SPARKPOST

# Email Security in the Era of the Cloud: An Executive Brief

By Steve Murray, Chief Information Security Officer

Email has long been—and continues to be—a major communication tool in the workplace. Beyond that, email has an even greater footprint as a way for businesses and services to communicate with their customers. From app or service notifications to transactions to  social media updates, email is a proven reliable and effective way for businesses to drive customer engagement and growth.

Email's ubiquity, non-proprietary protocols, and universal support are major reasons for its effectiveness. Yet, its nature as an open communication platform also means that email is susceptible to attack on the infrastructure that hosts it, as well as deception by outside parties who want to trick users into compromising their systems and divulging information.

**Email remains by far the top vector for attacks by bad actors around the world.**

While the email spam problem has largely been solved, email remains a significant target for malware attacks and phishing attempts. Email systems are constantly being tested for vulnerabilities by adversaries ranging from amateur hackers to advanced persistent threats (APTs) working on behalf of state actors and every threat in between.

In fact, the public Internet has become so hostile and the threat models so varied that only the world's largest companies can deploy the technology and staff needed to maintain data center security, while keeping up with the latest security methodologies to stay one step ahead of the threats.

Yet even then, breaches will occur, as shown by successful attacks on organizations like the Democratic National Committee, Anthem Health, Sony Pictures, and Seagate that all involved email as an successful attack vector. In each case, hackers exploited messaging security and authentication weaknesses to breach the perimeter and steal sensitive information. Once they had a foothold in an organization, they were able to wreak more havoc. In another example, at Harvard thousands of unprotected domains were used to launch attacks on additional organizations, particularly American think-tanks and non-profits.

While mainstream media coverage of attacks may make it seem like there are just a few high-profile ones each year, attacks are on the rise and show no sign of slowing down. Verizon recently released a report that showed a steep rise in hacking, malware, and phishing attacks over the past few years. Their extensive research was based on a dataset containing 64,199 incidents and 2,260 breaches during 2016. They noted that "no local, industry or organization is bulletproof when it comes to the compromise of data" and that over 80% of compromises were pulled off in mere minutes last year.

Those trends demonstrate that not only is it very difficult to build and maintain your own secure infrastructure  Security is even harder for organizations that continue to rely on traditional data centers. Here's why.

## TRADITIONAL DATA CENTER SECURITY IS COMPLEX AND FRAGILE

Hosting your email infrastructure in a traditional data center can leave you vulnerable. We won't pretend to provide a primer here, but consider just some of the factors that go into running a secure facility. It begins with physical elements, including, but not limited to:

- Secure site with good infrastructure access
- Redundant, fail-safe power, connectivity, and other utilities
- Surveillance, guards, biometric or other enhanced access authentication, with extra security layers, such as multi-factor authentication, for sensitive areas
- Walls, windows, and doors that can handle not only natural disasters but hostile threats like from intruders with weapons—or even terrorism
- Landscaping and barriers designed to thwart high-speed vehicles

Even if business outsources those physical siting concerns to specialized data center providers, you're responsible for securing your servers, applications, and data. That means a company's IT team still must deal with issues such as securing its housed technology equipment, including, but not limited to:

- Established various network perimeter defenses and isolating different machines in firewalled zones
- Fast patching and updating
- Server-level and operating system security, ranging form appliance and/or software encryption to locking down various default OS services to monitoring every process on individual machines
- Specialized hardware—perhaps even at the level of custom silicon chips—to lock down computing environments

Running applications in your own data center requires defending every one of the seven layers that make up a typical Open Systems Interconnection (OSI) model. That means you're dealing with everything from transmission of data over physical cables (such as Ethernet) or a wireless medium (such as Wi-Fi) to the application and data layers. A weakness in any of those seven layers means that one of the bad guys can gain a foothold into your network and use that leverage to move around and find soft targets for costly damage. In the case of a recent breach at Target, for example, the bad guys got in through systems embedded in the air conditioning control systems and used that access to find more valuable, vulnerable systems on the network.

It's no surprise that more and more businesses have come to realize the significant advantages and risk reduction won by leveraging the resilience, elasticity, and security by design inherent to cloud platforms.

## CLOUD SECURITY IS PROVEN AND RESILIENT

Modern cloud platforms like Amazon Web Services (AWS) make many of these complex risks much more manageable. Moving to the cloud helps business realize not only the reliability that comes from the redundant, distributed infrastructure of the cloud platform, but also the benefit of the security by design that is intrinsic to cloud architectures.

Consider some of AWS' strengths. AWS operates data centers in 42 availability zones within 16 geographic regions worldwide and spends millions of dollars annually on security, including the maintenance of a robust defense against DDOS (Distributed Denial of Service) attacks. In fact, AWS successfully fends off 50-60 TB of DDoS attacks every day.

Other security measures offered by AWS include, but are not limited to:

- One of the world's best information security teams staffed by top experts and professionals
- Leading edge application security architects building intrinsic security capabilities directly into AWS' IaaS and PaaS systems
- Dedicated monitoring and intrusion detection systems for both the perimeter and interior of their operations
- The ability to enable continuous and real-time auditing to meet the requirements of a variety of industry-specific standards
- The ability to launch an instance in a definable virtual network that functions as a private cloud
- TLS encryption in transit
- The ability to add additional layers of data encryption
- Identity and access control, including multi-factor authentication that offers hardware-based options
- Certifications that include ISO 27001, SOC, the PCI Data Security Standard, FedRAMP, and others

AWS has proved that they offer a best-of-breed, rock-solid cloud security foundation. SparkPost's messaging infrastructure is built on AWS because we know they have expertise and scale that exceeds any traditional data center. But more than that, the security by design that's part of any system built on the AWS model means there's less risk for vulnerability in the application and data layers as well.

## RELIABLE AND SECURE EMAIL DELIVERY THROUGHOUT

There's no question that the active risk management and infrastructure redundancy of the cloud is a real advantage. SparkPost leverages AWS and its foundational security and availability requirements to ensure that our customers can rely on high performing, secure, and reliable message delivery.

**SparkPost not only leads the industry on high-performance email delivery, but we're also the world's foremost experts on ensuring the integrity and security of email delivery.**

Our security, compliance, product, and deliverability teams work together to incorporate key controls throughout our service:

- End-to-end encryption with transport-layer security across all services
- Operational controls, including IP address restrictions, unique API keys, and multi-factor authentication
- Integral security design considerations and regular code reviews
- Customer privacy protection controls, such as minimal personally-identifiable information with a limited shelf life and a fully separate customer database with encrypted data storage
- Support for key email authentication standards such as SPF, DKIM, and DMARC to limit phishing and other attacks against our customers' reputations and recipients
- Active monitoring and compliance controls to mitigate abuse
- Feedback loop (FBL) and other cooperative mechanisms with ISP inbox providers

## A BOTTOM LINE COMMITMENT TO MESSAGING AND BUSINESS SECURITY

Good security means more than hardened technology or messaging best practices; it also requires sound business processes that support technical systems. At SparkPost, that business control underlies how we implement technical infrastructure. Key operational considerations include:

- Defined information security practices, backed by a culture of security and an accountable Chief Information Security Officer (CISO).
- Change management controls and quality assurance practices that minimize the likelihood of disruption, unauthorized alterations, and errors.
- Compliance with legal and regulatory requirements and contractual obligations, including audits to meet needs of customers in regulated industries
- Risk management framework, crisis response procedures, and business continuity plans.
- Sound operational management of IT systems, continuous monitoring of all production infrastructure, and timely response to issues.
- Site control with well-defined access procedures.

With proven technology and unmatched expertise, SparkPost demonstrates the utmost commitment to ensuring messaging security in the cloud. Our industry-leading email delivery performance is backed by the fundamental security of a true cloud platform and a sound and secure technical and business operation.

Security is essential to any company doing business in the cloud. That's why ensuring the integrity of our customers' messaging streams underlies every aspect of SparkPost's technical architecture design, treatment of data, and business practices. This care and operational expertise ensures that today's businesses can have utmost confidence in email security in the era of the cloud.