



CHECK POINT 3D SECURITY ANALYSIS REPORT

Prepared for:



COMPANY LTD.

Company Name:	COMPANY
Prepared by:	Check Point Solution Center
Date:	May 14, 2012
Document Version:	Ver2

Table of Contents

Table of Contents.....	2
Introduction	3
Web Security Events.....	4
Intrusions & Attacks Events	7
Data Loss Events.....	9
Bots & Viruses Events.....	11
Bandwidth Analysis	15
Remediation Recommendations	20
3D Security Report Analysis Summary	24
Introducing Check Point 3D Security.....	24
About Check Point Software Technologies	26

Introduction

This document provides the findings of a recent 3D Security Analysis of your infrastructure. The document represents a summary of these findings and presents a set of [recommendations](#) for addressing the discovered events.

The analysis is based on data collected using the characteristics below:

3D Security Analysis Date:	18/04/2012
In-Network Analysis Duration:	5 hours
Monitored Network:	Internal network facing the internet
Deployment type:	Check Point 4800 Appliance
Release version:	R75.40
Security Gateway Software Blades:	Identity Awareness, Application Control, URL Filtering, IPS, Data Loss Prevention, Anti-Virus and Anti-Bot
Security Management Software Blades:	Pre-Defined 7 Blades with SmartEvent

The following is a summary of the main high and critical risk security events detected:



8 High Risk Applications Events



288 Intrusions & Attacks Events



103 Data Loss Events



42 Bots & Viruses Events

Web Security Events

Top High Risk Applications & Sites

Within the areas of Application Control and URL Filtering, the following items are of the highest risk level (the *first* column specifies the number of events related to the mentioned application/site):

Count	Application / Site	Matched Category	App. Risk	User	Total Bytes
2	 Sopcast	P2P File Sharing	5 Critical	2 Users	431 KB
9	 LogMeIn	Remote Administration	4 High	9 Users	1.67 MB
15	 VNC	Remote Administration	4 High	15 Users	428.72 MB
5	 uTorrent	P2P File Sharing	4 High	5 Users	363 KB
9	 TeamViewer	Remote Administration	4 High	9 Users	620 KB
3	 YouSendIt	File Storage and Sharing	4 High	3 Users	4.32 MB
7	 Windows Live Office	File Storage and Sharing	4 High	7 Users	567 KB
70	 Dropbox	File Storage and Sharing	4 High	70 Users	194.45 MB
29	 RDP	Remote Administration	4 High	29 users	232.87 MB
4	 Windows Live Mesh	P2P File Sharing	4 High	4 Users	425 KB
15	 Sugarsync	File Storage and Sharing	4 High	15 Users	71.01 MB
1	 Netload	File Storage and Sharing	4 High	Joe Roberts	393 KB
1	 SoulSeek	P2P File Sharing	4 High	Erica Eyelash	56 KB
1	 Gigaup	File Storage and Sharing	4 High	Irena White	52 KB
2	 BitTorrent Protocol	P2P File Sharing	4 High	2 Users	177 KB
1	 SimpleHelp	Remote Administration	4 High	Chelsea Cash	183 KB
2	 Vuze	P2P File Sharing	4 High	2 Users	2 KB
1	 Curl	File Storage and Sharing	4 High	Danise Dash	2 KB
2	 Free Download Manager	Download Manager	4 High	2 Users	55 KB
1	 digsby	Instant Messaging	4 High	Joe Roberts	21 KB
1	 Sendspace	File Storage and Sharing	4 High	Peter Smith	4.07 MB

Top High Risk Applications Description

The following tables provide summary explanations of the top events found and their associated security or business risks:

Application and Description	Events
<p>Sopcast</p> <p>Sopcast is a media streaming application which allows media streaming via P2P networks. Sopcast allows users to broadcast media to other users or watchstreams broadcasted by other users.</p>	2
<p>Dropbox</p> <p>Dropbox is an application that allows the user to share files.</p>	70
<p>Sugarsync</p> <p>SugarSync provides online backup, syncing, and sharing files from the user's PC and mobile devices.</p>	15
<p>uTorrent</p> <p>uTorrent is a freeware closed source BitTorrent client that is designed to use minimal computer resources while offering functionality comparable to larger BitTorrent clients such as Vuze or BitComet. Torrent's development had started in 2005 by Ludvig Strigeus ,a Swedish programmer, and since 2006 the code has been owned and maintained by</p>	5
<p>Vuze</p> <p>Vuze (formerly Azureus) is a Java-based BitTorrent client that is used to transfer files via the BitTorrent protocol. The software provides users the ability to view, publish and share original DVD and HD quality video content as well. Vuze was released under the GNU General Public License.</p>	2

Top Users of High Risk Applications

The following users were involved in the highest number of risky application and web usage events:

Users*	Events
Irma Whitewash	23
Ingrid Whitewash	21
Zachary Zest	16
Leif Lash	11
Ella Eyelash	9
Carlos Cash	5
Hope Hash	2
Evan Eyelash	1
Joe Roberts	1

***Note:** User names will be displayed in the above table only when Check Point Identity Awareness Software Blade is enabled and configured.



Intrusions & Attacks Events

Top Intrusions & Attacks Events

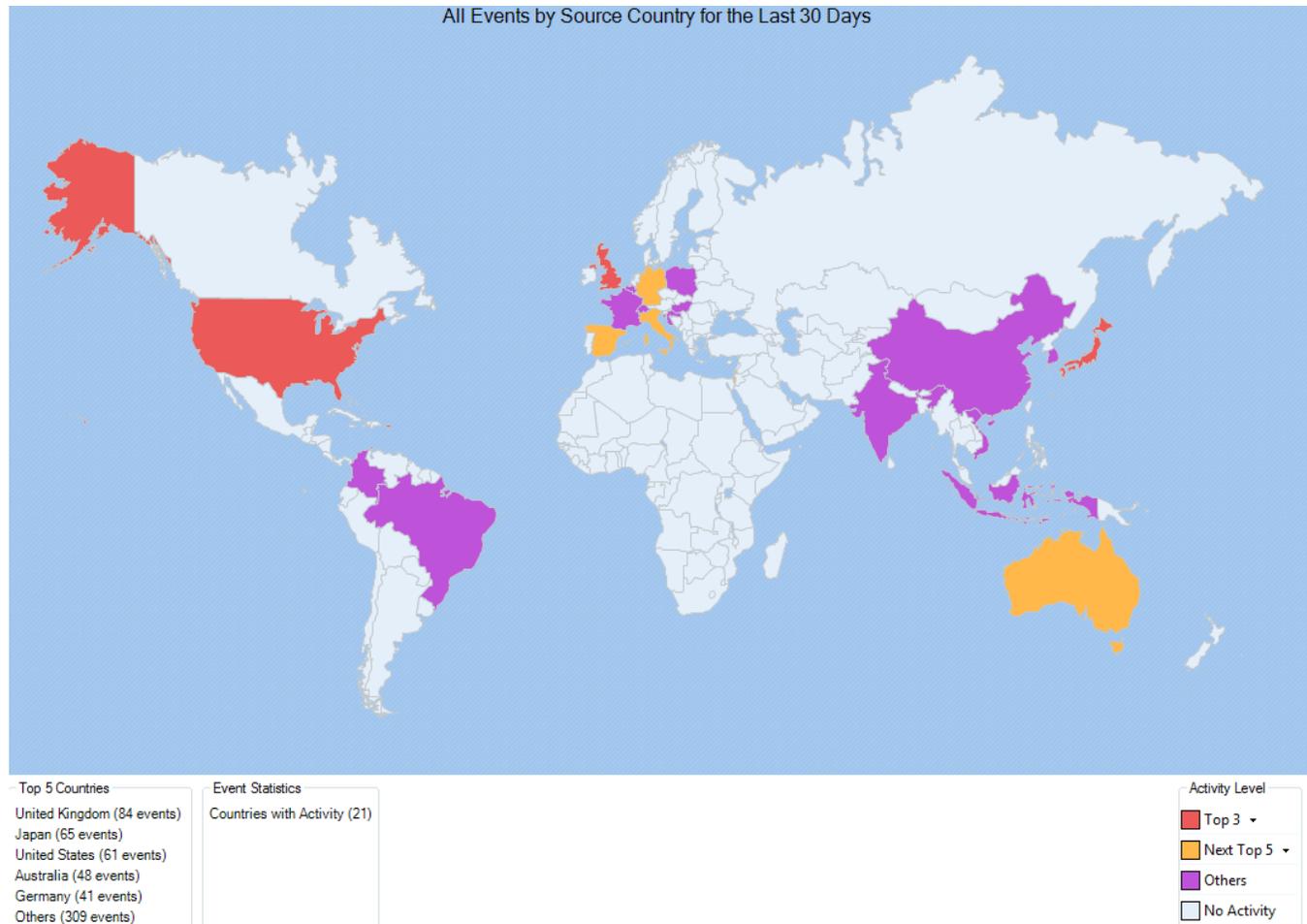
During the 3D Security Analysis, the Check Point solution identified a number of intrusion prevention-related events. Some of these events were categorized as critical. The following chart shows the distribution of events according to severity:

Severity	Event Name	CVE*	Events
Critical			
	Microsoft Windows Remote Desktop protocol code execution (MS12-020)	CVE-2012-0002	12
	Adobe Flash Player URL security domain checking code execution (APSB12-07)	CVE-2012-0772	11
High			
	Microsoft DNS server denial of service (MS12-017)	CVE-2012-0006	23
Medium			
	Interactive Data eSignal stack buffer overflow	CVE-2011-3494	4
Total			50

*CVE (Common Vulnerabilities and Exposures) is a dictionary for publicly known security vulnerabilities. To find more information about specific IPS event, search the CVE ID using [National Vulnerability Database CVE search web page](#).

IPS Events by Country

The following map shows the distribution of IPS events according to their origin countries. To mitigate attacks based on source or destination countries, create a policy using Check Point IPS Geo-protection feature.





Data Loss Events

Your company data is one of the the most valuable assets to your organization. Any intentional or unintentional loss can cause damage to your organization. The following represents the characteristics of the data loss events that were identified during the course of the anlysis.

Top Data Loss Events

The following list summarizes the identified data loss activity and the number of times that the specific type of events occurred for different data types configured for the DLP Software Blade.

Severity	Data	Events
Critical		
	Data containing credit card numbers was sent outside the organization (PCI compliance violation).	17
High		
	Data containing programming language lines (Source Code), such as C, C++, C#, JAVA and more, was sent outside the organization. Indicates leaks of intellectual property.	14
	Pay slip file was sent outside the organization.	16
	International Bank Account Number – IBAN was sent outside the organization.	61
	Data containing Mergers and Acquisitions (M&A) plans was sent outside the organization (e.g. corporate strategy, corporate finance and more)	2
Medium		
	Email sent to several internal recipients and a single external one. Such emails are usually being sent unintentionally to a wrong external recipient	18
Total		128

Top Data Loss Events by Mail Sender

This chart shows data leakage by mail sender on your network.

Sender	Events
giovannicash@myBiz.com	5
jezebeljosh@myBiz.com	5
dantedash@myBiz.com	5
daphnedash@myBiz.com	4
johnjosh@myBiz.com	4
ericaeyelash@myBiz.com	4
javonjosh@myBiz.com	4
artash@myBiz.com	4
hernandohash@myBiz.com	4



Bots & Viruses Events

A bot is malicious software that invades your computer. Bots allow criminals to remotely control your computer to execute illegal activities such as stealing data, spreading spam, distributing malware or participating in Denial of Service attacks, without your knowledge. Bots are often used as tools in targeted attacks known as Advanced Persistent Threats or APTs. A botnet is a collection of such compromised computers.

High and Critical Bots & Viruses Events Summary

The following table summarizes the total number of infected hosts involved in malicious activity and the number of Malware found (Bots and Viruses).

Description	Findings
Hosts Infected with Bots	5
Hosts Downloaded a Malware	4
Hosts Accessed a Site/Host Known to Contain Malware	3
Different types of High and Critical Malware Found	7

Traffic Sent and Received by Bots and Viruses

The following amount of traffic was sent and received as a result of Bots and Viruses activity. This traffic might indicate illegal activities executed remotely such as stealing data, spreading spam, distributing malware and participate in Denial of Service (DOS).



0.9 MB
Total Sent



6.5 MB
Total Received

Top Bots & Viruses Events

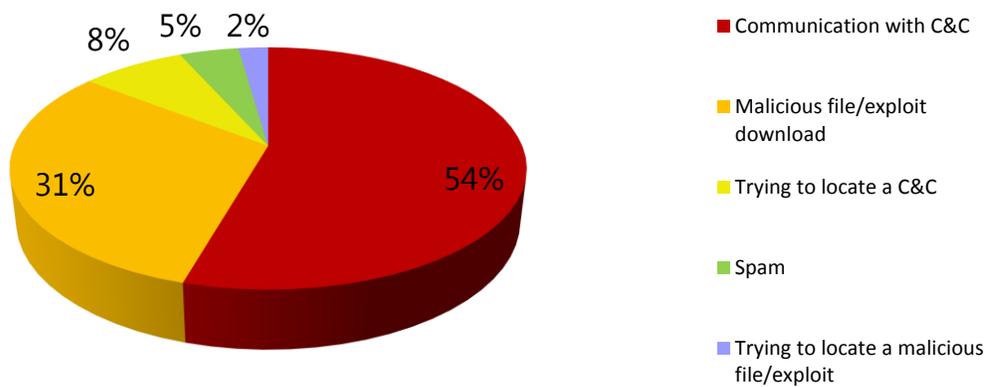
During the 3D Security Analysis, the Check Point solution identified a number of Malware-related events. The following table summarizes the top bots and viruses detected in your environment.

Severity	Bot/Virus Name	Events
Critical		
	Backdoor.IRC.Zapchast.zwrc	8
	Backdoor.Win32.Gbot.pzh	5
	P2P-Worm.Win32.Palevo.agth	8
High		
	Backdoor.Win32.Hupigon.ozqk	6
	Trojan-Downloader.JS.Expack.bn	1
	Worm.Win32.AutoRun.duv	5
Medium		
	Email-Worm.Win32.Bagle.pac	7
	Trojan-Downloader.JS.Agent.gco	25
	Trojan-Downloader.Win32.Pendix.d	24
	Worm.BAT.Autorun.gr	2
Total		91

More details about malware identified in this report can be found by searching Check Point ThreatWiki, Check Point's public Malware Database at threatwiki.checkpoint.com

Bots & Viruses Activity

The following chart shows the distribution of detected Malware activity according to their infected hosts. Bots usually communicate with Command and Control (C&C) which is the bot's remote operator server used to send data outside of the organization.



Top Hosts Involved in Malicious Activity

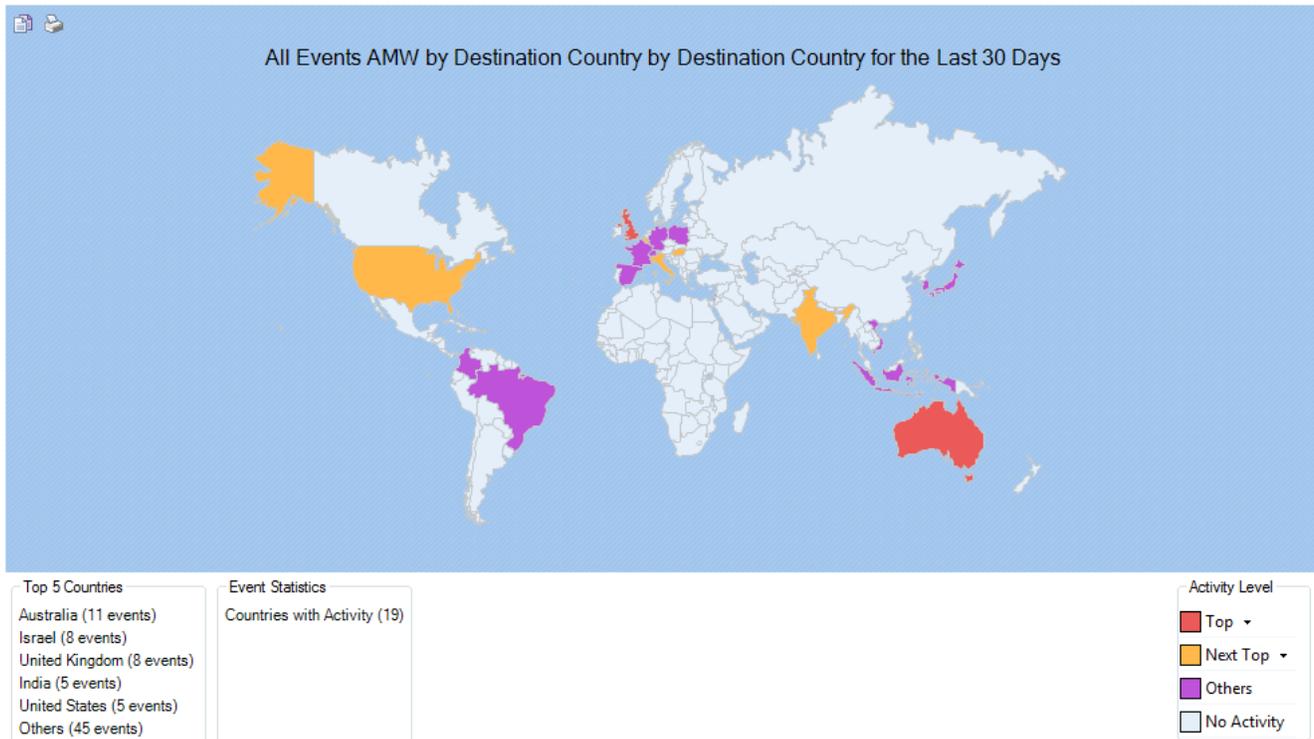
From a host perspective, the following machines have the highest number of Bots & Viruses events:

Host	User	Events
DiedreDash-desktop (125.0.0.63)	Diedre Dash	2
EvanEyelash-laptop (125.0.0.26)	Evan Eyelash	2
LindaLash-laptop (125.0.0.80)	Linda Lash	3
ArielAsh-laptop (86.0.0.57)	Ariel Ash	2
ClarissaCash-desktop (86.0.0.62)	Clarissa Cash	2
ElvinEyelash-laptop (86.0.0.25)	Elvin Eyelash	2
CesarCash-laptop (75.0.0.17)	Cesar Cash	2
FeliciaFlash-desktop (75.0.0.68)	Felicia Flash	2
JackJosh-desktop (75.0.0.38)	Jack Josh	2
JonJosh-laptop (75.0.0.40)	Jon Josh	2
SarahSash-laptop (75.0.0.48)	Sarah Sash	2
Total		23

***Note:** User names will be displayed in the above table only when Check Point Identity Awareness Software Blade is enabled and configured.

Top Destination Countries

The following map shows the distribution of detected Bots and Viruses according to their destination countries. In the case of bots, the destination country usually refers to the Command & Control center location. In the case of viruses, the destination country usually refers to the place where the virus was downloaded from.



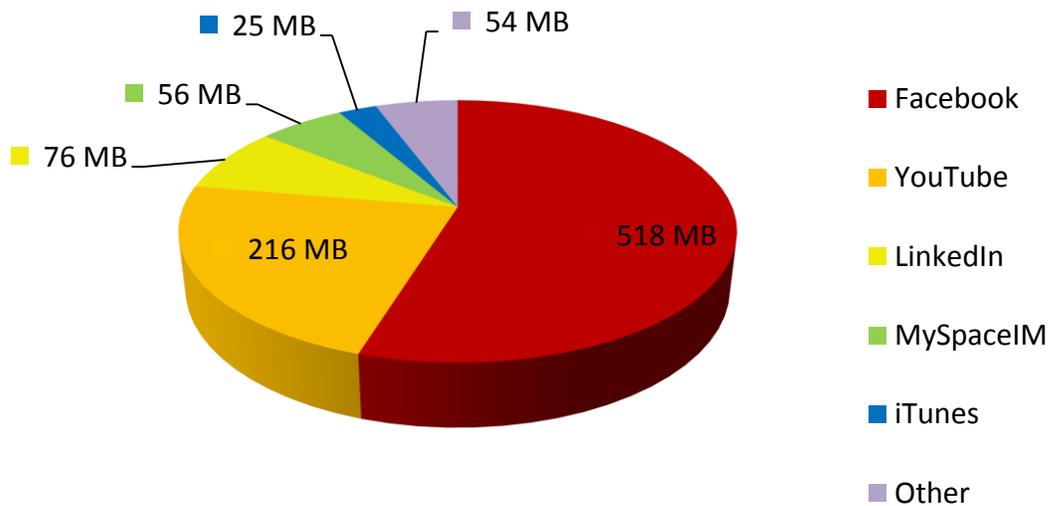


Bandwidth Analysis

The following section summarized the bandwidth usage and web browsing profile of your organization during the time of analysis.

Applications Bandwidth Utilization

During the course of the 3D Security Analysis, your company's employees used significant corporate network resources for non-work activity. The following chart shows how bandwidth was used by your employees:



Top Bandwidth Utilization by Applications & Websites

In all, the analysis process identified that the following applications and websites are used within your network as well:

Count	Application / Site	Matched Category	User	Traffic
21	Facebook	Social Networking	19 Users	518.48 MB
30	YouTube	Video Streaming	28 Users	215.65 MB
10	LinkedIn	Social Networking	10 Users	75.53 MB
2	MySpaceIM	Social Networking	2 Users	56.48 MB
1	iTunes	Multimedia	3 Adam Ash	24.69 MB
44	OpenSSH	2 Matched Categories	39 Users	10.75 MB
41	Twitter	Social Networking	41 Users	10.01 MB
35	Yahoo Mail	Webmail	33 Users	8.55 MB
31	Google Toolbar	2 Matched Categories	31 Users	7.57 MB
12	Windows Live Photo Gallery	2 Matched Categories	12 Users	2.93 MB
6	Apple Software Update	Software Update	6 Users	2.73 MB
11	Windows Live Writer	4 Matched Categories	11 Users	2.69 MB
11	Google Sites	Content Management	11 Users	2.69 MB
1	Picasa	Multimedia	1 Ariel Ash	1.96 MB
7	Adobe Update	2 Matched Categories	7 Users	1.71 MB
2	MSN Web Messenger	Social Networking	2 Users	500 KB
17	google.com	Search Engines / Portals	17 Users	443 KB
6	businessandeconomy.org	Business / Economy	5 Users	317 KB
11	metacafe.com	Media Sharing	11 Users	289 KB
11	yahoo.com	Search Engines / Portals	11 Users	283 KB
1	Google Earth	Virtual Worlds	2 Lydia Lash	250 KB
4	funnyjunk.com	Media Sharing	4 Users	214 KB
3	pcmag.com	Computers / Internet	3 Users	63 KB
1	aol.com	Search Engines / Portals	Earl Eyelash	23 KB
5	bing.com	Search Engines / Portals	5 Users	22 KB
13	Google Maps	Business Applications	13 Users	
15	Gmail	Webmail	14 Users	
4	nba.com	Sport	4 Users	
6	Flickr	File Storage and Sharing	6 Users	
1	Windows Media Player	Multimedia	2 webservice	
1	Xobni	Business Applications	3 Greg Cash	

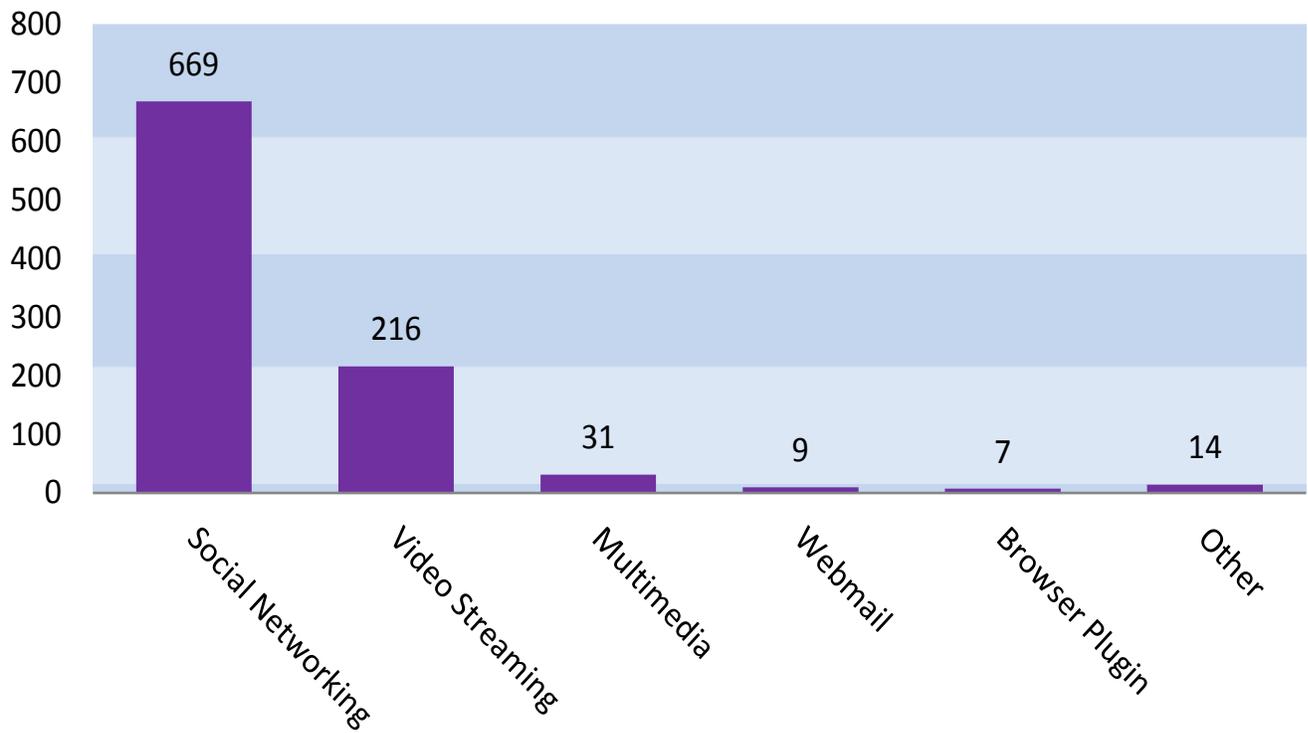
Top Web Categories

The following table shows the top 10 categories and number of hits associated with employee Internet browsing:

Category	Number of Hits	% of Total Hits
Social Networking	118	31%
Webmail	50	13%
Search Engines / Portals	34	9%
Video Streaming	30	8%
Browser Plugin	29	8%
Multimedia	21	5%
Network Utilities	20	5%
Business Applications	18	5%
Media Sharing	15	4%
Other	47	12%
Total	382	100%

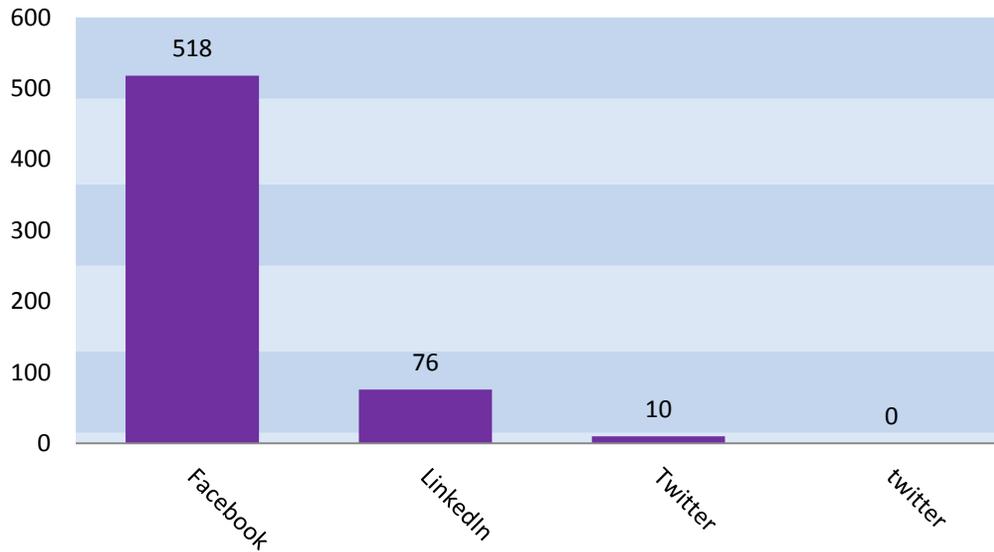
Network Bandwidth Utilization

During the course of the 3D Security Analysis, your company's employees used significant corporate network resources for non-work activity. The following chart shows how bandwidth was used by your employees:



Social networking bandwidth (MB)

The use of social networking sites has become common at the workplace and at home. Many businesses leverage social networking technologies for their marketing and sales efforts, and their recruiting programs. During the course of this project, and consistent with over-all market trends, the following social networking sites consumed the most network bandwidth:



Remediation Recommendations

This report addresses identified security events across multiple security areas and at varying levels of criticality. The table below reviews the most critical of these incidents and presents methods to mitigate their risks. Check Point provides multiple methods for addressing these threats and concerns. Relevant protections are noted for each event, with the software blades into which the defenses are incorporated.



Web Security Events Remediation Recommendations

Application	Events	Remediation Steps
Sopcast	2	In Application Control and URL Filtering Software Blades, you can activate, track and prevent the use of all the mentioned applications & web sites. You can define a granular policy to allow certain applications to specific groups only.
Dropbox	70	
Sugarsync	15	
uTorrent	5	Use UserCheck to educate users about the organization web browsing and applications usage policy.
Vuze	2	

Click for more information about [Application Control](#) and [URL Filtering](#) Software Blades.

To maximize web security on corporate laptops and desktops, use Check Point [Anti-Malware & Program Control](#) and [WebCheck](#) Endpoint Security Software Blades.



Intrusion Prevention Remediation Recommendations

Threat	Events	Remediation Steps
Microsoft Windows Remote Desktop protocol code execution (MS12-020)	45	In Check Point IPS Software Blade, enable the following protection: Microsoft Windows Remote Desktop protocol code execution (MS12-020)
Adobe Flash Player URL security domain checking code execution (APSB12-07)	23	In Check Point IPS Software Blade, enable the following protection: Adobe Flash Player URL security domain checking code execution (APSB12-07)
Microsoft DNS server denial of service (MS12-017)	12	In Check Point IPS Software Blade, enable the following protection: Microsoft DNS server denial of service (MS12-017)
Interactive Data eSignal stack buffer overflow	11	In Check Point IPS Software Blade, enable the following protection: Interactive Data eSignal stack buffer overflow

Click for more information about Check Point [IPS](#) Security Gateway Software Blade.

To maximize intrusions and attacks protection, use Check Point [Firewall & Compliance Check Endpoint Security Software Blade](#).



Data Loss Events Remediation Recommendations

Data Loss	Events	Remediation Steps
Data containing credit card numbers was sent outside the organization (PCI compliance violation).	17	<p>To remediate the detected events activate DLP Software Blade. Configure DLP policy based on the detected DLP data type and choose an action (Detect/Prevent/Ask User/etc..). If you consider the detected data type as sensitive information the recommended action is prevent.</p> <p>Use UserCheck to:</p> <ul style="list-style-type: none"> • Educate users about the organization’s data usage policy. • Provide users with instant feedback when their actions violate the data usage security policy.
Data containing programming language lines (Source Code), such as C, C++, C#, JAVA and more, was sent outside the organization. Indicates leaks of intellectual property.	14	
Pay slip file was sent outside the organization.	16	
International Bank Account Number – IBAN was sent outside the organization.	61	
Data containing Mergers and Acquisitions (M&A) plans was sent outside the organization (e.g. corporate strategy, corporate finance and more)	2	

Click for more information about [DLP](#) Software Blade.

To maximize data loss protection on corporate laptops and desktops, use Check Point [Full Disk Encryption](#) and [Media Encryption](#) Endpoint Security Software Blades.



Bots & Viruses Events Remediation Recommendations

Bots & Viruses	Events	Remediation Steps
Backdoor.Win32.Gbot.pzh	8	To block traffic generated by the detected Malware, enable Anti-Bot & Anti-Virus Software Blades and set the policy's profile settings to Prevent mode.
P2P-Worm.Win32.Palevo.agth	8	To start the remediation process of the infected machine, search the detected Malware in Check Point ThreatWiki to find additional remediation supporting information about the Malware. This information can help you better understand the infection and its potential risks.
Backdoor.Win32.Hupigon.ozqk	6	
Worm.Win32.AutoRun.duv	5	
Email-Worm.Win32.Bagle.pac	5	Use UserCheck to educate users about the organization web browsing and applications usage policy.

Click for more information about Check Point [Anti-Bot](#) and [Anti-Virus](#) Security Gateway Software Blades.

To maximize Bots & Viruses protection corporate laptops and desktops, use Check Point [Anti-Malware](#) and [WebCheck](#) Endpoint Security Software Blades.

3D Security Report Analysis Summary

In this document we have portrayed findings of a recent 3D Security Analysis of your infrastructure. In addition we have presented a set of recommendations for addressing the discovered events and issues.

If you need more information on how to enhance the security in your organization please contact your Check Point Partner or local [Check Point sales representatives](#).

Introducing Check Point 3D Security

Check Point 3D Security redefines security as a 3-dimensional business process that combines policies, people and enforcement for stronger protection across all layers of security—including network, data and endpoints. To achieve the level of protection needed in the 21st century, security needs to grow from a collection of disparate technologies to an effective business process. With 3D Security, organizations can now implement a blueprint for security that goes beyond technology to ensure the integrity of all information security.

Check Point 3D Security enables organizations to redefine security by integrating these dimensions into a business process:



Policies that support business needs and transform security into a business process



Security that involves **People** in policy definition, education and incident remediation



Enforce, consolidate and control all layers of security- network, data, application, content and user

Security Gateway Software Blades



Application Control Software Blade

The Check Point **Application Control Software Blade** provides the industry's strongest application security and identity control to organizations of all sizes. It enables IT teams to easily create granular policies—based on users or groups—to identify, block or limit usage of over 240,000 Web 2.0 applications and widgets.



URL Filtering Software Blade

The **Check Point URL Filtering Software Blade** integrates with Application Control, allowing unified enforcement and management of all aspects of web security. URL Filtering provides optimized web security through full integration in the gateway to prevent bypass through external proxies; integration of policy enforcement with Application Control for full Web and Web 2.0 protection; and UserCheck empowers and educates users on web usage policy in real time.



IPS Software Blade

The **IPS Software Blade** delivers complete and proactive intrusion prevention—all with the deployment and management advantages of a unified and extensible next-generation firewall solution.



DLP Software Blade

Check Point DLP Software Blade combines technology and processes to revolutionize Data Loss Prevention (DLP), helping businesses to pre-emptively protect sensitive information from unintentional loss, educating users on proper data handling policies and empowering them to remediate incidents in real-time.



Anti-Bot Software Blade

The **Check Point Anti-Bot Software Blade** detects bot-infected machines, prevents bot damages by blocking bot C&C communications, and integrates with other Software Blades to provide a comprehensive threat prevention solution on a single gateway.



Antivirus Software Blade

The **Check Point Antivirus** stops viruses and other malware at the gateway before they affect users. Using a continually updated list of antivirus and anti-spyware signatures and anomaly-based protections, the Antivirus and Anti-Malware Software Blade protects against threats transmitted through popular network protocols.

Endpoint Security Software Blades



Check Point Full Disk Encryption

The **Check Point Full Disk Encryption Software Blade** provides automatic security for all information on endpoint hard drives, including user data, operating system files and temporary and erased files. For maximum data protection, multi-factor pre-boot authentication ensures user identity, while encryption prevents data loss from theft.



Check Point Media Encryption

The **Check Point Media Encryption Software Blade** provides centrally-enforceable encryption of removable storage media such as USB flash drives, backup hard drives, CDs and DVDs, for maximum data protection. Port control enables management of all endpoint ports, plus centralized logging of port activity for auditing and compliance.



Anti-Malware & Program Control

The **Check Point Anti-Malware & Program Control Software Blade** efficiently detects and removes malware from endpoints with a single scan. Viruses, spyware, keystroke loggers, Trojans and rootkits are identified using signatures, behavior blockers and heuristic analysis. Program control allows only approved programs to run on the endpoint. This software blade is easily managed by unified Endpoint Security Management.



Firewall & Compliance Check

The **Check Point Firewall & Compliance Check Software Blade** protects endpoints by controlling inbound and outbound traffic and ensuring policy compliance, with centralized management from a single console. Definable zones and security levels protect endpoint systems from unauthorized access. Integrated stealth technology makes endpoints invisible to attackers. This software blade is easily managed by unified Endpoint Security Management.



Antivirus Software Blade

The **Check Point WebCheck Endpoint Software Blade** protects the enterprise against the rising number of web-based threats. Known and unknown web threats, such as drive-by downloads, phishing sites and zero-day attacks, are isolated with browser virtualization technology, while advanced heuristics stop users from going to dangerous sites. This software blade is easily managed by unified Endpoint Security Management.

About Check Point Software Technologies

Check Point Software Technologies' (www.checkpoint.com) mission is to secure the Internet. Check Point was founded in 1993, and has since developed technologies to secure communications and transactions over the Internet by enterprises and consumers.

When the company was founded, risks and threats were limited and securing the Internet was relatively simple. A firewall and an antivirus solution generally provided adequate security for business transactions and communications over the Internet. Today, enterprises require many (in some cases 15 or more) point solutions to secure their information technology (IT) networks from the multitude of threats and potential attacks and are facing an increasingly complex IT security infrastructure.

Check Point's core competencies are developing security solutions to protect business and consumer transactions and communications over the Internet, and reducing the complexity in Internet security. We strive to solve the security maze by bringing "more, better and simpler" security solutions to our customers.

Check Point develops markets and supports a wide range of software, as well as combined hardware and software products and services for IT security. We offer our customers an extensive portfolio of network and gateway security solutions, data and endpoint security solutions and management solutions. Our solutions operate under a unified security architecture that enables end-to-end security with a single line of unified security gateways, and allow a single agent for all endpoint security that can be managed from a single unified management console. This unified management allows for ease of deployment and centralized control and is supported by, and reinforced with, real-time security updates.

Check Point was an industry pioneer with our FireWall-1 and our patented Stateful Inspection technology. Check Point has recently extended its IT security innovation with the development of our Software Blade architecture. The dynamic Software Blade architecture delivers secure, flexible and simple solutions that can be customized to meet the security needs of any organization or environment.

Our products and services are sold to enterprises, service providers, small and medium sized businesses and consumers. Our Open Platform for Security (OPSEC) framework allows customers to extend the capabilities of our products and services with third-party hardware and security software applications. Our products are sold, integrated and serviced by a network of partners worldwide. Check Point customers include tens of thousands of businesses and organizations of all sizes including all Fortune 100 companies. Check Point's award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.