TOP 10
WHERE SECURITY-OBLIGATED EXECUTIVES SHOULD FOCUS

- 92% of data breaches perpetrated by outsiders
- 73% of all attacks
- 78% of initial intrusions based on low difficulty
- $100B in global data loss annually
- Process, secure, secure, optimize, prioritize
- Sustainable security
- Li.
“The power of computing has brought forth a digital age that values progress and innovation. As security-obligated executives, we must embrace this concept and understand our role in providing a safe environment for our businesses.”

—Security Battleground, an Executive Field Manual, by Michael Fey, Brian Kenyon, Kevin Reardon, Bradon Rogers, and Charles Ross

www.mcafee.com/securitybattleground

As the economy heals, IT organizations are shifting from process improvement designed to reduce costs to enabling enterprise growth, improving operations, and attracting and retaining new customers. In a recent Harvard Business Review blog, David Burrus said that today’s CIO needs to transform into the “chief innovation officer.” “The CIO’s role must shift from protecting and defending the status quo to embracing and extending new innovative capabilities.”

---

**SECURITY CONNECTED REFERENCE ARCHITECTURE**

<table>
<thead>
<tr>
<th>LEVEL</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
</table>

Introduction ................................................... 2
Targeted attacks ............................................. 4
Opportunistic attacks ....................................... 5
The case for information-centric security ............ 6
Scoping and shrinking the attack surface .......... 7
Real-time situational awareness ....................... 8
Coordinated threat analytics and active defenses . 9

The dynamic data center to cloud ..................... 10
Workers on the go: mobile, social, and business considerations ............................... 11
The Internet of Things: when technology proliferates ...................... 12
Sustainable security—prevention is no longer sufficient ......................... 13
Summary. .................................................... 14
This transformation depends on enabling unique business opportunities through technology and security. But with the threat landscape always changing, the delicate balance of enabling the business and keeping it secure requires that executives make smarter and more informed decisions.

Reactive and costly firefighting against security events, threats, and vulnerabilities just won’t cut it. Those strategies, at best, leave you with the status quo. To enable successful innovation, you need to transform your security systems to an adaptive, context-aware, synchronized security environment. That’s why we’ve created this guide.

Throughout this brief, we’ve bridged today’s big security ideas to a best practice framework: Security Connected from McAfee. Its guidance and reference architecture tools will help your organization improve your security posture, optimize your security for greater ROI, and align security strategically with business initiatives.
"Cyberrisk has moved from position 12 (malicious) and 19 (non-malicious) in 2011 to the world’s number three risk."
—Lloyds Risk Index 2013

Targeted attacks keep evolving, with more criminals, activists, and spies getting into and changing the rules of the game. Whether the means of attack is a quick spearphish for banking credentials, a distributed denial-of-service against your website, or a protracted effort to penetrate and persist inside your network, targeting is a key element of an increasing proportion of enterprise attacks.

Attackers first scout the target organization and its users looking for ways in. Recently, we have seen the exploitation of “watering holes” as the first entry point. Cybercrooks plant malware on a topical website visited by employees, such as a business partner’s web training page or a mobile developer forum. Just as they would with a phishing site, an attacker can secrete a keylogger, hidden iframe, or browser exploit on a watering hole and gain access to your employee’s computer.

As enterprises have grown more diligent in maintaining operating systems, attackers are leveraging vulnerabilities in other software, including databases, web servers, and browsers. For example, to deface or take down your website, scanning tools can find weaknesses in your website and its enabling technologies.

The initial vulnerability on a client or server provides a hiding place and access to valuable corporate data assets and critical user credentials. Next, attackers interested in more valuable treasures (or greater mayhem) may move laterally around the network looking for databases, setting up backdoors for persistent access, and compromising other assets.

<table>
<thead>
<tr>
<th>Examples</th>
<th>Key Concepts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft of secrets</td>
<td>Driven by economics or politics, the success of these exploits requires</td>
</tr>
<tr>
<td></td>
<td>exfiltration of data. Keep clients updated, protect data stores, and</td>
</tr>
<tr>
<td></td>
<td>monitor for suspicious network traffic.</td>
</tr>
<tr>
<td>Sabotage and business disruption</td>
<td>Advanced evasion techniques and zero-day vulnerabilities are often</td>
</tr>
<tr>
<td></td>
<td>required to penetrate e-commerce sites and enterprise networks, but</td>
</tr>
<tr>
<td></td>
<td>spies and hacktivists will pay that price.</td>
</tr>
<tr>
<td>Persistence</td>
<td>Attackers can use rootkits, malware that acts below the operating system,</td>
</tr>
<tr>
<td></td>
<td>to find a control point in a host. They then install hacker tools and</td>
</tr>
<tr>
<td></td>
<td>backdoors and embed themselves in other hosts.</td>
</tr>
</tbody>
</table>

For further reading, visit www.mcafee.com/securityconnected and download

- Neutralize Advanced Threats
- Achieve Continuous Monitoring
- Counter Stealth Malware
Today’s cybercriminals have decades of experience, long-term criminal relationships, and an extensive trust network. They develop profitable and sophisticated attacks rapidly and make full use of advances in cloud computing, mobility, and social media.

They’ve become specialists in various complementary criminal activities—carders, malware developers, botnet herders, phishers, money launderers, and certificate forgers. For instance, botnets are now a mature industry.

First, a compromised host is scanned for credit card information or marketable personally identifiable information. When there’s nothing of value on the target system, victims become unwitting members of the botnet, passing along malware and spam and participating in distributed denial-of-service (DDoS) attacks. Newly compromised bots enable criminals to avoid reputation-oriented defenses, as well as search engine algorithms. By keeping a low profile, criminal networks become more scalable and resilient.

While investing to detect and mitigate media-hyped targeted attacks, businesses must continue to combat the ever-present opportunistic ones.

“Internet-friendly content is a popular vehicle for malware, particularly common browser file types such as JPEG and QuickTime. In mid-2013, browser-based threats represented 73% of all attacks, up from 44% in Q1 2013.”

<table>
<thead>
<tr>
<th>Examples</th>
<th>Key Concepts</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Drive-by downloads and spam</td>
<td>Keyloggers and malware planted on web pages and publicized through email and social media help criminals collect vital data. Reputation can help defenses block malicious content, messages, and connections.</td>
</tr>
<tr>
<td>• Botnets</td>
<td>Vulnerable software leads to compromised hosts—bots. Use anti-malware as well as network filters that can block botnet communications.</td>
</tr>
<tr>
<td>• Ransomware</td>
<td>“Free” tools often lock users out of their systems and demand payment in order to unlock the drive or device. Prevent installation of unapproved applications.</td>
</tr>
</tbody>
</table>

For further reading, visit www.mcafee.com/securityconnected and download

• Protecting Information

• Protecting the Data Center
Information is vital to your business. Many companies are looking to harness the volume, velocity, and variety of data to get the most value from it. But data is everywhere and takes multiple forms. It’s at rest in your backup. It’s in motion as it travels around your network. And it’s being continually accessed and transformed through information sharing and collaboration among employees and with customers and partners. The ability to freely exchange data supports the goal of business innovation and growth.

Once we protected the perimeter. Then we protected predictable IT stacks. Now, as the cloud causes us to lose direct control over our systems and visibility into where our data lives, we need to adapt. Where is our most valued information? How can we find it given the volume of data being created? How do we track and protect it, given its variety? And how do we keep up, given the velocity of its creation and transformation?

The big new idea for many organizations will be finding the data reliably and continually—before it is at risk. Once found, tools like encryption and policy-based monitoring and prevention can help enable information-centric security.

“Information is the oxygen of the modern age. It seeps through the walls topped by barbed wire; it wafts across the electrified borders.”
—Ronald Reagan

### Examples

<table>
<thead>
<tr>
<th>Key Concepts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use tools to find rogue and managed devices on your network as well as sensitive and regulated data. Then use policies and encryption to manage interactions and enforce security standards.</td>
</tr>
<tr>
<td>More data protection regulations are looking at culpability in protecting data. Class action lawsuits are the reality of the aftermath of data breaches. Your ability to prove proper data handling and policy enforcement decreases risk.</td>
</tr>
<tr>
<td>Have tools to detect what social and Internet services are in use. Be alerted to the communication streams where data protection policies are being bypassed.</td>
</tr>
</tbody>
</table>

### For further reading

Visit [www.mcafee.com/securityconnected](http://www.mcafee.com/securityconnected) and download

- Protecting Information
“Malicious cyberactivity may cost the US economy $100 billion and as many as 508,000 US jobs annually.”
—Estimating the Cost of Cybercrime and Cyber Espionage, Center for Strategic and International Studies (CSIS)

To prepare for attack and prioritize response based on asset value prevents a culture of complacency. But perpetual preparedness is tough to maintain. For instance, vulnerability management tends to be a daunting task because of the dynamic array of devices on the network and the continual bombardment of warnings, security patches, and zero-day exploits. Mapping how these may affect the most critical systems and processes for business and establishing remediation plans can become an infinite loop—a resource black hole.

Best practices minimize the available attack surface, making it easier to monitor and manage the assets that will likely be targeted. Working toward speed and efficiencies in assessing the environment for vulnerabilities, then investing in measures that counter the potentially most damaging risks are the two top ways to directly increase your level of preparedness in the face of security events and threats.

### Examples

<table>
<thead>
<tr>
<th>Key Concepts</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Weakened databases working 24/7</td>
</tr>
<tr>
<td>“Mean time to patch” for databases is getting longer, exposing organizations to risk and creating opportunities for exploitation. Use virtual patching and database security tools to compensate while keeping databases running for business use.</td>
</tr>
<tr>
<td>• Managing the patch panic</td>
</tr>
<tr>
<td>Quickly assess the systems with the greatest exposure and highest importance to your business. Use selective and virtual patching, compensating controls, and countermeasures to optimize or defer ever-present, time-consuming patching.</td>
</tr>
<tr>
<td>• Managing and reducing the vectors for zero-day threats</td>
</tr>
<tr>
<td>From real-time data collection to tracking changes, take advantage of new automated tools that alert on user actions and installations to stay ahead of potential vectors of attack. Decrease threat options with enhanced memory protections and hardware-enhanced measures.</td>
</tr>
</tbody>
</table>

For further reading, visit [www.mcafee.com/securityconnected](http://www.mcafee.com/securityconnected) and download

- Neutralize Advanced Attacks
- Counter Stealth Malware
It used to be good enough to know about a system and have an occasional inventory of its software. But today a broader, richer, and more dynamic picture is necessary, which includes baseline of usage, applications running, state of current security protections, and continuous monitoring of change. This level of detail can indicate potentially risky and anomalous behavior and usage.

As security information and event management systems collect these details for an expanding set of events, security data volumes are growing. The data set expands further as the SIEM runs increasingly refined correlations and analytics. Predictive security—systems measures that characterize attacks, identify likely targets, and deploy countermeasures—rely on these faster and stronger tools and rich data feeds.

And we keep getting access to more data. We can integrate context with alternative sources of intelligence and data exchanges, producing faster notification and reaction times. Scarce security/IT personnel are being equipped to, in the most efficient manner, take risk-mitigating steps calculated on assessments made in real time.

A more transactional approach within our monitoring and management systems will enable IT teams to keep up with the onslaught of log, event, and contextual data.

"For most security leaders, there is a pervasive sense of vulnerability about the inevitability of a breach event coupled with a lack of confidence in the ability to detect the event accurately to stem the tide of any potential damage."

—2013 TELUS-Rotman IT Security Study Executive Summary

Examples

<table>
<thead>
<tr>
<th>Key Concepts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security management has to be more user-friendly, giving the advantage back to the administrators so they can react quickly to findings using natural language queries and real-time responses.</td>
</tr>
<tr>
<td>Analysis of the large volumes of security data reveals the key risk indicators for your unique business based on the current and ever-changing state of the environment. Correlating information with context can guide automated reactions to anomalies, such as blocking, quarantine, and remediation.</td>
</tr>
</tbody>
</table>

For further reading, visit www.mcafee.com/securityconnected and download

<table>
<thead>
<tr>
<th>TRENDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time situational awareness</td>
</tr>
</tbody>
</table>

Examples

- Ask the right questions and get quick, accurate responses
- Automate security for faster reaction

Key Concepts

- Manage Risk and Security
- Operationalize Intelligence-Driven Response
- Achieve Continuous Monitoring
- Neutralize Advanced Attacks
“Be more proactive about the threat—and react more rapidly when breaches do occur. Detect them quickly, respond, clean up, and adjust your tactics. Be outward-facing, prepared, and ready in advance. Anticipate and prevent when possible, but be ready to isolate and encapsulate intrusions to minimize impact. It’s better to lose a finger than to lose an arm.”

—Deloitte Tech Trends 2013
Elements of Postdigital

As fast as business is working to build protections, cybercriminals are developing evasive and disruptive techniques to gain access to your organization. They take advantage of the silos of responsibility and islands of visibility traditionally found in IT: isolated management and oversight of endpoint, network, email, web, and data centers.

For instance, a “low and slow” advanced persistent attack will follow a lengthy timeline (that can last months or years), the pattern McAfee Labs documented in the Operation Troy cyberespionage campaign. A vulnerable endpoint or website may enable the first compromise, followed by multiple malware payloads and tools delivered through multiple network communications. The extended timeline and complex interactions of persistent threats help them go unnoticed, and also provide your chance to break up the attack: find the malware, freeze the activity, and fix the problem.

Can you detect the patterns in an attacker’s code and techniques and recognize coordinated actions across threat vectors? Or do you detect technical indicators after the mission has succeeded?

An active defense preempts a system compromise or data breach, identifies what the attack is after, and makes it harder for the attacker to move toward their goal.

<table>
<thead>
<tr>
<th>Examples</th>
<th>Key Concepts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect advanced evasive techniques</td>
<td>Start looking into minor traffic anomalies that can be indicators of evasive attacks. Evasive code may be delivered in separate payloads. Malware must be collected and reassembled, and it may need to be analyzed using deep dynamic and static analysis in order to judge its intent and risk.</td>
</tr>
<tr>
<td>Adopt prescriptive security measures</td>
<td>Security intelligence and threat analytics give insight to newly identified and emerging risks and their attack vectors. Policy automation can apply countermeasures and layers of protection limiting the ability for a cyberattack to succeed, such as isolating network communication, increasing host protections, or blocking with whitelisting and hardware-based measures.</td>
</tr>
</tbody>
</table>

For further reading, visit www.mcafee.com/securityconnected and download

- Operationalize Intelligence-Driven Response
- Neutralize Advanced Attacks
Line of business owners continue to push business expansion, driving more reliance on IT to provide faster responses to infrastructure needs or deal with the risk of users going directly to cloud providers for solutions. IT is meeting these needs through greater efficiency, enabled by virtualization, private and public clouds, and software-defined networks. This mix of technology is blurring what were the distinct boundaries of server, network, and application protections. The data center is now more complex, with new elements such as hosts, zones, and dynamic load distribution policies.

Today’s flexible, scalable data center requires security that will not hinder the choices or options for growth. Providing security management and visibility across physical, virtual, and cloud environments becomes a fundamental concern.

Whether IT delivers data center services or is sourced to a cloud provider, your business is still accountable for security and compliance. Your hardest job may be proving that you are doing this job.

“Sophisticated IT shops are developing tools to map workloads to cloud-based hosting options using criteria like mission criticality, sensitivity of data, migration complexity, and peak processing requirements. This will make it possible for IT staff to pursue a mixed-cloud strategy and drive workloads to the hosting options that best balance risk and economic value.”

—“Protecting Information in the Cloud,” McKinsey & Company

### Key Concepts

- **Secure change management**: More services are being contracted, hosted, or deployed via cloud platforms—models where control and accountability are hard to manage. Use tools that can track changes and the integrity of the systems and use rules that can be applied uniformly across physical and virtualized systems.

- **Optimized for the environment**: Security has to provide similar results across all kinds of data centers and services, but should leverage the best methods without sacrificing performance.

- **Security management extended to the cloud**: Ensure systems provide visibility into the security status and attest to the integrity of the hypervisors the workloads run on. Get context about the environment these services are provisioned into, confirming adherence to policies set in place to protect business security and compliance standards.

For further reading, visit [www.mcafee.com/securityconnected](http://www.mcafee.com/securityconnected) and download:

- Manage Risk and Security
- Protecting the Data Center
Where do you draw the line? The majority of enterprises permit employees to use their own devices to access corporate resources, but most don’t manage or control the security and health of those devices. Web services and social platforms are being embraced by business for business purposes, but how do you differentiate and restrict access for business from access for personal use? Even thin-client models and virtualized desktops prove to be susceptible to malware-infested websites and email contamination.

Every business will have to make its own risk decisions, in addition to continuously educating users and monitoring. IT doesn’t have to say “no” if the tools are available to limit unwanted behavior, manage access, and also control the specific features that pose high risks to the organization.

For example, access to cloud storage can be acceptable and even embraced if controls are in place that allow downloads while blocking uploads, ensuring confidential data stays within the organization. The task for organizations is to make it easy, so there will be fewer reasons to find an insecure workaround. Giving flexibility to workers increases productivity but requires real trust between employees and employers.

### Examples

<table>
<thead>
<tr>
<th>Examples</th>
<th>Key Concepts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single sign-on for web services and social platforms</td>
<td>Maintain control of social platform and web application use through business authorization tools that allow single sign-on using corporate credentials.</td>
</tr>
<tr>
<td>Security policy management for mobile devices</td>
<td>Ensure basic protections are active prior to business access: enforce passwords, block jail-broken devices, encrypt or sandbox sensitive data, and wipe all business content when a device is lost or stolen.</td>
</tr>
<tr>
<td>Website warning advisor</td>
<td>Give employees tools to help them make better security decisions with visual warnings about suspicious and malicious websites.</td>
</tr>
<tr>
<td>Secure gateway to the web</td>
<td>Based on risk, define policies that allow the proper scope of access and functions appropriate for the workgroup role and responsibility. Look for tools that provide monitoring, alerting, and blocking when high-risk scenarios are detected.</td>
</tr>
</tbody>
</table>

For further reading, visit [www.mcafee.com/securityconnected](http://www.mcafee.com/securityconnected) and download

- Securing Mobile Devices
- Securely Enabling Social Media
More and more things are becoming interconnected, networked, and part of our business and personal lives. The value of receiving specific data from distributed sensors and systems can drive huge efficiencies and business opportunity. The “Internet of Things” can improve personal well-being and provide optimal and resource-efficient buildings and smart cities.

As we see with the privacy gaffes and invasions we experience today, these sensors and their data will also need to be secured. We also need to ensure the integrity of their interactions, for confidence that communications and data have not been modified or deleted.

Organizations involved in energy, industrial controls, telecommunications, and healthcare are developing innovations to maximize the advantages and minimize the downsides of this new paradigm. However, every enterprise will be affected eventually. How might your security model change when systems negotiate, collaborate, and create Big Data and digital exhaust? These systems may roam, form meshed networks, and communicate across a variety of protocols. They will be resilient, working for your organization to deliver feedback on environmental or product performance. They may be the foundation for the next generation of data-driven services.

At the same time, your employees are readily adopting these devices. How will you reply when your workers request or demand access for devices beyond tablets and smartphones—like their wearable computing devices?

### Examples

<table>
<thead>
<tr>
<th>Key Concepts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizations will design and partner to create their unique Internet of Things ecosystem. Utilizing security enabled for embedded systems will provide stronger security management and control.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key Concepts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing a great variety and diversity of interconnected systems on a large scale will require tools that can abstract key security elements, easily integrate with context information, and show trust relationships. Together, this intelligence provides a current state of security and risk.</td>
</tr>
</tbody>
</table>

For further reading, visit [www.mcafee.com/securityconnected and download](http://www.mcafee.com/securityconnected)

- Operationalize Intelligence-Driven Response
FOCUS 10
Sustainable security—prevention is no longer sufficient

Asserting more control can be counter-productive. Security needs to be value-based. After measuring the importance of the data, people, networks, and systems to your business, you must use these values to make informed decisions through ongoing awareness, intelligence, and reputation assessment.

Enabling a sustainable and agile security program requires more than just a reactionary response to events, threats, and vulnerabilities. It requires more than being proactive about hunting and fighting targeted threats and infected hosts. You need prevention and proactive action. But you also need resilience and the ability to persevere. Sustained security requires considerations about efficiencies—in the lifecycle of security, from policy creation to remediation. Every process should reduce friction, encourage prioritization, and promote progress. This discipline helps ensure that the important stuff happens—and that the unimportant stuff doesn’t get in the way.

“We will bankrupt ourselves in the vain search for absolute security.”
—Dwight D. Eisenhower

<table>
<thead>
<tr>
<th>Examples</th>
<th>Key Concepts</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Integration of tasks into workflows; integration of disparate data into contextual dashboards</td>
<td>One size does not fit all, and when a unique security problem arises, sometimes it’s best to partner with specialty vendors. Integrating these vendors into your processes and protections is vital to enhancing the security posture of your business.</td>
</tr>
<tr>
<td>• Predictive security measures</td>
<td>The speed with which new variants and threats are emerging means it’s no longer efficient to catalog and create known blacklists. Tools have to change to include whitelisting and graylisting. The intermediate status of graylisting helps to signal risk and guide blocking until code can be verified as good or bad.</td>
</tr>
</tbody>
</table>

For further reading, visit www.mcafee.com/securityconnected and download

• Manage Risk and Security
• Achieve Continuous Monitoring
This swirling environment of threats, strategies, trends, and priorities requires a connected security approach that can adapt to and protect the ubiquity of your IT infrastructure. A Security Connected model not only bridges any technology gaps, it addresses today’s evolving business priorities and can positively impact your success in a competitive environment.

You can probably relate to most of the topics we’ve covered here, but there are other important subjects that have not been addressed. If you would like to get more details about the Security Connected Reference Architecture, 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. It’s yet another example of how McAfee is relentlessly focused on finding new ways to keep our customers safe.
“As I’ve traveled around the globe to meet customers, I’ve become conscious of an evolution in the security conversations we have—from tactical concerns to strategic objectives. Customer questions have become very future-centric. It’s less about what a security technology will do, and much more about where will your technology take them. They want to understand how will it shape and impact long-term strategic plans.

Customers are moving from the ‘I’ve been breached, I must respond’ mentality to asking what their security architecture should look like tomorrow. They ask what their holistic approach to security should be.

Security Connected is how McAfee enables this holistic, sustainable strategy.”

—Michael Fey
Executive Vice President, General Manager of Corporate Products & Chief Technology Officer McAfee
About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ: INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its visionary Security Connected strategy, innovative approach to hardware-enhanced security, and unique global threat intelligence network, McAfee is relentlessly focused on keeping its customers safe.