The Future Threat Landscape and Next-Generation Security

Surender Kumar Bishnoi
General Manager, Cyberoam
Surender.bishnoi@cyberoam.com

Our Products

Unified Threat Management

Cyberoam – Endpoint Data Protection

- Data Protection & Encryption
- Application Control
- Device Management
- Asset Management

SSL VPN

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Agenda of Presentation

- **2010, a year of significant cyber security events**
- **Key questions to ask**
- **Cyberoam's future-ready UTM security**

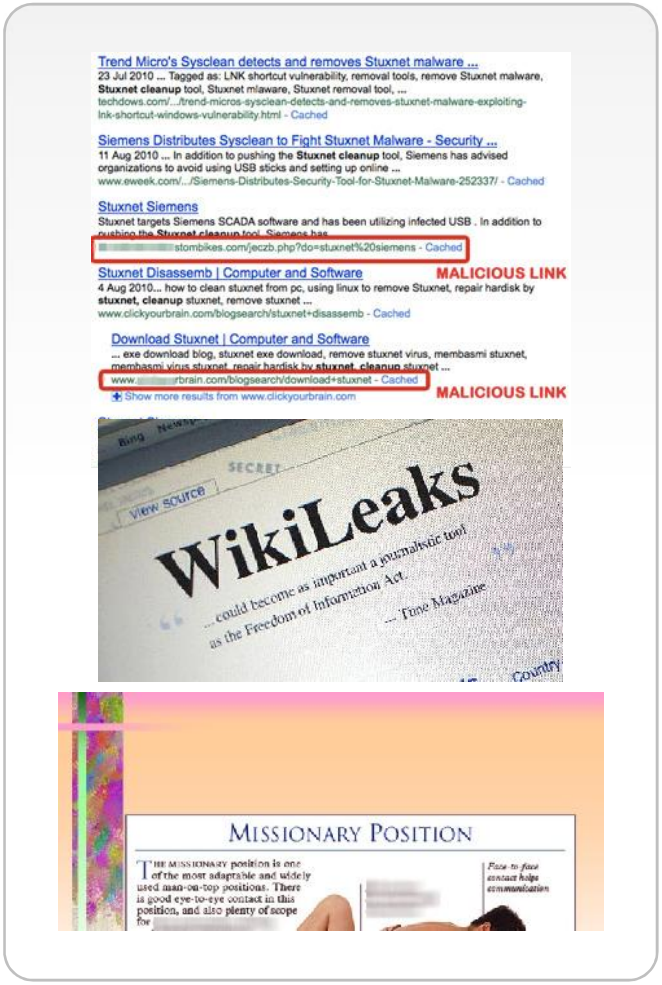
© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

2010, a year of significant cyber security events

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Major recent security incidents

- **Stuxnet**
  - Jan 2010: Targets industrial software and equipment
- **Hydraq Trojan**
  - July 2010: Hackers made backdoor entry to corporate Intranets
- **Kama Sutra virus via downloadable ppt**
  - Jan 2011: Downloaded presentation runs malware in the background
- **Current news events driving spam in corporate networks**
  - Wikileaks, Osama Bin Laden death



© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

2010: Key threat statistics

- **More than 300 million unique malicious programs in 2010**
- **Mobile threat landscape comes into view**
  - Public app stores leveraged for attacks
- **93% increase in web-based attacks**
  - Attacks emerge using shortened URLs
- **14 NEW zero-day attacks per day**
  - Including Hydraq, Stuxnet, Kama Sutra etc.
- **260,000 identities exposed per data breach**
  - Hacking incidents drive identity theft in organizations

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

The evolution of the threat landscape

- **Past**
  - Lesser complex networks that were manageable
  - Fewer mediums of security vulnerability
    - External drives, Instant Messengers, Email etc.

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

The evolution of the threat landscape

- **Present**
  - Complex networks
  - Rise in number of incidents due to
    - Wireless technologies
    - Handheld devices (like PDAs, cellphones)
    - Extending networks to partners, customers and more
    - HTTPS / SSL websites
    - Social media
    - Web 2.0 technologies
  - **Future**: The threats would grow more serious
    - Cloud-residing data
    - Heterogenous networks (HetNets)

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Security Executives are in a Middle of a Complex System

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Key questions to ask

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

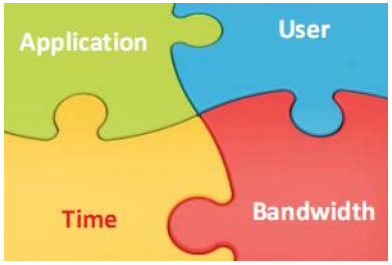
Applications and More Applications. Am I in control?

- **Who decides which applications are important to business and run on network ?**

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Guiding factors to enable productive use of applications

- **Managing the 4 elements**: Application, user, time and bandwidth
- **Know and classify applications trying to enter the network**
  - Business (White) e.g. Salesforce, CRM, ERP etc.
  - Non-business (Black) e.g. P2P, iTunes etc.
  - Socio-business (Grey) e.g. Twitter, Facebook etc.
- **User**: Gain visibility and controls on "who is accessing which" applications in the network
- **Time**: Schedule access to applications based on business need and time of the day
- **Bandwidth**: Committed bandwidth to business-critical applications



© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Prioritizing applications as per business need

Application Visibility & Control

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

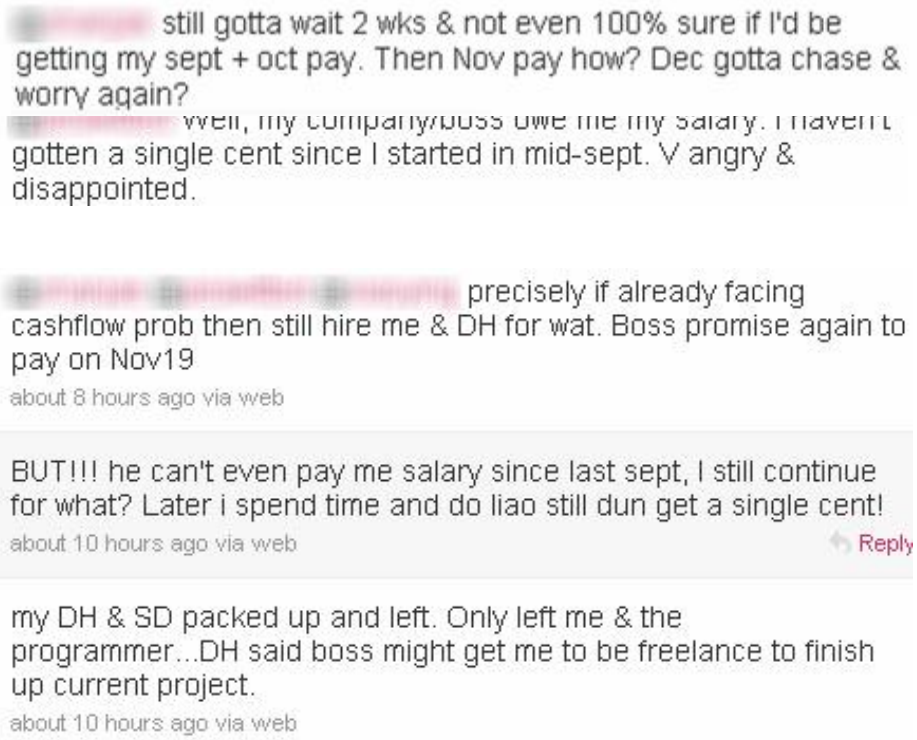
Social Media: An increasing risk

- **Individual tidbits of information lying across Twitter, Facebook, LinkedIn etc. when seen together, constitute insider threats**
  - The DNA of the entire organization can be decoded
- **INTANGIBLES**
  - Core values, hierarchy, communication patterns, industry environment, employee morale
- **TANGIBLES**
  - Intellectual property, financial information, trade secrets
- **What we did at Cyberoam**
  - Monitored 20 companies with active social media presence to learn about the disclosures made by employees

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Example in detail

Insider threat is represented by unwanted disclosures by employees belonging to a Singapore-based IT company



Employees not getting salary

+

Cashflow problems in organization

+

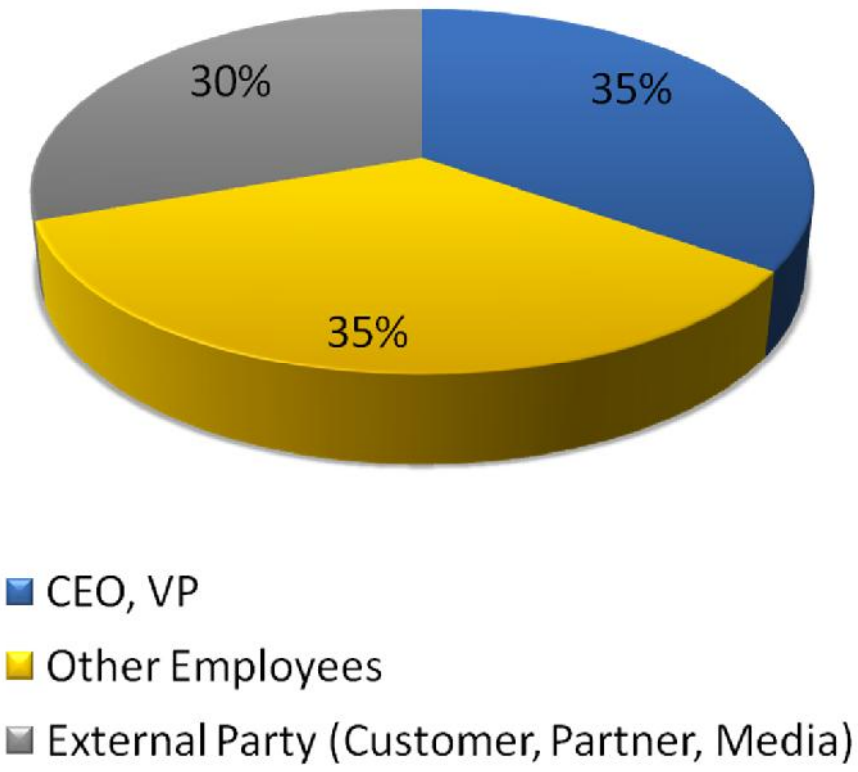
Bounced salary checks

+

Employees looking for new jobs

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

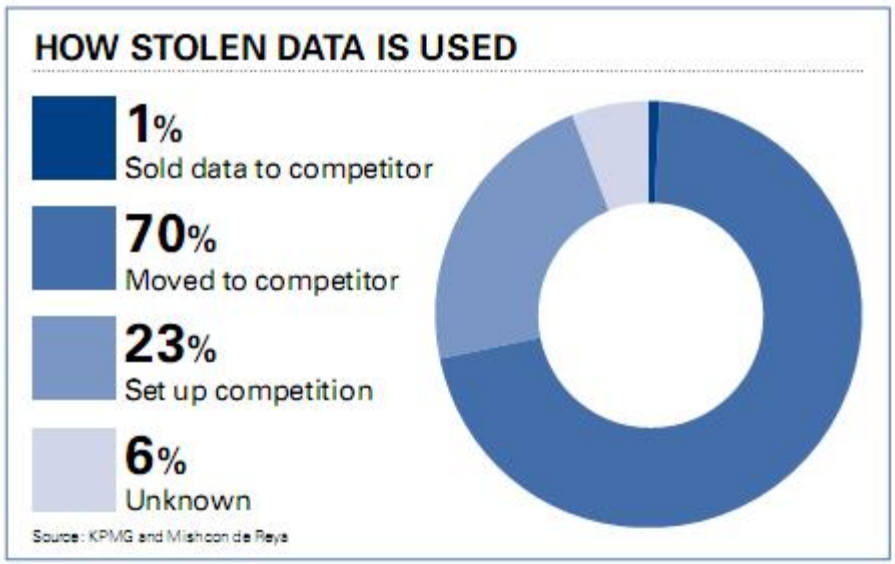
Surprising revelations on social media disclosure

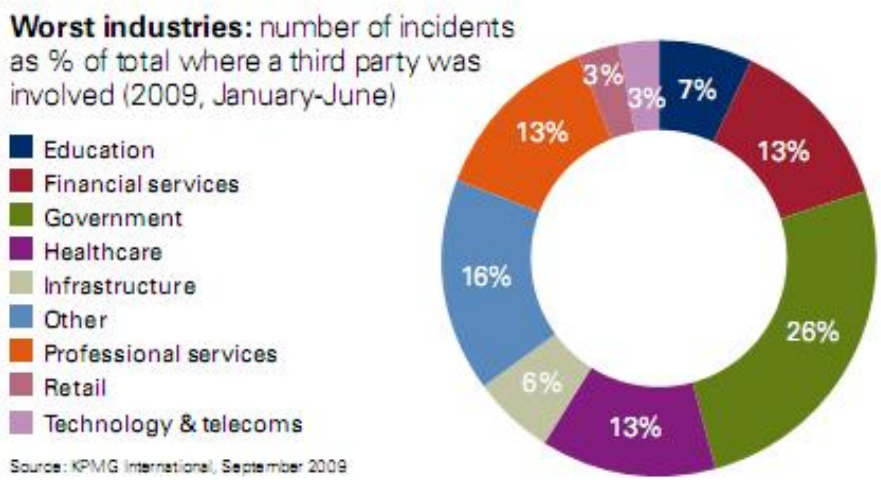


© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

How vulnerable is my organization to insider threats?

93% employees had betrayed the organization to directly benefit competition





(SOURCE – *KPMG Data Loss Baramoter, 2009)*

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Causes and motivations behind insider threats

Ignorant Users

- **Lack of awareness about an organization's security practices**
- **Vulnerable to targeted attacks**
  - Social engineering attacks by ex-employees
  - Social network exploits
  - Hackers, phishing

Users with malicious intent

- **Apathetic employee**
  - Ignores system alerts and IT security policies
- **Angry, disgruntled employee**
  - Sabotages, schemes, teams up with competitors
- **Opportunistic, cunning employee**
  - Motivated by personal and financial gains

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Why are insider attacks succeeding?

- **Greater fluidity of network parameter**
- **Employee access to business-critical applications, Web 2.0, social media**
- **Traditional security's inability to identify human role**
  - Victim - User ignorance, surfing patterns, trust, lack of awareness, lax security policy
  - Attacker - Malicious intent, vengeance, greed

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

How much control I have over users in my network?

- **What are my employees doing in my network all the time**
  - Who is doing what?
  - Who is the attacker?
  - Who are the likely targets?
  - Which devices are being used to connect to the web? Who accesses them?
- **How to combat insider threats?**
- **How to increase productivity?**
- **Does my existing security solution help me be proactive?**
- **Can I get reports on security incidents in real time?**

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Guiding factors to mitigate insider threats

- **Measure User Threat Quotient (UTQ)**
- **Deploy a network security solution**
  - Identity-based approach to control
  - Who can connect using which device?
  - What is being accessed over the network and by whom?
- **Security over Wi-Fi**
- **Securely extends network to customers, partners, remote workers**
- **Visibility into HTTPS /SSL traffic**
- **Role based access to resources and social media**

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Measuring User Threat Quotient (UTQ)

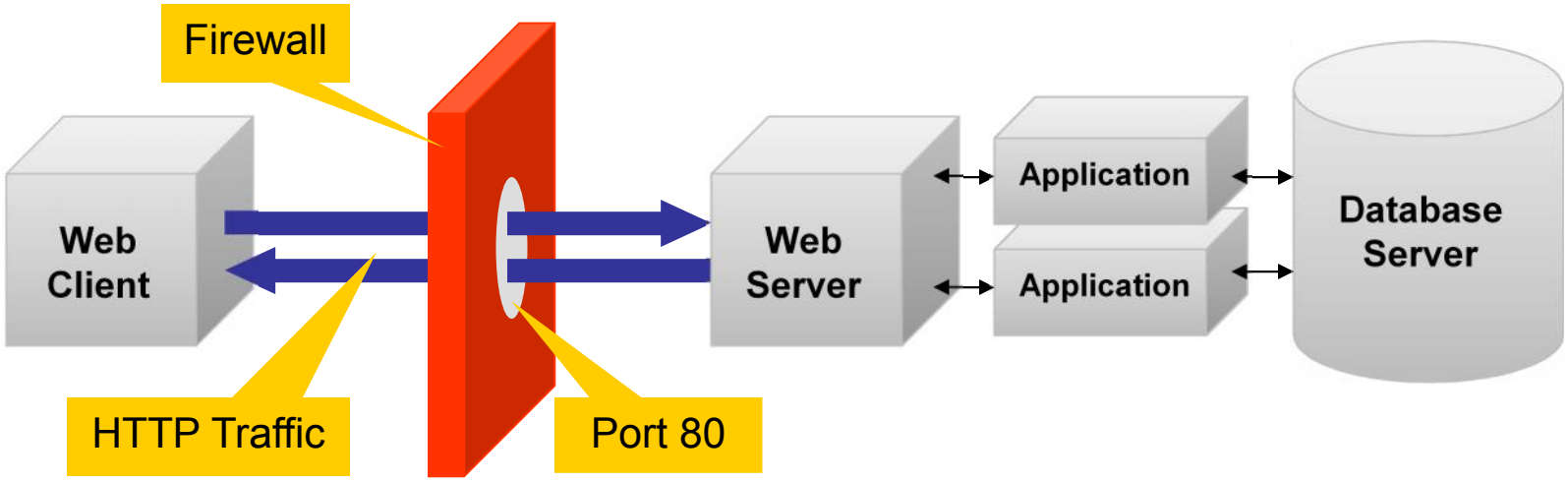
Building patterns of activity profiles - User Threat Quotient (UTQ)

- Identify deviations from the normal acceptable user behavior
- Red flag malicious activity based on UTQ
- Context of activity – repeated wrong password attempts by new vs. old employee
- Get Intrusion alerts with user identity information
- Train and educate employees on acceptable Internet use behavior

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Am I able to protect web applications in my network?

- **Does my firewall protect websites and applications hosted in my local network or data center?**
  - Traditional firewalls cannot determine if a properly addressed packet contains a threat.
  - Hackers exploit OWASP Top 10 vulnerabilities e.g. SQL command injection, cross-site scripting, session hijacking



© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Websites/ Web Application Security Breach: It happens to everyone

March 24th, 2008
Microsoft confirms Word attacks

XSS Vulnerability in Facebook Translations Posted on: 8 March 2011

24 December 2010
CitySights NY Website Hacked, and Users Credit Card Information Stolen

September 16, 2010
Polish hacker gets inside US Military's Defense Logistic Agency website

21 February 2011
Voice of America (VOA) website hacked by Iranian Cyber Army Iranian computer hackers on Monday hijacked the website of the Voice of America, replacing its Internet home page with a banner bearing an Iranian flag and an image of an AK-47 assault rifle..

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Guiding factors to protect web applications in your network

- **Web Application Firewall**
  - Inspect any incoming data before it reaches the web server, and also any outgoing data after it leaves the web server
  - Offers protection against exploitation of OWASP Top 10 Web Application vulnerabilities
  - Offers pro-active protection against Application layer attacks and business logic attacks
- **Should integrate with other security devices or features over one device**
- **Provides reports on attacks**

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Threat environment is dynamic. Can I keep up with it?

- **Is my existing network security setup rigid and hard-coded?**
- **Can it respond to latest threats without decline in system performance?**
  - E.g. newer AV/AS/IPS signatures to fight zero-hour malware threats, DoS attacks etc
- **Can the architecture grow to accommodate future threats?**
- **Does "hardware acceleration" cause drop in performance value?**

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Guiding factors to help overcome latest & unknown threats

- **Extensibility of security appliance**: Ability to accomodate additional features and capabilities
- **Stable Performance**: Additional features without degrading security appliance performance
- **Protecting investment**: No need to invest in new expensive hardware or additional rackspace
- **Multicore-aware software architecture**:
  - Parallelism – sharing computing load on multiple processors
  - High speed access to look up signature tables
  - Extra memory to manage dynamic attacks
  - Quickly deliver new patches and policies online

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Does my security solution facilitate compliance?

- **Regulatory compliance** is becoming increasingly mandatory for organizations in all verticals
  - **Why?**
    - Organizations must follow best practices laid down by industry
  - **Challenges to be addressed by security solution**
    - Complicated documentation processes
    - Identifying users and their online behavior
    - Painful audit process

HIPAA

CIPA

GLBA

PCI DSS COMPLIANT

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Am I ready for the new Internet?

- **Can my existing network security setup process both IPv4 and IPv6 Traffic?**
- **The IPv4 meter has stopped rolling (1-Feb, 2011)**
- **Any new Internet Addresses allotted will be IPv6**
  - New Perimeter Devices, Applications, Websites etc
- **Does it have 'IPv6 Ready' gold logo**
- **Third-party validation**
  - International Testing Program with 3000+ rigorous test cases

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

How effectively am I spending?

- **Am I spending lesser and smarter?**
- **How many security products I have to manage?**

- Firewall, Routers
- Content filters, Bandwidth Managers
- Multiple Link Managers, VPN

…and more

- **Does my Total Cost of Security Operations increase with multiple solutions?**

- How much am I spending on licensing and subscription costs?
- Do I spend lot of time configuring and managing my network security solution?

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Guiding factors to help you spend smartly on security

- **Reduced complexity:**
  - Single security solution, single vendor and single AMC
  - No need for multiple software applications to be installed or maintained
- **Troubleshooting ease:** Single point of contact with 24X7 support
- **Reduced technical training requirements:** one product to learn
- **Easy management:** Simple is always more secure; Web-based GUI; saves time
- **Future-ready:** Preparing against HTTPS/SSL attacks, Cloud-based attacks

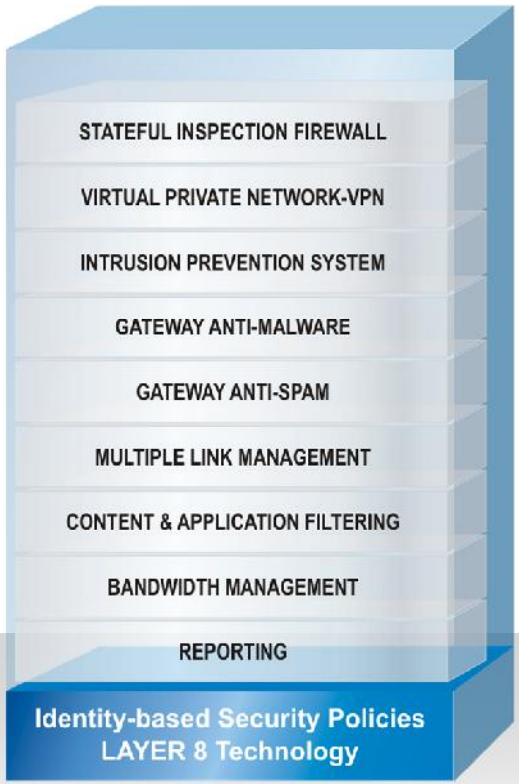
© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Cyberoam's future-ready UTM security

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Cyberoam's Next-Generation Unified Threat Management

- **Gateway Integrated security over single platform**
  - Reduces capital & operational expenses
  - Freedom from multiple security vendors
- **Continuous Focus on future security needs**
- **Right balance of Security, Connectivity, Productivity enabling growth**
- **Offers Layer 8 identity-based security based on granular user visibility/controls**



© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

What does Industry say about us?

Visionary in the Gartner UTM Magic Quadrant

Source: Gartner (October 2010)

SC MAGAZINE INNOVATOR 2010

SC MAGAZINE

IDC
Analyze the Future

FROST & SULLIVAN
Emerging Company of the Year for Network Security

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Q&A

If any??

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Thank you!

Surender.bishnoi@cyberoam.com

© Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.