Recent years have seen a dramatic rise in the scale and severity of Web attacks. SQL injection attacks are occurring more frequently than ever, and Denial of Service (DoS) attacks are happening on a much larger scale. The effects of these attacks extend long past the assault itself — in terms of lost revenue, resources, and productivity, along with damage to brand reputation and customer trust. With these issues top of mind, here are top considerations when developing your Web security strategy:

1. **Does your Web security strategy align with your business strategy?**
   Ernst & Young found that only 38% of respondents align their information security strategy to their organization's appetite and tolerance for risk. You need to put security measures in place to support your business plans.

2. **Have you devised a strategy for monitoring global attack trends?**
   The threat landscape is changing every day. Few organizations have the resources to stay current with Web attack trends. Partner with companies that can help you prepare for the broadest spectrum of attacks.

3. **What is your incident response strategy?**
   How much lag in response can your business tolerate? Are you staffed to respond quickly enough? Consider approaches that are always-on, automate response, and reduce the risk introduced by changing architectures in response mode.

4. **What does downtime mean to your revenue and brand?**
   The best practice is to quantify what it means for your site to be down for a minute, hour or day, both in terms of revenue and brand reputation.

5. **What would data theft cost your business?**
   Web security is more than DDoS. Because most attack vectors prey on Web application vulnerabilities, it’s critical to be able to detect and prevent these events even if Web availability isn’t mission critical.

---

**CRITICAL CONSIDERATIONS OF WEB SECURITY**

The average data breach in regulated industries costs $7.2 million USD.

— Symantec, 2010
6. **Is regulatory compliance an issue for your business?**
   Can you satisfy applicable regulations, e.g., PCI-DSS, FISMA, FFIEC, HIPAA, and SOX? Regulations evolve, complicating efforts to stay compliant. You need vendors that provide you with auditable transparency to their policies.

7. **Can you protect against all attack vectors?**
   Web attacks can occur at the application, network, or DNS layer. Regardless of where they occur, the result is the same. You will need to cover all types of attacks… preferably with fewer vendors covering multiple vectors each.

8. **How does your security strategy impact application performance?**
   Security measures consume processing power, slowing response time, and introducing the potential of false positives. New distributed cloud architectures offset these traditional trade-offs, providing security without impacting performance.

9. **Are you looking at appliance- or cloud-based security solutions?**
   Cloud-based solutions offer significant capital savings and add the ability to scale on demand. But, you still need to understand how big you can scale – today’s largest attacks will push the limits of the largest cloud players.

10. **How will you know if your Web security is effective?**
    It’s important to conduct regular Web vulnerability scans to ensure your policies match the threat. With a deeper understanding of potential exposure, your organization can make better choices about mitigating risk.

Akamai’s Web security solutions leverage the Akamai Intelligent Platform to offer a distributed, cloud-based approach to Web security. This provides an always-on layer designed to protect your applications against both high-volume DDoS attacks and Web application attacks, no matter where they are hosted. To learn more, visit our Web site for access to valuable whitepapers such as our guide Overcoming Security Threats. Visit [www.akamai.com/security](http://www.akamai.com/security) to learn more.