

SECURITY CONNECTED: OPTIMIZE YOUR BUSINESS

Top 10 security topics every
executive should know

10

SECURITY CONNECTED REFERENCE ARCHITECTURE

LEVEL

1

2

3

4

5

Attack Categories:

1. Opportunistic Attacks
2. Targeted Attacks

Trends:

3. Protecting Virtualized Environments
4. Enabling the Consumerization of IT
5. Leveraging Cloud Technologies Securely
6. Facilitating Safe Web 2.0
7. Protecting Information
8. Securing the Modern Data Center

Priorities:

9. Security Alignment as a Business Enabler
10. Reducing Complexity and Chaos While Achieving Connectedness

INTRODUCTION

Top 10 Topics

Organizations are constantly and rapidly evolving. According to a recent Gartner report, CIOs are transitioning from managing resources to demonstrating value in business terms. Gartner's *2011 CIO Agenda Survey* noted that by 2014, CIOs say their focus will move from process improvement and reducing enterprise costs to enterprise growth, improving operations, and attracting and retaining new customers. Supporting and enabling both business and security must be an integral component of a CIO's overall IT strategy.

In parallel, the threat landscape is changing faster than most IT organizations can cope with. The delicate balance of enabling the business and keeping it secure requires executives to stay informed about these changes so that they can consider them when making decisions. This guide was created to educate and inform. It is based on feedback from McAfee customers across various government and commercial organizations around the globe. This is not an exhaustive analysis of each of the 10 topics, but rather a short synopsis of the topics, various use cases, key concepts, and references to our Security Connected Reference Architecture that provide details on solutions, technology modules, best practices, and implementation guides.

The Security Connected approach from McAfee is a framework for integrating multiple products, services, and partnerships to provide centralized, efficient, and effective risk mitigation. With more than two decades of experience, we continue to help organizations of all sizes, all segments, and across all geographies increase their security posture, optimize security for greater cost effectiveness, and align security strategically with business initiatives. The Security Connected approach from McAfee delivers security that provides ubiquitous protection for your IT infrastructure.

1

THREATS

Opportunistic Attacks



The new school of malware and bots is very application-centric. To understand the gravity of the situation, consider Facebook, with more than 350,000 applications, Apple iPhones, with more than 100,000, and the introduction of HTML 5 as a vehicle to further blur the line between local and remote applications.

In the nineteenth century, the Industrial Revolution accelerated and advanced methods of assembly from single to mass production. Similarly, today's cybercriminals have matured and are now using automation to develop more profitable and sophisticated cybercriminal (or hacking) activities more rapidly. These opportunistic attacks are organized and almost always financially motivated. In many cases, the groups mounting these attacks have more than a decade of experience, long-term criminal relationships, and trust networks. Their roles have become specialized to promote scalability. Some examples of these specialized roles include carders, malware developers, botnet herders, spammers, money launders, and document forgers.

Many of the opportunistic bots attempt to steal data like credit card information or personally identifiable information. If there is nothing of value on the target system, at minimum, the victim will become an unwitting member of the botnet herd and be used to further distribute malware, spam, and distributed denial-of-service (DDoS) attacks. To maximize range, anonymity, efficiency, and effectiveness, many of these attackers will use bots to exploit how search engines operate so that popular searches will result in malicious pages being served up to unsuspecting users. This is called black hat search engine optimization. For example, the top five most dangerous celebrity searches of 2010 that are most likely to result in malware that exploits web browser or similar application vulnerabilities are: Cameron Diaz, Julia Roberts, Jessica Biel, Gisele Bündchen, and Brad Pitt. It doesn't matter if it is one individual or a multinational organization; if there are assets online, they will be targeted. It's not personal—it's just business.

Use Cases	Key Concepts
<ul style="list-style-type: none">• Spear-phishing and spam• Distributing malware	<ul style="list-style-type: none">• Most opportunistic attacks are profit driven• Bots have seemingly unlimited bandwidth and computing resources. For example the malware "Conficker" infected more than 6.4 million systems across 230 countries with greater aggregate processing power and bandwidth than Amazon and Google combined
<ul style="list-style-type: none">• Disrupting service with DDoS	<ul style="list-style-type: none">• Attackers have had more than a decade to mature their business model, develop trust networks, and create specialization of skills
Security Connected Reference Architecture Level 2 Topics to Consider	
<ul style="list-style-type: none">• Protecting Information• Protecting the Data Center	

2

THREATS Targeted Attacks



Targeted attacks have resulted in media censorship, organizations going bankrupt, billions in intellectual property being stolen, and military campaigns that blended kinetic and non-kinetic warfare techniques for tactical advantage.

Targeted attacks have taken on many different forms that are highly automated, low, and slow, leveraging device tampering to gain access or information and combining social engineering components. Perpetrators of these types of attacks are on a mission. While targeted attacks encompass so much more than sabotage or surveillance, they are often associated with espionage, and, as such, the concept predates the digital era and can be traced back to the earliest documentation of intelligence gathering recorded by military strategists, including Sun-Tzu and Chanakya. Targeted attacks have received significant media coverage. This is, in part, because of a series of cyberattacks dubbed Operation Aurora, Night Dragon, Shady Rat, and Stuxnet. These targeted attacks, while not always highly sophisticated, were focused, stealthy, and designed for long-term manipulation of their targets. Targeted attacks need only be as advanced as the target requires; in many cases spear-phishing and SQL injection attacks act as the attack vectors.

Use Cases	Key Concepts
<ul style="list-style-type: none">Stealing commercial secretsStealing government secrets	<ul style="list-style-type: none">Targeted attacks are most often driven by economics or politics
<ul style="list-style-type: none">Sabotaging critical infrastructure assets	<ul style="list-style-type: none">Behind the attacks are motivated and often well-funded attackers, generally associated with nation-states and or their supporters, their competitors, organized crime, activists, and possibly even terroristsThey seek to maintain stealth and access over long periods of time
Security Connected Reference Architecture Level 2 Topics to Consider	
<ul style="list-style-type: none">Protecting InformationProtecting the Data Center	

3

TRENDS

Protecting Virtualized Environments



A virtualized machine was originally defined by Popek and Goldberg as “an efficient, isolated duplicate of a real machine.” This includes security bugs and all. Virtualization doesn’t equal security.

Virtualization and virtualized machines (VMs) have become a force in the industry. There are a few primary vendors of virtualized desktops and servers and more entering the market that are solving unique challenges created by virtualized environments. In addition, many companies are starting to look at virtualization services delivered via the cloud. The driving forces behind virtualization include lower hardware costs, better system administration, and reduced power consumption (green computing, reduced physical space, and other advantages). While virtualization is still a relatively new technology, it is being broadly adopted by many industries. The business benefits of these new platforms often overshadow the concerns of security professionals. However, there is a misperception that because a solution is virtualized, it is secure—and this is simply not the case. And, there is another misconception that adding layers of security will reduce the performance/capacity available in virtualized environments. The takeaway is this: the same considerations that are applied to physical systems need to be applied to virtualized ones while taking into account the operating environment adjustments.

Use Cases	Key Concepts
<ul style="list-style-type: none">Protecting online and offline VMs	<ul style="list-style-type: none">VMs are dynamic; they are brought up and down and frequently moved, making security standardization difficult
<ul style="list-style-type: none">Protecting hypervisors from attack	<ul style="list-style-type: none">Hypervisors will be targeted just like any common operating system, but threats can also come through virtualization solution consoles and management applications
<ul style="list-style-type: none">Protecting guest VMs from attacks; other VMs or external systems	<ul style="list-style-type: none">VM security can be achieved that does not hinder the operational efficiencies of virtualization

Security Connected Reference Architecture Level 2 Topics to Consider

- Securing Mobile Devices
- Enabling Consumerization of the Workforce

4

TRENDS Enabling the Consumerization of IT



“Consumer IT will affect every enterprise,” said David Mitchell Smith, vice president and Gartner Fellow. “Attempts by enterprises to deny this are doomed to failure, just as previous attempts to deny Wi-Fi, ‘smart’ mobile phones, the Internet, and even the PC itself failed.”

Imagine an office without Internet access, email, the web, or even computers. Imagine not having printers or telephones. Most businesses simply wouldn't be able to operate. As technology has advanced and become more affordable, individuals are finding that their personal technology solutions, which appear in the consumer market first, are powerful enough and versatile enough for business use. In many cases, they are actually more powerful and less expensive. As such, the division between IT and consumer electronics devices that employees feel they need to conduct business has become blurred. This has resulted in explosive growth in the use of personal technology for business—laptops, tablets, smartphones, MP3 players, and USB storage devices. A very common question is: “How can we protect our assets and intellectual property when employees are connecting personal devices?”

Use Cases	Key Concepts
<ul style="list-style-type: none">• Allowing employee flexibility—while minimizing business risks	<ul style="list-style-type: none">• The smartphone is here to stay, and be prepared to support many other types of devices and tablet. In 2010 alone, more than 35 different types of tablets were introduced into the market, and their rapid adoption rate in business is evident in airports and offices around the world.
<ul style="list-style-type: none">• Leveraging the power that consumer electronics can introduce into the workplace	<ul style="list-style-type: none">• Users cite great efficiencies with consumer electronics and ability to work more readily
<ul style="list-style-type: none">• Protecting sensitive data on mobile devices, in particular, smartphones	<ul style="list-style-type: none">• While the consumerization of IT is a somewhat new concept, the security controls for mitigating risks associated with consumer devices already exist

Security Connected Reference Architecture Level 2 Topics to Consider

- Securing Mobile Devices
- Enabling Consumerization of the Workforce

5

TRENDS

Leveraging Cloud Technologies Securely



Cloud computing is one of the fastest growing segments in information technology. Enterprises of all sizes are looking to cloud computing as a way to increase business agility and drive cost efficiencies. Organizations are attracted to the prospect of accelerating their ability to use business applications like email and customer relationship management (CRM) or leveraging an infrastructure with greater resources than they have in house at a reduced cost. The cloud, however, has had some high-profile security vulnerabilities and service failures such as: the Google App Engine crash, Gmail outages, network device failures shutting thousands out of Salesforce.com's Software-as-a-Service (SaaS) applications, and similar issues with Apple, Yahoo, and Amazon.

Two major barriers to cloud adoption for the 1,500 enterprises surveyed by IDG Enterprise Cloud Computing Research, Nov 2010 were:

- *Security—67 percent cited it as a concern, including risk of unauthorized access, being able to maintain data integrity, and data protection*
- *Access to information—41 percent were concerned about being able to preserve a uniform set of access privileges across cloud apps*

Use Cases	Key Concepts
• Embracing SaaS	• Identify where your data lives, what systems it traverses as part of the service delivery, and where it is stored and archived
• Leveraging outsourced data center or infrastructure as a service	• Know who will have physical and logical administration rights for both production and failover scenarios
• Extending the conventional data center	• Understand how you will monitor network, system, and data assets

Security Connected Reference Architecture Level 2 Topics to Consider

- Protecting the Data Center
- Securing Cloud Applications

6

TRENDS Facilitating Safe Web 2.0



“The Internet is the first thing that humanity has built that humanity doesn’t understand; the largest experiment in anarchy that we have ever had.”

—Eric E. Schmidt
Chairman of the Board
and CEO Google

Facebook is the most popular site on the Internet, and other social networking and Web 2.0 solutions aren’t far behind. Companies of every size are finding new routes to market or new ways to expand their business using web applications. Employees and organizations are leveraging Web 2.0 capabilities for personal and business use. It’s not that dissimilar to the early days of email and web browsers. Blocking access is a temporary fix at best—eventually people will require access and/or find ways around the controls. Organizations must strike a balance between an effective and agile workforce and effective security controls and policies. Existing security solutions might not be able to address the problem; managing the problem across multiple vendors can be highly complex, require manual effort, and be error prone. Attracting and retaining employees may be difficult with policies that are too strict.

Business opportunities may be missed because of an overly cautious approach. But a lack of security controls could introduce individuals and organizations to threats such as malware.

Use Cases

- Controlling application access, downloads, and posts
- Being agile enough to allow employees, customers, and partners to take advantage of Web 2.0 solutions securely

Key Concepts

- Web 2.0 solutions are becoming as common and important as email and web browsers
- Blocking the use of Web 2.0 is a short-term fix at best

Security Connected Reference Architecture Level 2 Topics to Consider

- Securely Enabling Social Media
- Enabling Consumerization of the Workforce

7

TRENDS

Protecting Information



"All life is the management of risk, not its elimination."

—Walter Wriston
Former Chairmand and
CEO of Citicorp

Data protection has become one of the most critical aspects of an effective security strategy. Regulated information related to financial records, health records, and sensitive data is highly valuable. It is the object of desire for insiders, opportunistic attackers, and targeted attacks motivated by profit or politics. Traditional network security controls alone don't provide adequate protection; purpose-built solutions able to protect data at rest, in motion, and in use are needed. These solutions must span transaction points such as applications and databases and endpoints such as file servers, laptops, and mobile devices. They must also monitor how this data is being accessed and the behavior of those using it. This monitoring reveals how data is being moved across the network.

Data protection cannot be effective if it operates in a silo. Uniting data protection across all transports and enforcement technologies is mutually beneficial. By leveraging these controls in a coordinated way, situational awareness becomes more vivid as blind spots left by one control are filled in by another, elevating the overall security posture of the organization. Organizations are able to make more informed decisions more rapidly because they have empirical evidence of nefarious activity across data and networks. The right data protection solution can provide quick answers to these difficult questions:

- Where is the data that needs protection?
- Who has access to it?
- How is the data used?
- Who else is involved, what else might be happening, and how long has this been occurring?

Use Cases

- Protecting sensitive data from careless and malicious activity while securing access
- Gaining rapid insight into data and network risks while demonstrating compliance

Key Concepts

- Effective data protection must transcend data at rest, in motion, and in use across applications and databases, endpoints, and mobile devices
- One of the most valuable results of uniting data and network controls is the ability to generate a complete understanding of how users are interacting with data

Security Connected Reference Architecture Level 2 Topics to Consider

- Protecting Information
- Protecting the Data Center
- Controlling and Monitoring Change

8

TRENDS

Securing the Modern Data Center



“Four top reasons behind a company’s plans to upgrade their data center are: improving availability/uptime, reducing risk, flexibility to respond to changing market conditions, and improved security.”

—Network World survey on behalf of McAfee and Brocade, March 2011

Data centers run organizations. Generating revenue, storing sensitive data, and providing business-critical services are just a few of their roles. Because of their criticality and value, they are targets. Sensitive data, business applications, databases, network devices, storage, and supporting infrastructure have all long been in the crosshairs of external and internal attackers as well as auditors armed with regulatory mandates.

Virtually every data center security issue and regulatory mandate has spawned a point solution. This reactive process, where new point solutions are added at every turn, has resulted in data center controls that are complex, numerous, expensive, and disconnected, thus overwhelming most organizations. In addition to existing requirements, new threats and trends are continually entering the fray. For example, organizations are requiring their data centers to support mobility and Web 2.0, provide protection against targeted and opportunistic attacks, and do all this while minimizing downtime and producing frequent reports for demonstrating compliance.

Classic data center security lacks the business agility for quickly and seamlessly embracing new requirements, the security management for efficiencies and effectiveness, the availability and integrity necessary for today’s mission-critical operations, and the optimized design for cost effectiveness. Data centers have evolved to be more mission-critical than ever. Today’s IT departments are blazing new trails. We can only speculate about the next “big thing” five years out, but if the last five years are any measure, what we thought made us secure isn’t going to keep us secure. A strategic framework is needed that helps connect the historically disparate pieces.

Use Cases	Key Concepts
<ul style="list-style-type: none">• Embracing data center trends including consolidation, virtualization, and the cloud	<ul style="list-style-type: none">• The complexity of data center operations must be reduced in order to achieve reduced risk and higher levels of efficiency
<ul style="list-style-type: none">• Protecting sensitive data within the data center while optimizing operations	<ul style="list-style-type: none">• Data center architectures must be built atop a flexible framework that can facilitate new trends such as the consumerization of IT, mobile computing, virtual environments, and the like—this flexibility will allow for more rapid adoption of these trends with minimal disruption while maximizing risk mitigation

Security Connected Reference Architecture Level 2 Topics to Consider

- Securing the Data Center
- Managing Security and Risk
- Enabling Consumerization of the Workforce

9

PRIORITIES

Security Alignment as a Business Enabler



A decade ago, thinking about security as a mechanism to impact business operations positively, act as a competitive differentiator, and enable new business initiatives was an academic debate at best. However, as threats have continued to mature, consumers and organizations alike have become more aware about the risks and are demanding elevated levels of security.

Consumers are not willing to give up the conveniences that the Internet, mobile devices, and Web 2.0 offer. But statistics have shown that customers now see security as one of their criteria when deciding to do business with an organization and that a data breach would be a compelling reason for them to terminate a business relationship.

“Opportunities are seldom labeled.”

—John A. Shedd
American author and professor

How does security enable business?

- It positively impacts business operations by enabling online business applications without sacrificing data integrity or confidentiality
- It acts as a competitive differentiator by allowing employees and customers to securely take advantage of mobile applications and Web 2.0 to interact with the business
- It enables new business initiatives by keeping sensitive data, such as customer information, new product releases, merger and acquisition activity, and marketing campaigns from leaking out through careless or malicious acts

Security Connected Reference Architecture Level 2 Topics to Consider

- Securing Mobile Devices
- Securely Enabling Social Media
- Securing Cloud Applications
- Enabling Consumerization of the Workforce

10

PRIORITIES

Reducing Complexity and Chaos While Achieving Connectedness



"To be simple is to be great."

—Ralph Waldo Emerson
American essayist and poet

Not so long ago, all you had to protect at your organization were stationary computing systems in designated physical locations. Today, you need security that protects a virtual network of people, data, applications, networks, and services, that can be anywhere at any given moment. Security needs to achieve the same ubiquity. In achieving this goal, perhaps the greatest enemy is complexity. Throwing one security solution on top of another in a disjointed fashion to address a particular security risk introduces complexity, often making the cure worse than the disease. The old model of defense in depth needs to be updated. A more thoughtful approach is required, one that optimizes the security investment resulting in improved risk profile and improved security at a reduced cost.

For years, security has been attempting to move into a more strategic role within IT and within overall business operations. This is nearly impossible when the standard operating procedure is to take a security threat and address it with a point solution. Now operational teams are called upon to address a growing number of threats using a growing number of disparate point solutions with the same or fewer security personnel.

With security experts pushing organizations to address network security, system security, data security, and compliance as part of a unified strategy, what can organizations do to reduce complexity to the point where this is operationally feasible and not just an academic argument? The answer is what McAfee calls the Security Connected framework. By centralizing traditionally disparate sources across multiple vendors, leveraging each source to enhance the other, and having commonality across all security countermeasures, complexity is minimized, operational efficiencies are maximized, and risk is reduced. This is analogous to an air traffic control system where extremely complicated and disparate information is aggregated and made actionable through a single pane of glass.

Security Connected Reference Architecture Level 2 Topics to Consider


- Protecting the Data Center
- Securing Mobile Devices

SUMMARY

Addressing threats, trends, and business priorities requires a connected security strategy that protects the ubiquity of your IT infrastructure. From opportunistic and targeted attacks to emerging technologies and leveraging security as a strategic business differentiator, having a connected security strategy that not only bridges the technology gaps, but also business priorities, can positively impact a business success in a competitive environment.

Many organizations will likely relate to several, if not most of these topics, but there are other very important subjects that have not been addressed. If you would like to discuss these and other related security topics to better understand our position and get more details about the Security Connected Reference Architecture from McAfee, please visit www.mcafee.com/securityconnected.

The Security Connected framework from McAfee enables integration of multiple products, services, and partnerships for centralized, efficient, and effective risk mitigation. Built on more than two decades of proven security practices, the Security Connected approach helps organizations of all sizes and segments—across all geographies—improve security postures, optimize security for greater cost effectiveness, and align security strategically with business initiatives. The Security Connected Reference Architecture provides a concrete path from ideas to implementation. Use it to adapt the Security Connected concepts to your unique risks, infrastructure, and business objectives. McAfee is relentlessly focused on finding new ways to keep our customers safe.



McAfee and the McAfee logo are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright © 2011 McAfee, Inc. 36502br_top-10-security_1011_wh



2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com