



Rewriting the Rules

Top Five Security Trends Affecting Security Strategy



“The IT infrastructure is under constant attack from a variety of players, from mischief-makers to nation states and everyone in between. The cybercrime environment is most interested in committing financial fraud, data theft, corporate espionage, and disruption or destruction of infrastructure and processes. Enterprises and organizations are engaged in a constant arms race with the attacking elements, and generally the perception is that the offense is winning.”¹

—Charles Kolodgy,
Research Vice President,
Security Products,
IDC

Introduction 3

Targeted Attacks 4

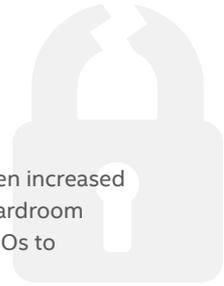
Data Center Transformation 6

Cloud Security 8

Data Protection 10

Securing Specialty Environments 12

What's Next? 14



Introduction

As damaging attacks continue to haunt companies and threaten increased regulatory action, security strategy is on the agenda in the boardroom and C-suite. But targeted attacks are not the only topic for CISOs to strategize around.

Security professionals are challenged to protect company and customer data as it proliferates on more devices, located in more places, and accessed by more applications than ever before. IT itself is transforming as the traditional data center evolves into a mix of public, private, community, private-hosted, and hybrid cloud configurations. Specialized IT environments have developed with unique devices and community clouds for specific industries, requiring tailored security built to meet business requirements.

These disruptive, long-term influences have unique requirements and common denominators. They call for a shared and thoughtful risk posture, security and compliance infrastructure, and operational plan. This guide offers recommendations on the options and inflection points CISOs should factor into their security and risk management strategy.

1. Targeted attacks have revealed the clear risks that extend beyond data exposure to device, data, and application availability.
2. Data center transformation requires different protection for software-defined services based on virtual and cloud constructs.
3. Cloud security demands a strategy to keep data secure and compliant in, to, and from the cloud as a part of increasing “Everything-as-a-Service,” shadow IT, and digital business trends.
4. Data protection must extend compliance efforts to intellectual property protection, risk management, and proof of due care.
5. Specialty environments shift security’s role from protecting users and their systems to also protecting the connected devices comprised by the Internet of Things, as well as the data these devices generate.

Targeted Attacks



While some companies are getting better at detecting attacks, many still learn of such incidents after the fact. Why? Highly targeted, stealthy attacks result in low threshold breaches that are difficult to detect against the background noise of events and routine behavior.

CISOs and their security operations teams are faced with analyzing millions of security events and suspicious files to find evidence of incidents, and then need to assemble this data into a reconstruction of the targeted attack. Often this analysis is manual or short-term, which greatly impairs the accuracy and speed of the response process.

What they need is a way to minimize the attack surface, identify potential risky behaviors, and contain events before damage can occur. However, this is easier said than done due to the increasing volume and sophistication of targeted attacks that successfully pass through existing, isolated defensive controls.

Most companies are just beginning to get their strategies in place for applying threat intelligence across their organizations. Rather than only sharing raw threat data, products must also share context, critical events, and organizational intelligence and then act in concert. Today's approach integrates updated endpoint and network countermeasures with continuous monitoring and analytics to block, detect, and investigate events in real time. By reducing attack dwell time, the CISO can minimize the likelihood, damage, and cost of a data breach or disruptive attack.



“While at least 60% of enterprises will discover a breach in 2015, the actual number of breached entities will be much higher (80% or more).”

—Forrester Predictions 2015: Security Budgets Will Increase, as Will Breach Costs, Fines, and Lawsuits

Desired Outcome	Key Concept
Protect against targeted attacks.	A health check often reveals “quick wins” that reduce the attack surface and catch some never-before-seen payloads and techniques. Often just updates to existing controls, these efforts improve blocking and reduce alert traffic. In addition, connecting countermeasures to share localized intelligence across threat vectors and operational domains enables orchestration to effectively disrupt targeted attack campaigns. This capability also feeds detection insights back into defenses.
Detect targeted attacks.	The overwhelming volume of alerts means indicators of attack (IoAs) are often missed, ignored, or detected too late. The SOC must have better tools to discover compromises and hunt attack footholds that would otherwise go unnoticed. Progressive security operations adopt centralized, continuous monitoring as well as deviation- and correlation-based analytics that identify anomalous behavior—in both historic and ongoing activities.
Correct targeted attacks.	Siloed operations lead to poor visibility, unclear remediation, and cumbersome workflows that impede containment, cleanup, and closure of investigations. Instead, the monitoring systems that detect events should prioritize the most critical incidents and facilitate centralized investigation and rapid remediation with minimal operational friction. If response actions repeat, they should be automated to increase capacity and improve response time. Findings should also factor back into intelligence databases, policies, and processes for adaptive security.

Data Center Transformation



Today, practically every company has employees and customers accessing web services, databases, and applications from a myriad of mobile devices and locations. To support this volume of data and transactions and meet the user's expectation of real-time processing, data centers are implementing software-defined services delivery based on virtualized architectures.

A core piece of driving efficiencies for the data center has been server virtualization, which helps to reduce total cost of ownership while establishing a foundation for agility and automation of the underlying computing infrastructure. The emergence of server virtualization created a need for optimized server security for virtualized environments. Data centers today have the ability to deploy security policies seamlessly as virtual machines (VMs) are provisioned, and if VMs are moved within the data center, the security policy will move with that VM.

A new virtualized network of compartmentalized applications in your data center allows for increased flexibility and security—if architected with purpose-built security solutions made for the software-defined network. Unfortunately, many organizations apply and leverage traditional security models in these critical environments, rather than adapting security to this technology and operational model.

Traditional tools fail in the face of determined adversaries, who realize the value of the data within and can exploit virtual and cloud vulnerabilities. A different approach is required. It is best not to try to retrofit traditional security into the modern data center, but instead to determine how to leverage the new compartmentalized, highly available data center to secure critical information assets. Most often these new deployment models will emerge as new application environments are being rolled out.



*“In 2015, IT organizations will reach an inflection point, at which **business velocity outpaces IT’s ability to meet its demands.** With the help of a bimodal IT strategy, new architectures such as software-defined data center will transform infrastructure planning and deployment for increased agility.”*

—2015 Planning Guide for Data Center
Modernization and Consolidation—Summary

Desired Outcomes	Key Concepts
Security for the services-oriented delivery model.	Data centers are in a transition from server and storage virtualization to a services-oriented architecture. Old static designs must be rethought to capture the benefits expected from the software-defined data center, in which every element in the data center is delivered as a service. An abstraction layer can broker interactions between the security infrastructure and virtualization management of software-defined infrastructure (SDI) in the data center. Dynamic processes can support automated security provisioning, policy synchronization, protection, and remediation consistent with SDI.
Appropriate identity, trust, and access in the age of IoT.	With so many devices connecting into the data center from so many locations, IT needs to identify who has legitimate access, ensure secure transactions, and prevent data exfiltration. The volume of connections creates an enormous scale challenge and exponential growth in log data. Extensible integration, management, and monitoring models facilitate visibility, control, and device and data integrity for users and things.
Uniform and centrally managed security across our hybrid data center.	The CIO would like to benefit from the cost savings of transitioning operations to cloud data centers, while the security team would like uniform security across multiple locations and administrators. Management tools and reporting systems should facilitate centralized policy definition, monitoring, incident response, and audit processes while accommodating organizational regulatory requirements.

Cloud Security



The volume of applications and services hosted in the cloud is exploding, enabling agile digital business. While security concerns remain a key reason why organizations refrain from embracing the cloud, the productivity benefits mean that users find a way to access cloud services without IT support.

The resulting power struggle pits centralized IT, which wants to control the flow of data, against individual users or lines of business that want to quickly share data or place workloads in the cloud for business efficiency. IT departments need to be able to: extend on-premises data centers into public cloud architectures, such as Software-as-a-Service (SaaS) and Infrastructure-as-a-Service (IaaS); quickly uncover instances of SaaS, Platform-as-a-Service (PaaS), and IaaS in use by their organizations; and automatically apply security policies to protect data in, to, and from the cloud.

Use of the cloud doesn't reduce risk and appliance accountability. Since they don't control the infrastructure in a public cloud service, IT security teams need to completely understand the shared security model in place with their service providers, while maintaining control over what they can. This increases pressure on companies to fully understand which security controls they are in control of deploying in order to extend security policies effectively across multiple environments.

Many companies are embracing a "cloud first" delivery approach when looking at purchasing new applications for the business. In the process of making this shift, they need to consider the risk factors and incident response processes affected by moving to the cloud, including how data will remain secure and compliant.



“The key drivers for cloud adoption are organizational agility, cost benefits, and increased innovation. These drivers are offset by persistent concerns about security and privacy, which continue to inhibit adoption, particularly of public cloud services.”

—*Cloud Adoption Trends Highlight Buyer Preferences and Provider Opportunities, March 27, 2015. Gartner Analyst, Ed Anderson*

Desired Outcome	Key Concepts
Protection for data and applications residing in the cloud.	The largest concern is data loss from hacking of a cloud application or into cloud storage. Portable and consistent data protection, ensuring that sensitive documents stored in the cloud are inspected and encrypted, enables compliance and peace of mind. Inspecting traffic to cloud workloads and securing data stores can also thwart attacks within shared infrastructure. In addition, underlying protection capabilities, such as file integrity monitoring and application control, should be deployed, especially for IaaS, to help strengthen protection and compliance.
Elastic security for workloads.	Consistent controls should extend easily from on-premises systems into hybrid and public cloud environments to secure workloads, wherever they reside and wherever they move. Policies should be centrally managed to enforce compliance and organizational risk posture, regardless of the data center deployment model. For many, SaaS security solutions are chosen to scale along with cloud instances, SaaS applications, and hybrid infrastructure.
Visibility and control over usage of SaaS and the public cloud.	Lines of business are embracing services such as Dropbox and Amazon Web Services without involvement of IT and security, introducing hidden vulnerability and risk. Tools must uncover shadow IT instances of SaaS, PaaS, and IaaS in use and help IT apply security policies and controls.
Consolidated compliance, incident management, and reporting.	Evolving cloud models mean data centers are spread across locations—some owned by you and some owned by public cloud providers. Management tools and reporting systems should facilitate incident response and audit processes while accommodating organizational regulatory requirements. Consistent data protection must be documented on demand through integration and automation of all logs in a central location.

Data Protection



A few years ago, enterprises made major investments in data protection which were largely justified by compliance demands. Since then, there has been a lull. That is, until recent massive breaches brought the spotlight back to data protection and the need to secure information.

Organizations have discovered that traditional infrastructure security fails to prevent loss of data. In addition, hackers are no longer only after personally identifiable information (PII) and credit cards, but also operational information and trade secrets. A data breach, if it involves regulated data, must be disclosed to the public (regulatory compliance), unless the data can be proven to have been encrypted at the time of exposure.

In an increasingly mobile world, your company's data is as well traveled as you are. Gone are the days when information resides in one locked room. Now your data moves across an expanse of potentially defenseless devices, operating systems, and Internet-ready locations.

Just being compliant is just not good enough in today's environment of stealth cyberattacks, increased adoption of cloud services, the explosion of Internet-enabled devices, and widespread data capture. Securing data isn't the difficult task you may believe it is. Encryption minimizes exposure risk while visibility helps you adjust controls and processes to protect data as it is in motion, in use, and at rest in portable and fluid infrastructures.



\$400 million—the estimated financial loss from 700 million compromised records shows the real importance of managing data breach risks.

—Verizon 2015 Data Breach Investigations Report

Desired Outcomes	Key Concepts
Lock down lost data.	Recent hacks of operational information, as well as customer data, shows that traditional infrastructure protection is failing to prevent data breaches. It is essential to encrypt data in case there is a loss, and ensure encryption remains active on disconnected and portable devices.
Visibility and control over data flows.	The first step in information protection is defining what your data is, knowing where it resides, and determining who should be using it. Creating a baseline of what normal data flows look like in your organization will let your systems alert you when abnormal activity occurs. You should also eliminate channels of data loss via data-in-motion controls.
Manage data.	Companies often have multiple, disjointed security products, delaying response times when confronted with a data breach. Connected security solutions monitor and manage data easily with a central console to watch data flows, alert when abnormal activity occurs, and help you respond.

Protecting Specialty Environments



While it is true that the adoption of IoT in enterprises hasn't been as quick as in the consumer market, IoT is growing rapidly, with the potential to radically change almost every business process—from manufacturing and design to marketing and sales. Verizon predicts that the number of business-to-business (B2B) IoT connections will increase 28% annually from 2011 to 2020, with more “things” connecting directly to one another without human input.²

For example, traditionally isolated critical infrastructures, industrial control systems (ICS), and supervisory control and data acquisition (SCADA) computing environments are becoming connected to gain new capabilities, redefining the infrastructure to include IoT. These new connections introduce risks and vulnerability, exposing weaknesses that were previously hidden by the obscurity of non-connectivity.

As a result, energy, healthcare, retail, financial services, and manufacturing are all rethinking their security models, as they are no longer tasked to only protect people and their connections to systems, but also to secure things connecting to other things. The transition from closed networks to enterprise IT networks connected to the public Internet is accelerating at an alarming pace—and is raising alarms about security.

With the billions of objects that are expected to be networked within the next few years, questions of identity and trust, data protection, access control, and device control are all areas of concern. How do we identify these objects and trust them as they attempt to connect into our network? How do we ensure that the data they are transmitting is good data from a trusted source?



*“The Internet of Things (IoT) has enormous potential to drive economic value and social change. But with **85% of things still unconnected and security threats pervasive**, the industry has yet to tap IoT’s enormous potential.”*

— The Intel® IoT Platform: Secure, Scalable, Interoperable

Desired Outcomes	Key Concepts
<p>Protect device integrity, service availability, and data protection throughout healthcare environments.</p>	<p>As more medical devices are coming online and share patient data, the attack surface expands, putting sensitive healthcare data at risk of being breached. Devices must be built to withstand attack, yet be easy to update and manage. Embedding device integrity into IoT systems can enforce and validate trust using industry-leading whitelisting, change control, and memory protection to lock down systems and applications in multitenant environments.</p>
<p>Evolve security to protect point-of-sale and retail networks.</p>	<p>Having endured targeted attacks, retailers now face new mobile payment systems from non-traditional devices and expanding wireless and wired connections. They require security across the new supply chain network to ensure compliance, as well as customer data protection. This new approach must protect device and user identities, device integrity, and operational data while enabling secure application traffic.</p>
<p>Defend industrial control systems and critical infrastructure.</p>	<p>Energy, manufacturing, telecommunications, and financial services now qualify as critical infrastructure, enabling ongoing operation of government, emergency, and civilian infrastructures. Device identity, malware protection, data protection, and resiliency are required—all tailored to today’s machine-to-machine environments and highly distributed operations.</p>

What's Next?

Several, if not all, of these disruptive trends will likely affect you and your organization this year. As a security leader, you should both understand them individually, and look across them as a whole to detect commonalities and opportunities. These themes are the cornerstones of an adaptive security architecture, a concept brought to life in an integrated security system.

- Modular, up-to-date countermeasures that cross threat vectors and infrastructure tiers.
- Applied threat intelligence to combat low-prevalence, targeted threats and “unknown” malware.
- Context and orchestration to minimize costs, latency, and manual labor inhibiting threat management.
- Advanced analytics to pinpoint problems immediately and take action directly, often automatically.
- Centralized security management to minimize capital and operational costs and improve day-to-day security across mixed vendor environments.
- Approved and consistent automated workflows to reduce manual tasks and errors.

Our architecture reduces complexity and improves operational efficiency. It also provides critical integrated, adaptive, and orchestrated intelligence and response capabilities. This means pervasive security from client to cloud and positions you to defeat adversaries quickly. Intel Security is committed to being our customers' number one security partner—providing a complete set of integrated security capabilities.

Begin by initiating a conversation with Intel Security about your current infrastructure and your desired outcomes. We can help formulate your best plan, leveraging our expertise, partners, and a unified and open framework for hundreds of products and services from Intel Security and across all security technologies.

Learn more at mcafee.com/securityconnected.

“The business transformation driven by cloud-connected devices and services demands more than changes in data centers and network infrastructure. It demands an integrated security architecture that can expand across all systems and adapt to changes in infrastructure and threats. Fragmented security architectures lead to a state where products fail in isolation. With the sophistication and the volume of targeted attacks on the rise, the need for unified security architecture has never been greater.”

Our integrated security system enables our customers to respond quickly to emerging threats across their entire infrastructure. We resolve more threats faster and with fewer resources in a more complex world through stronger protection, superior detection, and faster correction. We secure your enterprise with an end-to-end portfolio of trusted and relevant on-premises and cloud-enabled solutions and services. Intel Security is committed to be our customers' number one security partner—providing a complete set of connected and integrated security capabilities.”

*—Christopher Young
Senior Vice President and
General Manager,
Intel Security*

About Intel Security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security combines the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world. **www.intelsecurity.com**.



McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

1. <https://www.mita.gov.mt/en/ict-features/Pages/2015/The-Malta-Independent-ICT-Feature-Week-202.aspx>

2. http://www.verizonenterprise.com/resources/reports/rp_state-of-market-the-market-the-internet-of-things-2015_en_xg.pdf

Intel and the Intel and McAfee logos are trademarks of Intel Corporation or McAfee, Inc. in the US and/or other countries. Other marks and brands may be claimed as the property of others. Copyright © 2015 Intel Corporation.
62175br_top-5-security_1115_wh