOUR NETWORK

	FILE CATEGORY	FILE TYPE	COUNT	PROTOCOL
DOWNLOADS	Archive	BZ	11,872	HTTP
	Archive	GZ	3,519	HTTP
	Multimedia	SWF	1,603	HTTP
	Archive	ZIP	1,096	HTTP
	Archive	JAR	633	HTTP
UPLOADS	System files	DMP	38	HTTP
MISC				

IV. RECOMMENDATIONS

Despite existing protections, your organization's application usage exposes it to added risks. This assessment, which contains a profile of your network, has identified risky assets. New countermeasures and security controls are required to mitigate the risks to these assets.

Cisco recommends that FirePOWER Appliances with Application Control and URL Filtering are depoyed to:

1) Establish continuous network visibility into its application and asset risk.
2) Augment its existing controls in order to mitigate this risk

1) ESTABLISH CONTINUOUS NETWORK VISIBILITY INTO APPLICATION RISK

Existing security infrastructure provides inadequate protection against application and asset risks. Cisco recommends deployment of network-based protections via FirePOWER Appliances (NGIPS/ NGFW). These will provide the following new capabilities and benefits to augment your network visibility:

NEW CAPABILITY	BENEFIT
Network Map	Profiles hosts on the network, including network infrastructure, desktops, servers, mobile devices, virtual machines, and many others.
Application Awareness	Identifies over 1,500 applications, including client applications that run on desktops, server applications such as Web servers, and Web applications carried over HTTP. Profiles application actions, like the ability to send email or chat using a Web mail application.
Mobile Awareness	identifies and profiles mobile devices, including iOS, Android, Amazon, Blackberry, and other mobile device types. Identifies jailbroken devices.
Real-time Contextual Awareness	Profiles hosts and identifies communications that are of unusual bandwidth or hosts that are running inappropriate applications for the environment.

2) AUGMENT CONTROLS TO MITIGATE RISK

Deploying additional countermeasures can help mitigate the risk applications pose. These measures may entail reduction of the application threat surface and blocking risky URLs. Cisco recommends deployment of network-based protections via FirePOWER Appliances with Application Control and URL Filtering. These provide the following new capabilities and benefits:

NEW CAPABILITY	BENEFIT
Granular Application Control	Reduce potential area of attack through granular control of thousands of applications. Filter and enforce usage policy on millions of URLs.
URL Filtering	Control on a database of millions of URLs, by risk or productivity characteristics
Virtual Protection	Protect VM-to-VM communications the same as physical network

In addition, Cisco offers NGIPS capabilities and optional Advanced Malware Protection for networks and hosts, to help better protect against the latest threats. Please contact your Cisco representative or reseller for more information.

ABOUT CISCO

It's no secret that today's advanced attackers have the resources, expertise, and persistence to compromise any organization at any time. As attacks become more sophisticated and exploit a growing set of attack vectors, traditional defenses are no longer effective.

It's more imperative than ever to find the right threat-centric security products, services, and solutions for your current environment. These solutions must also easily adapt to meet the evolving needs of your extended network, which now goes beyond the perimeter to include endpoints, mobile devices, virtual machines, data centers, and the cloud.

For nearly three decades, Cisco has been a leader in network security protection, innovation, and investment. Our expertise and experience helps us increase intelligence and expand threat protection across the entire attack continuum for a level of security you can build your business on.

Cisco delivers intelligent cybersecurity for the real world.

CONTACT US

Want to learn more about getting this information on your network? Go to http://cisco.com/go/security and request a live demo.