

PROTECTING THE DATA CENTER

Epsilon After The Breach

In 2011, a data breach of email marketer Epsilon exposed the names and email addresses of millions of customers. Because Epsilon services are used by a large number of highly visible companies, there was a rash of notifications sent out to warn customers of potential fraud. Companies having to engage in customer notification warnings included: Barclaycard US, Capital One, Best Buy, JPMorgan, Citigroup, Tivo, Disney Destinations, New York & Company, Walgreens, Marriott, and many others. (Source: <http://mcaf.ee/5342e>)

Security Connected

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.

Stronger Security for a More Agile Data Center

Challenges

Data centers run organizations. Among the roles of a data center are generating revenue, storing sensitive data, and providing business-critical services. 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.

According the March 2011 Ponemon Institute Cost of a Data Breach report, each compromised record costs \$214, averaging \$7.2 million per data breach event.²

Heartland Payment Systems After The Breach

In 2010, Heartland reached a \$60 million settlement with VISA to resolve all potential claims with respect to the 2009 breach. A year earlier, Heartland reached a similar settlement with Amex for \$3.5 million.¹



Solutions

Business agility

The data center operations team is being tasked with responsibilities from building solutions for continuous compliance and virtualization to consolidation and leveraging the cloud. A security framework should be agile enough to allow for rapid change and the adoption of new trends without bearing additional risk. A strong security framework that allows for this level of agility has a positive impact on security operations and business operations.

Security management

Breaches are expensive, with costs ranging from regulatory penalties, class action lawsuits, and public relations costs to diminished brand loyalty, lost customers, and, ultimately, reduced revenue. Because of the complexity of data centers mixed with some of the aforementioned trends and threats, successful risk mitigation requires a holistic approach to security. A centralized security management solution that connects disparate solutions across data, endpoint, network, and the cloud should be used when managing data centers of all sizes and complexities. Extensible security management is vital for visibility into the applications and databases that process transactions and the storage devices that retain that data.

Availability and integrity

It's a challenge to provide availability and integrity in the face of internal and external threats, embrace new trends like mobile equivalents for websites, integrate with third-party Web 2.0 services, take advantage of various cloud infrastructures. And it can also be extremely risky if a level of care isn't taken to provide a robust security posture that isn't myopically focused on content security or network security but instead blends endpoint, content, and network security while integrating with the cloud. A security framework should minimize latency, reduce the risk of manual configuration errors, prohibit

the installation of malicious software, and protect information irrespective of the data center footprint, whether consolidated, virtualized, or cloud based. Protecting virtualized environments—virtualized servers and virtualized desktop infrastructures (VDIs) are essential. VDI is commonly installed on everything from smartphones to laptops and virtual servers—and this is the norm in data centers. Today's solutions need to be optimized to address trends in virtualization, but the basics are still important too. Latency and unscheduled downtime is not an option for mission-critical environments. Network operations, access control, endpoint protection, and firewalls must be engineered with the needs of IT operations in mind—not just security, as subpar security solutions that introduce latency can be just as damaging as an attack.

Security optimization

Security optimization moves organizations away from the purely technical question regarding security controls—"Can we do it?"—and instead addresses "What's the best way to do it?" There are many security solutions out there, and most do a good job. But collectively they introduce complexity—the greatest enemy of security. Having disparate silos and solutions that lack interconnectivity and depend on ever-increasing resources to operate isn't sustainable. Instead, today's security frameworks should support an optimized security model that aims to centrally manage security controls, allows those controls to enrich each other, and aligns the solutions with business priorities while reducing security operational costs. As threats evolve and a greater number of trends are rapidly adopted, an optimized security framework will be a necessity for cost-effective, efficient, and secure business operations. Optimized solutions are an integral part of automating the compliance process so that security tasks and processes surrounding regulatory mandates are aligned without creating additional overhead.

Best Practices Considerations

- Understand that data centers are going through rapid change: consolidation, virtualization, and cloud
- Implement solutions that meet needs for: agility, security management, availability and integrity, and security optimization
- Deploy solutions that centralize security operations for key data center components: networks, virtualized solutions, databases, servers, and storage devices
- Ensure that the security solutions utilized also assist in automating compliance
- While addressing security ensure that operational mainstays surrounding availability and latency are factored in

According to the Data Loss DB Open Security Foundation, as of April 2011, 75 percent of the data loss was a result of nefarious activity while the remainder is attributed to carelessness.³

Value Drivers

Your data center initiatives should leverage security-based technology to drive operational efficiency. Consider the following areas where data centers can be optimized:

- *Consolidation*—The solutions for consolidation should be deployed across hardware, software, and supporting infrastructure
- *Standardization*—The solutions should support standardization of the endpoint, data, and network protection capabilities. This will help ensure that threat analysis and response are efficient and effective.
- *Decrease audit, compliance and monitoring cost*—The solutions should provide for (or be justified with) a decrease in IT audit and compliance costs—because you can audit the systems and process instead of all the individual nodes
- *Decreasing network traffic*—The solutions that can exist at the core serve to protect and should also serve to help eliminate unnecessary network traffic and spam
- *Decreasing help desk costs*—The efforts of securing the core data center should lead to a decrease in end-user help desk calls due to security related incidents

Related Material from the Security Connected Reference Architecture

Level II

- Protecting Information
- Controlling and Monitoring Change

Level III

- Assessing Vulnerabilities
- Enforcing Endpoint Compliance
- Preventing Denial of Service (DoS and DDoS) Attacks
- Protecting Servers

For more information about the Security Connected Reference Architecture, visit:
www.mcafee.com/securityconnected.

About the Author



Brian Contos, CISSP, is director of global security strategy at McAfee. He is a recognized security expert with nearly two decades of security engineering and management experience. He is the author of several books, including *Enemy at the Water Cooler* and *Physical and Logical Security Convergence*. He has worked with government organizations and Forbes Global 2000 companies throughout North, Central, and South America, Europe, the Middle East, and Asia. He is an invited speaker at leading industry events like RSA, Interop, SANS, OWASP, and SecTor and is a writer for industry and business press such as *Forbes*, *New York Times*, and *The Times of London*. Brian is a Ponemon Institute Distinguished Fellow and graduate of the University of Arizona.

brian_contos@mcafee.com || <http://siblog.mcafee.com/author/brian-contos/> || @BrianContos

¹ <http://mcaf.ee/gvxkh>

² <http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010%20Global%20CODB.pdf>

³ <http://datalossdb.org/>

