

## Creating the Trusted, Dynamic Enterprise

### An enterprise security blueprint

Securing communications for all voice and data applications as well as employee mobility is the key to supporting new business models and enabling a trusted, dynamic enterprise that competes effectively in today's business environment. Rapid advances in communications technology have been accompanied by an equally rapid multiplication in security threats, the growth of cybercrime, and the introduction of new security regulations. To take advantage of the latest business models and ensure they are still protected enterprises must change how they view security. Security must become a positive enabler for driving business performance. To achieve this objective enterprises must have a corporate-wide strategy — a security blueprint — that allows the enterprise to be open for business and provide a trusted environment. Security must also be more dynamic by constantly evolving to meet new threats and allowing for real-time adjustment of security policies to reduce risk. This requires a shift to a user-centric approach to security that is delivered from within the network to protect networks, people, processes and knowledge.

## Table of contents

---

<b>1</b>	<b>The Need for a New Approach to Enterprise Security</b>
<b>2</b>	<b>Enterprise Security Challenges</b>
2	New business models drive new communications requirements
3	The emergence of organized cybercrime
3	The new regulatory frontier
4	Three enterprise security requirements
<b>5</b>	<b>A Fresh Perspective on Enterprise Security</b>
<b>6</b>	<b>The User-Centric Security Blueprint</b>
7	Network
7	People
7	Process
8	Knowledge
<b>8</b>	<b>Applying the Blueprint</b>
9	Perimeter security
10	Network access control
10	Identity management
10	Application security
10	Mobile security
10	Security management
<b>11</b>	<b>Conclusion</b>
<b>11</b>	<b>Acronyms</b>

## The Need for a New Approach to Enterprise Security

---

The business of doing business is changing more rapidly today than it ever has. With advances in communications technology enterprises around the world continue to find new, exciting and efficient ways of leveraging the ubiquity of the Internet and the Web to conduct daily business:

- Business-to-business applications that foster greater cooperation with partners and suppliers are extending the border of the enterprise taking it out further into the global Internet.
- The adoption of IP Telephony with voice over IP (VoIP) and the movement to all IP networks is creating more opportunities for enterprises to converge voice and data networks. This improves employee productivity and efficiency with unified communications, while streamlining communications infrastructures and reducing communications costs.
- The widespread adoption of mobile communications services and applications allows mobile employees to stay connected with the corporate network and colleagues when they are on the move. Not only with just voice connections, but with mobile Internet access and a new generation of smartphones to improve efficiency and collaboration.
- Web 2.0 which allows information to be sourced from many locations and displayed as composite parts of new applications is changing the way enterprises use the Internet for business interactions with employees, customers, partners and suppliers.
- Cloud computing is on the horizon with the promise to reduce costs by creating virtual computing “clouds” in cyberspace.

All these changes are creating opportunities for enterprises worldwide to transform themselves into dynamic enterprises by connecting their network, people, processes, and knowledge to build a competitive advantage.

However, while making the transformation to a dynamic enterprise, enterprises must also deal with a technology-driven multiplication in security threats and the growth of cybercrime:

- Automating business processes with partners can expose an enterprise to significant potential for information security breaches and malicious activity conducted from outside the enterprise.
- The adoption of VoIP has made voice a new network security risk and is exposing enterprises to potential breaches to the traditional security perimeter, denial of service (DoS) attacks, and theft of company-sensitive information, such as the company directory.
- Mobile communications services and applications are opening the door to new mobile malware risks and the potential for private corporate data to be lost or stolen when stored on mobile devices.
- New business models enabled by Web 2.0 and cloud computing are creating more challenges by externalizing business processes and moving them to cyberspace where there is less control of private data and the traditional enterprise perimeter can no longer provide a sufficient defense.

At the same time, the introduction of new security regulations requires enterprises to create and manage a more secure business environment that protects end-user information and privacy.

Being a dynamic enterprise in this environment is only half of the formula for success. The other half requires an organization to become a trusted, dynamic enterprise by making security a positive enabler and a dynamic, integral part of the enterprise rather than a static add-on.

A trusted, dynamic enterprise has open and secure interfaces to communications, data and services that enable the enterprise to take advantage of new collaborative business models while protecting against new threats, protecting private data and complying with governance requirements.

The transformation to a trusted, dynamic enterprise requires a user-centric approach to security. Enterprises must have a corporate-wide security blueprint that allows them to be open for business and provides a trusted environment for employees, business partners and customers. This blueprint must also enable enterprise security to be more dynamic by constantly evolving to meet new threats and by allowing for real-time adjustments of security policies to reduce risk.

User-centric security is supplied from within the network. It gives an enterprise fine-grain control of end-user activity. It equips the enterprise to enable employees to get their work done more efficiently, while at the same time controlling risk. In addition, a user-centric approach supports detailed audits for managing risk and demonstrating compliance.

With a security blueprint, enterprises can efficiently transform themselves into a trusted, dynamic enterprise by addressing enterprise security from the perspective of the network, people, processes, and knowledge to drive business performance — the same vectors that are used to model communications for a dynamic enterprise.

## Enterprise Security Challenges

---

Early in 2009 industry experts presenting to the U.S. Senate committee hearing on improving cyber security estimated profits from the cybercrime economy totaled close to \$1 trillion U.S., more than the cash generated by drug crime.<sup>1</sup> This was reinforced in a report by Symantec in April 2009 that noted there was a 265 percent increase in malicious code threats in 2008 compared to 2007.<sup>2</sup>

Security has always been a major concern for enterprises worldwide. Today's requirement for new business models, the pace of technological change and the emergence of a new, more sophisticated wave of cyber criminals, and demanding regulatory environment are making security more challenging for enterprises of all sizes.

### **New business models drive new communications requirements**

New business models, such as cloud services and Web 2.0 mashups, are being rapidly adopted without mastering how to make the technology less vulnerable. As companies embrace mobile communications, enable employees to work from remote locations, and co-market and sell with partners, the enterprise IT team must respond with new security methods to keep the enterprise secure.

An advanced and secured communications network is the key to enabling an enterprise to respond to this new business environment and become a dynamic enterprise. A dynamic enterprise — a term that describes a successful, profitable company that is constantly evolving to quickly adapt to its market environment and differentiate itself from its competitors — must simplify communications, strengthen relationships and increase productivity in a continuous transformation process. This ongoing process must efficiently and securely interconnect four key business assets (Figure 1):

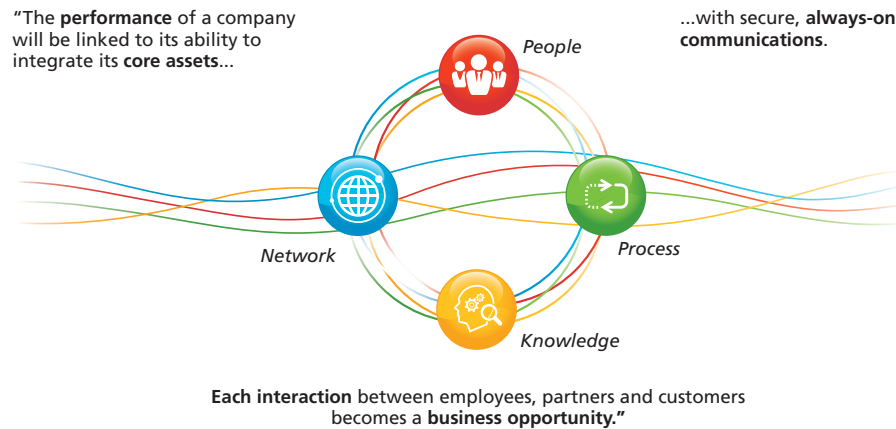
- *Network*: which is the foundation for the enterprise communications infrastructure
- *People*: which includes employees, contractors, partners and suppliers
- *Process*: which are the tasks carried out by employees
- *Knowledge*: in the organization, which is typically in people's heads or scattered across multiple databases

By securely interconnecting these four assets, the dynamic enterprise can quickly adapt to new market environments and differentiate itself from competitors. And it can benefit from simplified communications, stronger relationships, and increased productivity to enable continuous and transformative growth.

<sup>1</sup> "Cybercrime More Profitable Than Drugs," IT Pro, March 2009, <http://www.itpro.co.uk/610344/cybercrime-more-profitable-than-drugs>.

<sup>2</sup> "April Internet Security Threat Report," Symantec, April 2009, <http://www.symantec.com/business/theme.jsp?themeid=threatreport>.

**Figure 1. The dynamic enterprise securely interconnects its network, people, processes and knowledge**



## The emergence of organized cybercrime

One of the biggest challenges to arrive on the scene as a direct result in the number of devices now connected to the mobile Internet is the way cyber criminals now operate.

In an October 2008 report, the Georgia Tech Information Security Center (GTISC) stated that "sources of cybercrime will become increasingly organized and profit-driven in the years ahead."<sup>3</sup> The report described the new wave of cyber criminals as "an international conglomerate of professionally trained authors motivated by high profit." It went on to explain that cyber criminals can now:

*"... buy, lease, subscribe and even pay-as-you-go to obtain the latest malware kits, which are much more sophisticated than their predecessors... The new sophisticated malware-for-sale features encrypted command and control channels, built-in Web services for hosting phishing content, man-in-the browser proxy engines for identity theft, along with drive scanners for capturing sellable data like e-mail addresses and credit card details... several malware kits are supported by product guarantees and service level agreements. A few malware developers are even offering multiple language 'customer support' in order to reach a wider audience of criminals. New Web-based attack platforms have been developed in tandem so that social engineering and end-user action are no longer required for exploitation. All of these trends are expected to evolve further in the coming year."*

As cybercrime becomes more sophisticated and organized, enterprises will have a tougher challenge securing their networks against cyber threats that can happen at any time.

## The new regulatory frontier

As new technologies enable new business models and cyber criminals continue to search for ways to circumvent network security, end-user privacy becomes more important. Consumers, employees, partners, and suppliers want to be sure their data and their personal information is secure and that the enterprise they are dealing with has taken all the necessary precautions to maintain security.

In most countries, government and industry regulations have been or are being implemented to ensure enterprises have specific security mechanisms in place to protect user privacy. For example:

- **ISO 27002**, the information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining Information Security Management Systems (ISMS).

<sup>3</sup> "Emerging Cyber Threats Report for 2009," Georgia Tech Information Security Center, October 2008.

- *Alcatel-Lucent Bell Labs* developed ITU-T X.805 and ISO 17799/27001 security architecture for systems providing end-to-end communications. It provides a comprehensive, multilayered, end-to-end network security framework across eight security dimensions in order to combat network security threats.
- The *Payment Card Industry Data Security Standard (PCI DSS)* outlines a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures intended to help organizations protect customer account data.
- The *Control Objectives for Information and related Technology (COBIT)* is a framework for IT management created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). It outlines accepted measures, indicators, processes and best practices that help organizations use IT and develop IT governance and control.
- The *Health Insurance Portability and Accountability Act (HIPAA)* enacted by U.S. Congress in 1996 provides a set of standards for electronic health care transactions for health care providers, insurance companies, and employers that are designed to keep health care information private and secure.
- The *Family Educational Rights and Privacy Act (FERPA)* is a U.S. law that requires U.S. educational agencies to provide students with access to their education records and governs how state agencies transmit testing data to federal agencies.

These and other regulations make it necessary for enterprise IT teams to ensure their organization is secure for their own employees, as well as anyone else who connects and interacts with it. As noted by Gartner in a recent report:

*“... privacy protection goes beyond the installation of technologies. Organizations must implement efficient incident-response processes, maintain enterprise-specific employee and customer privacy policies, and ensure that privacy-related controls are included in all contracts with business partners, external service providers, and other third parties. Extending such controls to software-as-a-service (SaaS) offerings and services that are delivered in the Cloud will be a particular challenge in 2009 and beyond.”<sup>4</sup>*

### Three enterprise security requirements

With new threats and regulations arriving on the landscape coupled with new business models, emerging technologies and an increasingly mobile workforce, the enterprise security challenge can be seen from three perspectives: managing risk, protecting data and managing costs.

- Managing risk requires enterprises to be prepared for new, more sophisticated threats that can occur anytime and from anywhere. It also requires enterprises to be able to evaluate and adjust enterprise security risk profiles and be compliant with standards and regulations.
- Protecting data includes managing data flow to third parties and the Cloud, protecting mobile data and preventing internal fraud and information breaches.
- Controlling cost requires removing security-imposed productivity barriers, improving security with constrained budgets across existing infrastructure investments, and coordinated enterprise-wide security management.

These requirements present a daunting security challenge for the enterprise Chief Information Officer (CIO) who must ensure the enterprise, its customers, partners and suppliers are all secure.

<sup>4</sup> “Top Five Issues and Research Agenda, 2009-2010: The Privacy Officer,” Gartner, May 2009.

## A Fresh Perspective on Enterprise Security

---

To date, security teams have focused on building network perimeters and securing each application individually to mixed success. IT departments have spent a lot of time and effort on a defensive and perimeter-centric approach to keep cyber criminals and malware off of the enterprise network. Importantly, sometimes these security-related efforts have made it more difficult for employees to do their jobs and for the enterprise to be competitive.

The reality of current approaches to application security is that any one application alone does not have a complete picture of what a user is attempting to do while connected to the corporate network. Therefore, despite all the efforts to build security into applications there are still many breaches.

In addition, despite all of the industry standardization around security for applications and networks, the operational side of security carries large costs and still leaves large gaps for many enterprises, especially when the need to be compliant with new pieces of legislation is factored into the mix.

To get the maximum return on their security investment, enterprises need a fresh perspective on enterprise security for it to be effective. Enterprises must adapt their security to protect both the network infrastructure and their end users with user-centric security delivered from within the network.

By approaching security in this way, an enterprise can make security more dynamic. It can ensure security mechanisms constantly evolve and adopt new mechanisms to protect the enterprise against new threats that continue to emerge at an ever-increasing rate. And it can ensure that as security events occur, the security infrastructure can make automatic adjustments to policy that can significantly reduce security risks in the future.

With user-centric security enterprises can also retain a level of openness. They can ensure business processes are able to function as efficiently as possible because security does not get in the way of the users. This also means that the interfaces are open and enable secure connections with cloud computing platforms, with Web 2.0 platforms and with external business partners, whenever required.

With user-centric security a dynamic enterprise becomes a trusted, dynamic enterprise for:

- *Employees*, by surrounding them with security to ensure they are protected and enabled to carry out their expected role efficiently
- *Business partners*, by ensuring all information and shared business processes are secured so they can be sure the risk they take in “connecting electronically” with the enterprise is minimized
- *Customers*, by ensuring all private information will remain secure and thereby minimizing the risk of doing business with the enterprise

To make a dynamic enterprise secure, enterprises must change how they view, adopt and measure security. They must view security as a positive enabler and a dynamic, integral part of the enterprise with a focus on managing risk, protecting data and controlling cost, rather than as a static add-on.

Managing risk ensures reduced risk of external intrusion and Internet-based attacks with always-on, persistent security, increased visibility on enterprise security risk profiles, and demonstrated and enforced compliance.

Protecting data delivers a controlled information flow and non-repudiation for transactions with security extended to remote and mobile workers, and preempted internal fraud and information breaches.

Controlled costs bring improved productivity with transparent security, enabling improved access to information and services, enhanced security that leverages existing infrastructure, and reduced security operations costs with centralized management.

The end result is a trusted, dynamic enterprise with open and secure interfaces to communications, data and services that enable an enterprise to take advantage of new collaborative business models. The enterprise is protected against new threats, protects private data and complies with governance requirements.

## The User-Centric Security Blueprint

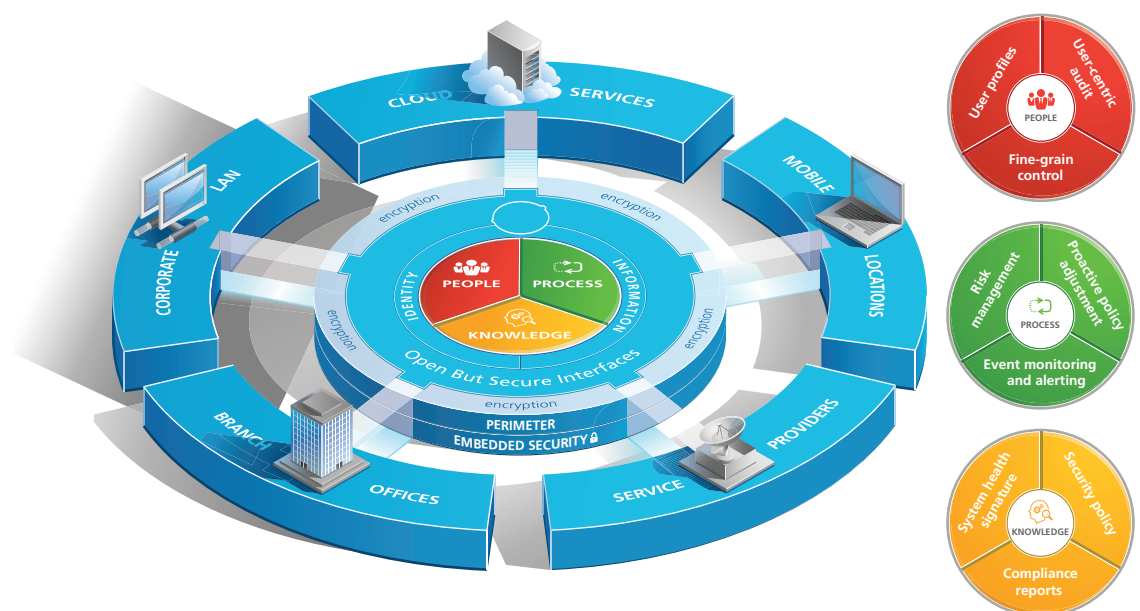
A user-centric security blueprint can enable the transformation to a trusted, dynamic enterprise. It ensures efficiency for enterprises as they make this transformation by taking advantage of the latest security solutions to drive business performance. At the same time, enterprises manage risk, protect private data and are compliant. With the blueprint, enterprises can satisfy the demands of employees, business partners, and customers for always-on, always available voice and data applications that can be accessed from anywhere and at any time.

The blueprint looks at security for the enterprise as being delivered from within the network to protect across networks, people, processes and knowledge. Following the blueprint allows the enterprise to benefit from:

- A *network* that is user-aware and provides security for voice, data and mobility, and enables compliance with policy enforcement and audit
- *People* securely collaborating across organizational boundaries, leveraging business-to-business relationships, Web 2.0, and cloud computing without security-imposed human productivity barriers
- *Processes* that are agile, automated and secured with always-on security
- *Knowledge* in the form of private data that is protected, and any knowledge sharing that is secured

The user-centric security blueprint prescribes a global, corporate-wide security infrastructure that provides a consistent and corporate-wide application of security. At the same time it includes the separation of security from endpoints and applications, and development of an independent chain of control for security, regardless of the endpoints to be protected. Most importantly, it mandates always-on and highly available security that is transparent to the end user. Figure 2 offers a visual representation of the user-centric security blueprint that achieves these objectives.

Figure 2. User-centric security blueprint for the trusted, dynamic enterprise



The user-centric security blueprint for transforming to a trusted, dynamic enterprise is intended for enterprises of all sizes. It covers the need for security to extend beyond the physical borders of each enterprise site as enterprise perimeters become virtualized. Enterprise security must enable a secured internal environment for the global enterprise that connects all sites and includes secured access to service providers, cloud-based services, and remote locations visited by employees. This blueprint describes the elements required to:

- Secure the voice and data fabric of the network given new requirements for security
- Truly empower the employees of the enterprise to maximize productivity
- Drive down the cost of securing the enterprise
- Deliver the information concerning security that must be managed

## **Network**

Security starts with protecting the voice and data fabric and ensuring that a proper perimeter is in place. This perimeter must include the traditional elements, such as IP firewall, virtual private network (VPN) and threat management. Recognizing that the perimeter is becoming virtualized will require a migration to security based on identity and to protect the information content of each message. With the move to include identity-based protection for the content of each message, the ability to encrypt and sign message content, maintain chain of custody, and ensure non-repudiation becomes feasible.

In many cases today, security is added to the voice and data fabric mostly as an overlay. As networks evolve in the coming years, security will become increasingly embedded into the network devices themselves where functionality such as being able to identify a user and set access rights will be done by the switching fabric interfacing directly with identity management platforms. Moving forward, this migration of security functionality into network devices has the potential to improve security because it will be delivered closer to the first point of contact the user makes with the network and because it also reduces the cost of security.

This evolution of network security is a critical step to providing the security required to allow for open but secure interfaces to connect to branch offices, with the Cloud, to external business partners, external service providers and with mobile employees.

## **People**

Protecting people in an enterprise starts with enabling the network to deliver fine-grain control and enabling people to carry out their duties without tripping over the security system. Fine-grain controls are dependent on user profiles (or roles) and policies that indicate expected acceptable behavior for individuals. These network resident platforms typically interface with existing identity management platforms.

From the perspective of protecting people from queries about their activity, the enterprise must have a comprehensive audit capability in place that can be used to demonstrate that users have acted according to policy and the enterprise is compliant with regulations. Again this functionality should be delivered by taking advantage of the unique perch point of the network to ensure all activity is captured no matter where it occurs within the enterprise.

## **Process**

The operational process of delivering security is required to drive efficiency by ensuring key enterprise-wide platforms are in place for risk management dashboarding, event monitoring and alerting. Risk management platforms fed with data from networked devices across the enterprise provide comprehensive dashboards on the current risk profile of the enterprise. They allow the organization to assess and adapt current security policy to adjust the balance between enabling the enterprise to function

efficiently and mitigating risk. Event monitoring and alarm platforms also fed with data from networked devices are critical to ensuring security-related events occurring across the corporation are visible and tracked, and that alarms are raised if certain events require immediate attention.

A new dimension to be included in the process of delivering enterprise security is the ability for security systems to be proactive and adjust policy at run time. This allows for the automatic reduction of the current risk profile of the enterprise based upon events that impact security and a current state vector. It can include the occurrence of particular security events, capturing the context of user and machine activity, as well as environmental conditions, such as time of day.

### **Knowledge**

The knowledge concerning security that an enterprise must maintain, protect, and ensure visibility and consistency across the enterprise includes security policy, compliance reports and system health check signatures. Security policy governs the functioning of all aspects of the enterprise, compliance reports must be ready to be produced on demand, and system health signatures reflect the “gold” standard that each device was configured to when originally connected to the network. Having platforms that manage security policy and ensure that the policy is visible and consistent across the entire organization is central to the transformation of an enterprise and enables individuals to drive business performance and manage risk.

Efficiently creating compliance reports that are safely stored until needed to demonstrate compliance with regulations can directly impact operation costs for securing the enterprise, especially when an audit is requested. System health check data leverages the X.805 standard for measuring the level of security achieved by an organization to enable periodic verification that all devices on the network are still configured closely enough to their original configuration to be trusted to be connected to the network. This is used to control drift of device configuration that can naturally occur in production environments.

## **Applying the Blueprint**

---

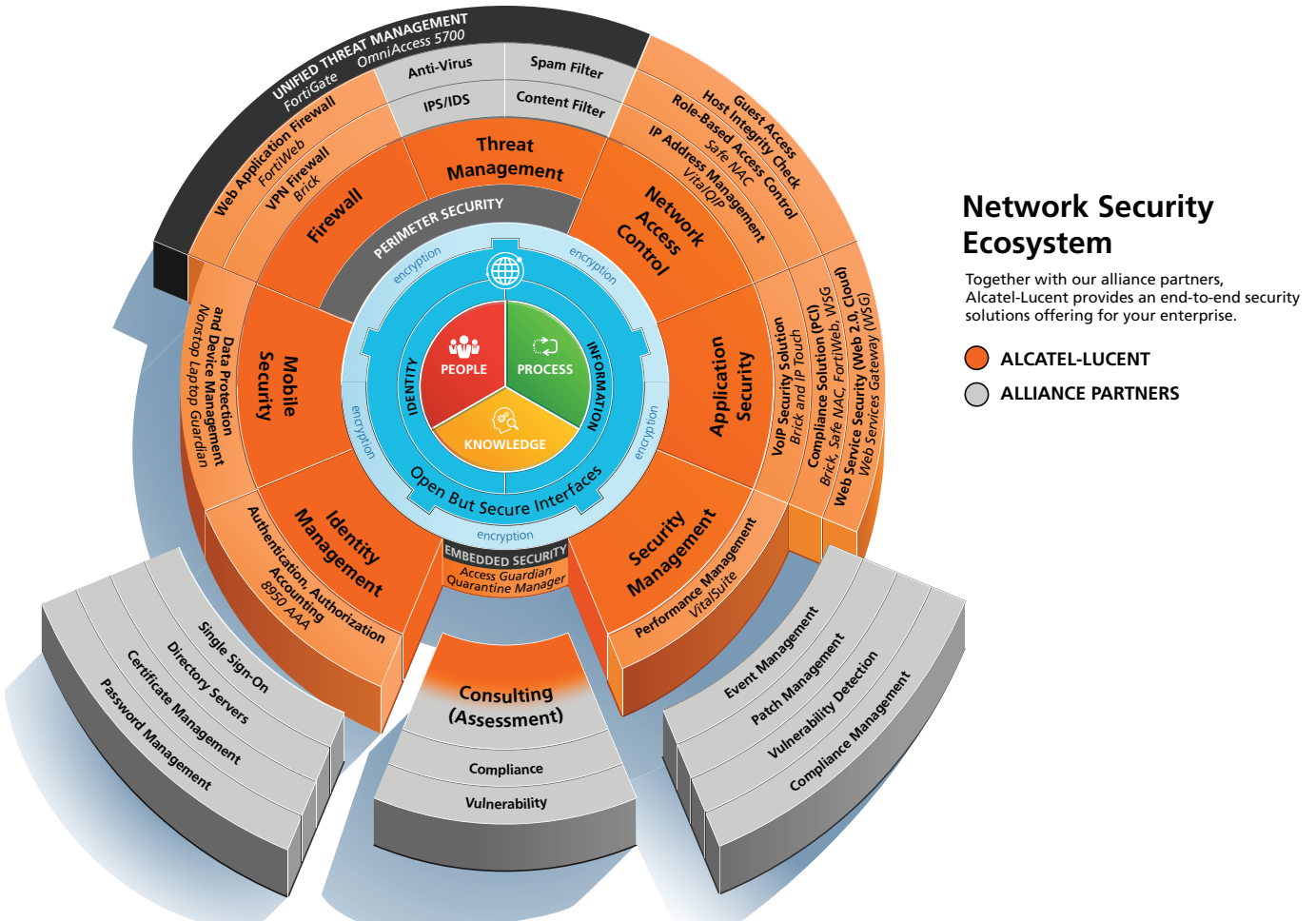
By following the user centric security blueprint, enterprises will be positioned to leverage new business models made possible by Web 2.0, cloud computing and mobile communications technology. They will also be able to continually evolve to respond to new and increasingly sophisticated security threats, the growth of cybercrime and the introduction of new regulations.

Applying this security blueprint for a trusted, dynamic enterprise requires an end-to-end approach to security. Enterprises must move beyond looking at point solutions that address specific security requirements for one area of the enterprise, to integrated solutions that enable the user-centric security blueprint. Figure 3 offers a visual representation of the solution map that achieves these objectives.

Deploying solutions to follow the user centric security blueprint requires gaining an understanding of what perimeter security exist in the enterprise and how it must be augmented to ensure there are the required open but secure interfaces in place protected by proper encryption to allow for virtualization of the enterprise perimeter. Along the path laid out by the blueprint, the next step is to examine the need for network access control solutions that ensure adequate controls are in place. This allows the user and/or a device onto the network and also, if needed, fine-grain controls that enable users to access the network resources and applications they need. Again referring back to the blueprint — we can see that the fine-grain control delivered by network access control (NAC) is dependent upon the deployment of an enterprise-wide identity management solution.

With the voice and data fabric secured and appropriate fine-grain controls in place, the next consideration is security directly targeting specific applications that require extra special treatment. This is followed by solutions to protect the mobile user and mobile assets of the corporation such as laptops. Finally, the requirement to allow the enterprise to manage risk, handle security-related events dictate the need for security management solutions.

Figure 3. Solution roadmap to deploy user-centric security



### Perimeter security

Choosing a perimeter security solution usually means different choices for various types of enterprises and is also dependent upon security strategy. If an enterprise prefers to follow a best-of-breed approach to threat management, then separate solutions are required for firewall/VPN, anti-virus, anti-malware and web filtering. If an integrated approach to threat management is preferred then a unified threat management and firewall solution is attractive. If an enterprise has many independent branch offices, an integrated solution which includes routing functionality, referred to as a security router, is an approach to be considered.

In today's network, a web application firewall is a must to protect web servers and web-facing applications. One overall consideration in controlling security operations costs is scalability and manageability of the perimeter solution chosen, especially for enterprises with many locations to protect.

## **Network access control**

Network access control can be achieved by looking for comprehensive solutions that meet current and future business needs for providing controlled access to guests, partners and contractors while ensuring each device that connects to the LAN is configured as required and enables the enterprise to meet compliance requirements. A comprehensive NAC solution starts with robust IP address management that offers a pure ability to provide an address to devices connected to the network, followed by an authentication to determine access privileges and a host integrity check to ensure that it is safe to allow a device on the network, concluding with role-based access control for ensuring compliance.

Host integrity check solutions will determine if a device is configured according to enterprise policy and that it contains no malware before the device is allowed onto the network. It is a must in any wireless environment where users connect devices to the network at will. Enterprises that have a stringent need to protect certain servers and applications or are in highly regulated industries, should consider solutions that provide user-aware network controls for secured role-based access to resources with audit. These solutions can be deployed without the need to reconfigure networks on a physical level to achieve security requirements.

## **Identity management**

Identity management is central to user-centric security and starts with an enterprise-wide password management platform and directory server farm. Many organizations today will consider the move to some form of strong authentication based on certificates coupled with two factor identification of end users and devices. Providing a rich set of interface and control points to the voice and data fabric of the enterprise is key to the deployment of an Authentication, Authorization and Accounting (AAA) infrastructure.

Of course, an enterprise-wide single sign-on capability is also important to providing an internal secured environment for enabling employees. With the move to Web 2.0 and cloud computing the addition of a federated identity management capability may be necessary.

## **Application security**

The deployment of new applications such as VoIP, the adoption of new business models leveraging the Web 2.0 and the Cloud, and new compliance regulations create the need for security solutions that protect user activity with an understanding for the application being used by the end user.

With the deployment of VoIP, it is important that the enterprise security in place can ensure that the new virtualized perimeter defense and possibly encryption requirements for VoIP are met.

In the case of Web 2.0 and the Cloud, solutions that secure individual Web services and can act as a trusted intermediary with the Cloud are becoming a must-have for protecting enterprises. Solutions ensuring enterprises are compliant with regulations in the processing of monetary transactions and controlling the cost of being compliant are important to many enterprises.

## **Mobile security**

Many enterprises today have employees that spend much of their working hours outside the enterprise perimeter using mobile computing devices such as laptops. Solutions for securing the mobile laptop must address the concern of private information that is stored on them being lost or stolen and also address the need to be able to manage the laptops at any time.

## **Security management**

Security management requires a number of platform choices covering performance and event management, patch management, vulnerability detection and compliance management. Solutions deployed for performance and event management must be install-able in a global enterprise, collect a rich set of data from the voice and data fabric, and provide a robust event response and escalation engine.

Solutions for patch management should be able to integrate with enterprise platforms that manage mobility.

Solutions for compliance management must be able to provide proper dashboards for the current set of regulations, be expandable to include new legislation, and also be able to carry out run-time monitoring of end-user access to any corporate documents and applications.

## Conclusion

---

It is important for enterprises to follow a security blueprint to ensure efficiency as they transform themselves into a trusted, dynamic enterprise. A trusted, dynamic enterprise takes advantage of the latest security solutions to drive business performance while managing risk, protecting private data and controlling costs. With a security blueprint, enterprises will be positioned to leverage new business models made possible by Web 2.0, cloud computing and mobile communications technology. They will satisfy the demands of employees, business partners, and customers for always-on, always-available voice and data applications that can be accessed from anywhere and at any time. They will also be able to continually evolve to respond to new and increasingly sophisticated security threats, the growth of cybercrime and the introduction of new regulations.

Alcatel-Lucent provides the security blueprint and a complete suite of security solutions for becoming a trusted, dynamic enterprise that will be open for business and provide a trusted environment. The Alcatel-Lucent security blueprint leverages its Bell Labs innovation and carrier-class roots to provide a strategy for enterprises to deploy user-centric security, delivered from within the network that drives greater business performance. This security blueprint is based on experience securing carrier networks and a complete understanding of the network and multiple deployment models worldwide (Web 2.0, Cloud).

The Alcatel-Lucent security blueprint provides:

- A global, corporate-wide security infrastructure
- Consistent and corporate-wide application of security (voice, data, mobility)
- Security delivered separately from endpoints and applications
- An independent chain of control for security
- Security that is transparent to the user
- Always-on and highly available security

With the Alcatel-Lucent security blueprint, enterprises enable a trusted web experience for all their end users by combining the trusted capabilities of their network with the creative communications services of the Web (Web 2.0, Cloud and beyond). In this way they enable secure, private, and quality enterprise communications from any device at any time.

## Acronyms

---

AAA	Authentication, Authorization and Accounting
CIO	Chief Information Officer
COBIT	Control Objectives for Information and related Technology
DoS	Denial of Service
FERPA	Family Educational Rights and Privacy Act
HIPAA	Health Insurance Portability and Accountability Act
ISMS	Information Security Management Systems
PCI DSS	Payment Card Industry Data Security Standard
SaaS	software-as-a-service
VoIP	Voice over IP
VPN	virtual private network



**[www.alcatel-lucent.com](http://www.alcatel-lucent.com)** Alcatel, Lucent, Alcatel-Lucent and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Alcatel-Lucent assumes no responsibility for inaccuracies contained herein. Copyright © 2010 Alcatel-Lucent. All rights reserved. EPG3310091205 (01)