




KASPERSKY SECURITY

INTELLIGENCE SERVICES

2015



A portrait of Eugene Kaspersky, Chairman and CEO of Kaspersky Lab. He is a middle-aged man with short, light brown hair and a beard, wearing a light blue t-shirt under a grey blazer. The background is a soft, light blue gradient. A dark green rectangular box is overlaid on the bottom right of the image, containing white text.

Cybercrime today knows no borders, and its technical capabilities are improving fast: we're seeing how attacks are becoming increasingly sophisticated. Our mission is to save the world from all types of cyberthreat. To achieve this, and to make using Internet safe and secure, it's vital to share threat intelligence in real time. Timely access to information is central to maintaining effective protection of data and networks.

Eugene Kaspersky
Chairman and CEO, Kaspersky Lab

▶ INTRODUCTION

More cyberthreats are appearing every day, in all their different guises and through many different attack vectors.

There is no single solution that offers comprehensive protection. However, even in our big-data world, knowing where to look for danger is a large part of being able to combat the latest threats.

As a CISO/senior-level security professional, it is your responsibility to protect your organization against today's threats, and to anticipate the dangers that lie ahead in the coming years. This needs more than just smart operational protection against known threats; it demands a level of strategic security intelligence that very few companies have the resources to develop in-house.

At Kaspersky Lab, we understand that it takes long-lasting relationships to bring long-term prosperity to a business.

Kaspersky Lab is a valuable business partner, always available to share its up-to-the-minute intelligence with your team via different channels. Our broad range of delivery methods helps your security operation center (SOC)/IT security team remain fully equipped to protect the organization from any online threat.

Even if your organization does not use Kaspersky Lab products, you can still benefit from Kaspersky Lab Security Intelligence Services.

SECURITY WITH A DIFFERENCE

World-leading Security Intelligence is built into our DNA – helping us deliver the most powerful anti-malware on the market and influencing everything we do.

- We're a technology-driven company – from top to bottom – starting with our CEO, Eugene Kaspersky.
- Our Global Research & Analysis Team (GReAT), an elite group of IT security experts, has led the way in uncovering many of the world's most dangerous malware threats and targeted attacks.
- Many of the world's most respected security organizations and law enforcement agencies – including INTERPOL, Europol, CERT, City of London Police – have actively sought our assistance.
- Kaspersky Lab develops and perfects all of its own core technologies in-house, so our products and intelligence are naturally more reliable and efficient.
- The most widely respected industry analysts – including Gartner, Forrester Research and International Data Corporation (IDC) – rate us as a Leader within many key IT security categories.
- Over 130 OEMs – including Microsoft, Cisco Meraki, Blue Coat, Juniper Networks, Alcatel Lucent and more – use our technologies within their own products and services.

► CYBERSECURITY EDUCATION

Leverage Kaspersky Lab's cybersecurity knowledge, experience and intelligence through this innovative education program.

Cybersecurity awareness and education are now critical requirements for enterprises faced with an increasing volume of constantly evolving threats. Security employees need to be skilled in the advanced security techniques that form a key component of effective enterprise threat management and mitigation strategies.

Kaspersky Lab's Cybersecurity Education program has been developed specifically for any organization looking to promote the role of cybersecurity in order to better protect its infrastructure and intellectual property. The program offers a broad curriculum in cybersecurity topics and techniques and assessment ranging from basic to expert.

IMPROVE YOUR IT SECURITY SKILLS TODAY

A COMPREHENSIVE OFFERING

All training courses are offered in English, and are available either in-class on customer premises or at a local or regional Kaspersky Lab office, if applicable. Courses are designed to include both theoretical classes and practical 'labs'. On completion of each course, attendees will be able to complete an evaluation to validate their knowledge.

BEGINNER, INTERMEDIATE OR EXPERT?

The program covers everything from security fundamentals to advanced digital forensics and malware analysis, helping customers to improve their cybersecurity knowledge in three main domains:

- Fundamental knowledge of the topic
- Digital Forensics and Incident Response
- Malware Analysis & Reverse Engineering

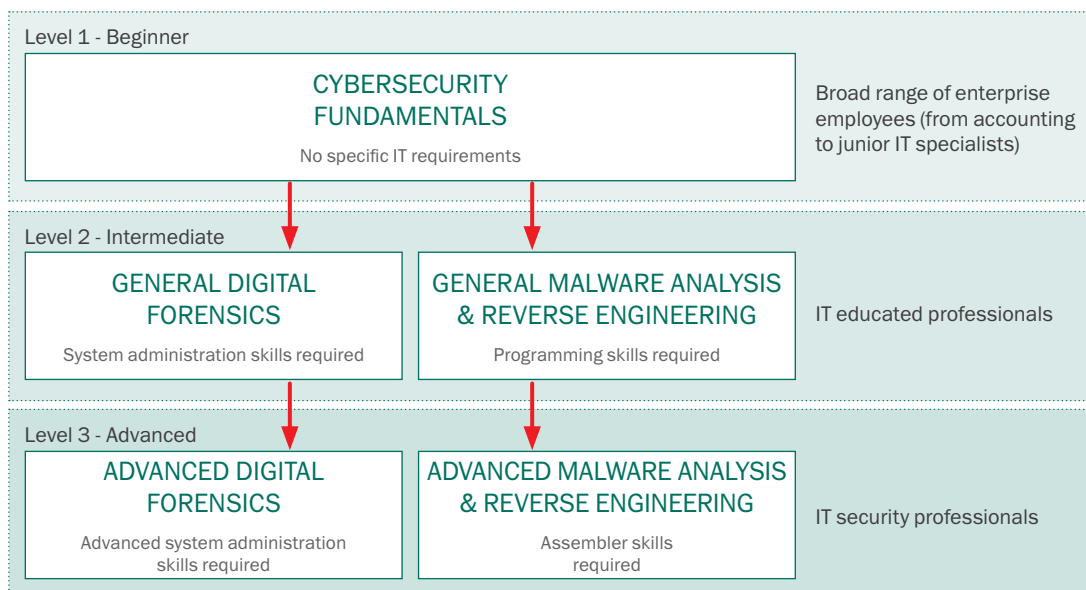
SERVICE BENEFITS

Educating staff in cybersecurity helps organizations to:

- **LEVEL 1 – Cybersecurity Fundamentals**
Reduce expenditure / mitigate reputational risks / mitigate the leakage of confidential information related to generic security mistakes and unawareness of the functionality of major threats.
- **LEVELS 2-3 – Digital Forensics**
Improve the expertise of the in-house digital forensics and incident response team.
- **LEVELS 2-3 – Malware Analysis & Reverse Engineering**
Improve the expertise of the in-house Malware Analysis & Reverse Engineering team.

HANDS-ON EXPERIENCE

From a leading security vendor.



PROGRAM DESCRIPTION

TOPICS	Duration	Skills gained
LEVEL 1 – Cybersecurity Fundamentals		
<ul style="list-style-type: none"> • Cyberthreats & Underground market overview • Spam & Phishing, Email security • Cyber threat types & protection technologies • Advanced persistent threats • Investigation basics using public web tools • Securing your workplace 	2 days	<ul style="list-style-type: none"> • Understand the threat landscape • Be able to use your PC more safely • Recognize different types of attacks • Classify cyber weapons and malware and understand their goals and working principles • Analyze phishing mails • Recognize infected or faked websites
LEVEL 2 – GENERAL DIGITAL FORENSICS		
<ul style="list-style-type: none"> • Introduction to Digital Forensics • Live Response and Evidence Acquisition • Windows Registry Internals • Windows artifacts analysis • Browsers Forensics • Email analysis 	5 days	<ul style="list-style-type: none"> • Build the Digital Forensics lab • Collect digital evidence and deal with it properly • Reconstruct an incident and use time stamps • Find traces of intrusion on investigation artifacts in Windows OS • Find and analyze browser and email history • Be able to apply with the tools and instruments of digital forensics
LEVEL 2 – GENERAL MALWARE ANALYSIS & REVERSE ENGINEERING		
<ul style="list-style-type: none"> • Malware Analysis & Reverse Engineering goals and techniques • Windows internals, executable files, x86 assembler • Basic Static analysis techniques (strings extracting, import analysis, PE entry points at a glance, automatic unpacking, etc.) • Basic Dynamic analysis techniques (debugging, monitoring tools, traffic interception, etc.) • .NET, Visual basic, Win64 files analysis • Script and non-PE analysis techniques (Batch files; Autoit; Python; Jscript; JavaScript; VBS) 	5 days	<ul style="list-style-type: none"> • Build a secure environment for malware analysis: deploy sandbox and all needed tools • Understand principles of Windows program execution • Unpack, debug and analyze malicious object, identify its functions • Detect malicious sites through script malware analysis • Conduct express malware analysis
LEVEL 3 – ADVANCED DIGITAL FORENSICS		
<ul style="list-style-type: none"> • Deep Windows Forensics • Data recovery • Network and Cloud forensics • Memory forensics • Timeline analysis • Real world targeted attack forensics practice 	5 days	<ul style="list-style-type: none"> • Be able to perform deep file system analysis • Be able to recover deleted files • Be able to analyze network traffic • Reveal malicious activities from Memory dumps • Reconstruct the incident timeline
LEVEL 3 – ADVANCED MALWARE ANALYSIS & REVERSE ENGINEERING		
<ul style="list-style-type: none"> • Malware Analysis & Reverse Engineering goals and technics • Advanced Static & dynamic analysis techniques (manual unpacking) • Deobfuscation techniques • Rootkit & Bootkit analysis • Exploits analysis (.pdf, .doc, .swf, etc.) • Non-Windows Malware Analysis (Android, Linux, Mac OS) 	5 days	<ul style="list-style-type: none"> • Use the world best practices in reverse engineering • Recognize anti-reverse engineering technics (obfuscation, anti-debugging) • Apply advanced malware analysis for Rootkits/Bootkits • Analyze exploit shellcode, embedded in different file types • Analyze non-Windows malware

► INCIDENT INVESTIGATION

MALWARE ANALYSIS | DIGITAL FORENSICS | INCIDENT RESPONSE

Personalized incident investigation support to help your organization identify and resolve IT security incidents.

Cyberattacks are an increasing danger for enterprise networks. Tailor-made to exploit the unique vulnerabilities of the criminal's chosen target, these attacks are often designed to steal or destroy sensitive information or intellectual property, undermine operations, damage industrial facilities or steal money.

Protecting an enterprise against these sophisticated, well-planned attacks has become increasingly complicated. It can even be difficult to establish for certain whether your organization is in fact under attack.

Kaspersky Lab's Investigation Services can help organizations formulate their defense strategies through providing in-depth threat analysis and advising on appropriate steps toward resolution of the incident.

SERVICE BENEFITS

Kaspersky Lab Investigation Services help our customers to **resolve live security issues and understand malware behavior and its consequences, providing guidance on remediation**. This approach indirectly helps organizations to:

- **Reduce the costs** of resolving the issues arising from a cyber-infection
- **Stop the leakage of confidential information** that can potentially flow from infected PCs
- **Reduce reputational risks** caused by the infection harming operational processes
- **Restore the normal work of PCs** that were damaged by infection

Kaspersky Lab's investigations are carried out by highly experienced analysts with practical expertise in digital forensics and malware analysis. On completion of the investigation, you as the customer are provided with a detailed report, giving the full results of the cyber investigation and proposing remediation steps.

DIGITAL FORENSICS

Digital Forensics is an investigation service aimed at producing a detailed picture of an incident. Forensics can include malware analysis as above, if any malware was discovered during the investigation. Kaspersky Lab's expert use various pieces of evidence to understand exactly what is going on, including HDD images, memory dumps and network traces. All of this helps to produce a detailed explanation of the incident.

The customer carries out its own incident assessment and collects evidence, presenting Kaspersky Lab with an outline of the incident and the evidence gathered in-house. Then Kaspersky Lab experts analyze the incident symptoms, identify the malware binary (if any) and conduct the malware analysis in order to provide a detailed report including remediation steps.

MALWARE ANALYSIS

Malware Analysis offers a complete understanding of the behavior and objectives of specific malware files that are targeting your organization.

The customer begins the investigation for itself, assessing the incident, collecting evidence and performing a digital forensic analysis. Then it provides Kaspersky Lab with the malware binary. Kaspersky Lab's experts carry out a thorough analysis of the malware sample provided by your organization, creating a detailed report that includes:

- **Sample properties:** a short description of the sample and a verdict on its malware classification
- **Detailed malware description:** an in-depth analysis of your malware sample's functions, threat behavior and objectives - including IOCs - arming you with the information required to neutralize its activities
- **Remediation scenario:** the report will suggest steps to fully secure your organization against this type of threat

INCIDENT RESPONSE

Incident response is our top-level service, covering the full incident investigation cycle. All the expertise in Digital Forensics and Malware Analysis can be brought to the customer's site to assist in the resolution of a security incident.

Kaspersky Lab's experts visit the scene of the incident and carry out all aspects of the investigation in order to deliver targeted incident resolution instructions, including remediation steps. The incident is described in a detailed investigation report.

DELIVERY OPTIONS

Kaspersky Lab Investigation Services are available:

- on subscription, based on an agreed number of incidents
- in response to a single incident

INCIDENT INVESTIGATION WORKFLOW

Kaspersky Lab offers three levels of investigation:

- Malware Analysis – helping you to understand the behavior and objectives of specific malware files that are targeting your organization.
- Digital Forensics – providing a complete picture of the incident and how your organization could be affected.
- Incident Response – a full cycle incident investigation that includes an on-site visit from Kaspersky Lab’s experts.

No	Investigation phases	Malware Analysis	Digital Forensics	Incident Response
1	Incident assessment <ul style="list-style-type: none"> • Rapid response to the incident • Minimization of the consequences • Initial analysis of the incident, that can be done onsite if required, to establish a full understanding of the issue and determine how to collect the necessary evidence 			X
2	Collecting evidence Depending on the situation, gather HDD images, memory dumps, network traces etc related to the incident under investigation			X
3	Performing forensic analysis <ul style="list-style-type: none"> • Establishing a clear, detailed picture of the incident: <ul style="list-style-type: none"> – What happened – Who was targeted – When it happened – Where it happened – Why it happened – How it happened • Analyzing the evidence to find the malware that caused the incident 		X	X
4	Performing malware analysis Analyzing the malware to understand how it works, including its: <ul style="list-style-type: none"> • Classification • Functions • Related vulnerability and exploits • Means of propagation • Destructive activity • Means of installation 	X	X	X
5	Creating a remediation plan <ul style="list-style-type: none"> • Understanding the objective of the malware binary • Developing ways to stop its propagation • Developing uninstallation plans 	X	X	X
6	Creating an investigation report Upon the completion of their analysis Kaspersky Lab experts provide a detailed report, including investigation details and a remediation scenario	X	X	X

▶ THREAT DATA FEEDS

Get more from your SIEM system with an additional layer of protection against malware and dangerous URLs by leveraging KL's comprehensive intelligence data.

Malware families and variations have grown exponentially in the last few years; Kaspersky Lab is currently detecting about 325,000 unique new malware samples every day. To defend their endpoints against these threats, most organizations deploy classical protection measures like anti-malware solutions, intrusion prevention or threat detection systems. In a fast-changing environment where cybersecurity is always trying to stay one step ahead of cybercrime, these classical solutions need to be reinforced with access to up-to-the-minute threat intelligence.

Kaspersky Lab's Threat Data Feeds are designed to integrate into existing Security Information and Event Management (SIEM) systems, providing an additional layer of protection. Integration makes it possible to correlate the logs coming to the SIEM from different network devices with the URL feeds from Kaspersky Lab. **A connection with HP ArcSight SIEM is included.**

USE CASES / SERVICE BENEFITS

- **Improves the SIEM solution by leveraging data about harmful URLs from Kaspersky Lab feeds.**
The SIEM is notified about malware URLs, phishing URLs, Botnet C&C URLs from logs coming to the SIEM from different network devices (user PCs, network proxies, firewalls, other servers)
- **Research purposes.** Leveraging the information about harmful URLs and MD5 hashes of malicious files in research purposes

FEED DESCRIPTION

Kaspersky Lab offers two types of Threat Data Feeds:

1. Malicious URLs and masks
2. MD5 hashes of malicious objects database

FEED DESCRIPTION
Malicious URLs – a set of URLs covering the most harmful links and websites. Masked and non-masked records are available.
Phishing URLs – a set of URLs identified by Kaspersky Lab as phishing sites. Masked and non-masked records are available.
Botnet C&C URLs – a set of URLs of botnet command and control (C&C) servers and related malicious objects. Mobile C&Cs are included.
Malware Hashes (ITW) – a set of file hashes covering the most dangerous in-the-wild (ITW) malware encountered by Kaspersky Security Network users. The base contains hashes with Kaspersky verdicts for each object.
Malware Hashes (UDS) – a set of file hashes detected by Kaspersky cloud technologies (UDS - Urgent Detection System) based on a file's metadata and statistics (without having the object itself). This allows the system to identify malware that is not detected by other methods. This can also be described as "recently identified malware hashes"
Android Malware Hashes – a set of file hashes for detecting malicious objects that infect mobile Android platforms

► INTELLIGENCE REPORTING

Increase your awareness and knowledge of the threats your organization and your sector face with comprehensive and practical reporting from Kaspersky Lab.

Tracking, analyzing, interpreting and mitigating constantly evolving IT security threats is a massive undertaking. And it's not even your core business. Enterprises across all sectors are facing a shortage of the up-to-the-minute, relevant data they need to help them manage the risks associated with IT security threats.

A subscription to Kaspersky Lab's Intelligence Reporting helps to mitigate these risks, giving your enterprise access to the intelligence, provided by our top analysts based on more than 80 million user statistics gathered across 200 countries.

Kaspersky Lab's knowledge, experience and deep intelligence on every aspect of cybersecurity has made it the trusted partner of the world's premier law enforcement and government agencies, including INTERPOL and the most important CERTs. You can leverage this intelligence in your organization today.

KASPERSKY'S INTELLIGENCE REPORTING SHOULD BE A KEY ADDITION TO YOUR ORGANIZATION'S PROACTIVE SECURITY PROCEDURES:

EFFECTIVE AND ACTIONABLE

A subscription to Kaspersky Lab's Intelligence Reporting provides the security professional with heightened intelligence and awareness in their chosen security areas. In addition to using the reports to learn, detect and mitigate risks posed by new attack techniques, big campaigns or recently-developed malware, many organizations leverage them for private research purposes, to detect the described threats in their own organizations, or to develop a security strategy.

SERVICES BENEFITS

- Improved awareness among security personnel, especially about hot trends in Financial Threats
- The latest technical description, campaign details, indicators of compromise and evidence of cyberthreats detected by Kaspersky Lab

SUBSCRIPTION LEVELS AND DELIVERABLES

1-year subscription to Intelligence reporting (quarterly)

- Executive summary
- Description of the most recent and dangerous threats
- Cyber threat statistics

▶ BOTNET THREAT TRACKING

Expert monitoring and notification services to identify botnets threatening your customers and your reputation.

Many network attacks are organized using botnets. These attacks can target casual internet users, but often these threats are aimed at the online customers of specific organizations and their online customers.

Kaspersky Lab's expert solution tracks the activity of botnets and provides rapid (within 20 minutes) notification of threats associated with the users of individual online payment and banking systems. You can use this information to advise and inform your customers, security services providers and local law enforcement agencies about current threats. Protect your organization's reputation and customers today with Kaspersky Lab's Botnet Threats Notification Service.

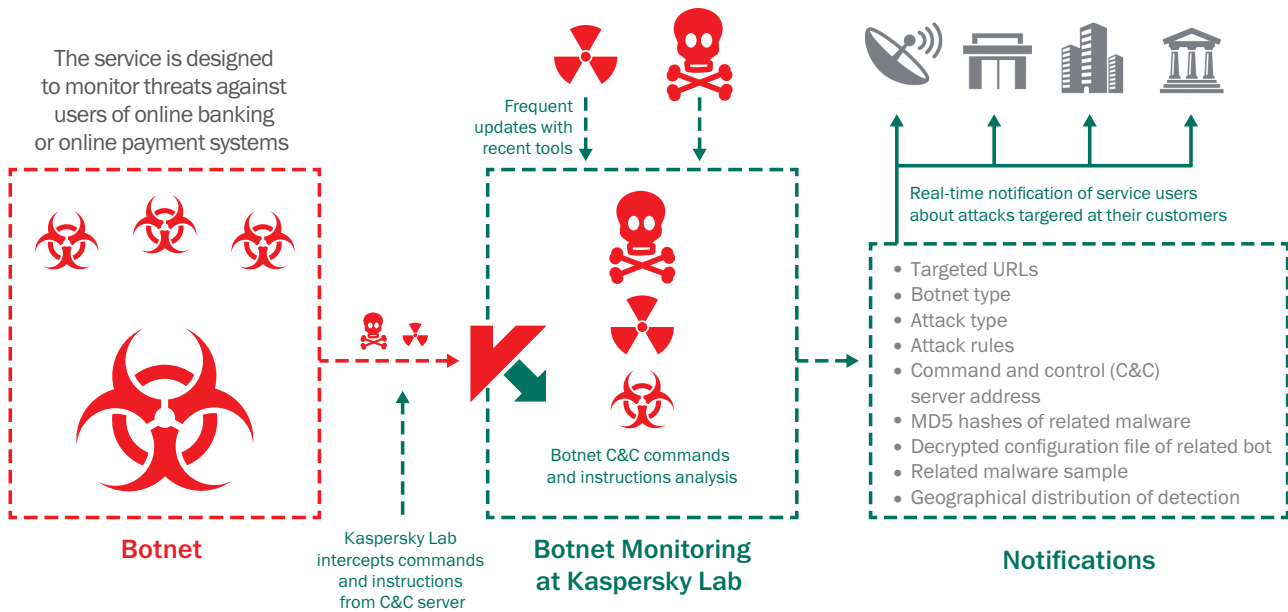
USE CASES / SERVICE BENEFITS

- **Proactive alerts** about threats coming from botnets that target your online users allow you to always remain one step ahead of the attack
- **Identifying a list of Botnet Command & Control server URLs** that are targeting your online users allows you to block them by sending requests to CERTs or Cyber Police
- **Improve your online banking / payment cabinets** by understanding the nature of attack
- **Train your online users** to recognize and avoid falling foul of the social engineering used in attacks

TAKE ACTION WITH REAL-TIME DELIVERABLES:

The service provides a subscription to personalized notifications containing intelligence about matching brand names by tracking keywords in the botnets monitored by Kaspersky Lab. Notifications can be delivered via email or RSS in either HTML or JSON format. Notifications include:

- **Targeted URL(s)** — Bot malware is designed to wait until the user accesses the URL(s) of the targeted organization and then starts the attack.
- **Botnet type** — Understand exactly what malware threat is being employed by the cybercriminal to jeopardize your customers' transactions. Examples include Zeus, SpyEye, and Citadel.
- **Attack type** — Identify what the cybercriminals are using the malware to do; for example, web data injection, screen wipes, video capture or forwarding to phishing URL.
- **Attack rules** — Know what different rules of web code injection are being used such as HTML requests (GET / POST), data of web page before injection, data of web page after injection.
- **Command and Control (C&C) server address** — Enables you to notify the Internet service provider of the offending server to dismantle of the threat faster.
- **MD5 hashes of related malware** — Kaspersky provides the hash sum that is used for malware verification.
- **Decrypted configuration file of related bot** — identifying the full list of targeted URLs.
- **Related malware sample** — for further reversing and digital forensic analysis of the botnet attack.
- **Geographical distribution of detection (top 10 countries)** — Statistical data of related malware samples from around the world.



Kaspersky Lab's solution is available in either Standard or Premium, offering a variety of service terms and monitored URLs. Consult with Kaspersky Lab or your reseller partner to determine which package is right for your enterprise.

SUBSCRIPTION LEVELS AND DELIVERABLES

Standard	Premium	<p>Notification in email or JSON format</p> <ul style="list-style-type: none"> • Decrypted configuration file of related bot • Related malware sample (on demand) • Geographical distribution of detections for related malware samples 	10 URLs monitored
	Standard	<p>Notification in email format</p> <ul style="list-style-type: none"> • Target URL (identifying the URL(s) were the bot program is targeting users) • Botnet type (e.g., Zeus, SpyEye, Citadel, Kins, etc.) • Attack type • Attack rules, including: Web data injection; URL, screen, Video capture, etc. • C&C address • MD5 hashes of related malware 	5 URLs monitored

For more information on Kaspersky Security Intelligence Services,
please contact us via intelligence@kaspersky.com.
TO LEARN MORE VISIT www.kaspersky.com



Kaspersky Lab
www.kaspersky.com

All about Internet security:
www.securelist.com

Find a partner near you:
www.kaspersky.com/buyoffline

Feb 15/Global

© 2015 Kaspersky Lab ZAO. All rights reserved. Registered trademarks and service marks are the property of their respective owners.
Microsoft, Windows Server and SharePoint either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

