

IMPERVA®

Delivering
Cyber Security
Confidence
for the Modern
Enterprise



Executive Summary

Traditional network and endpoint security cannot keep pace with the industrialization of cyber crime, the growing sophistication of cyber threats, insider abuse, increasing user mobility and the wholesale changes cloud computing is bringing to IT service delivery. What's needed instead, and what Imperva enables with its solutions, is an approach to cyber security that is focused on protecting business-critical data and applications wherever they are located, in the cloud or on-premises.

For organizations that share our vision and subscribe to such an approach, the benefits to be gained include:

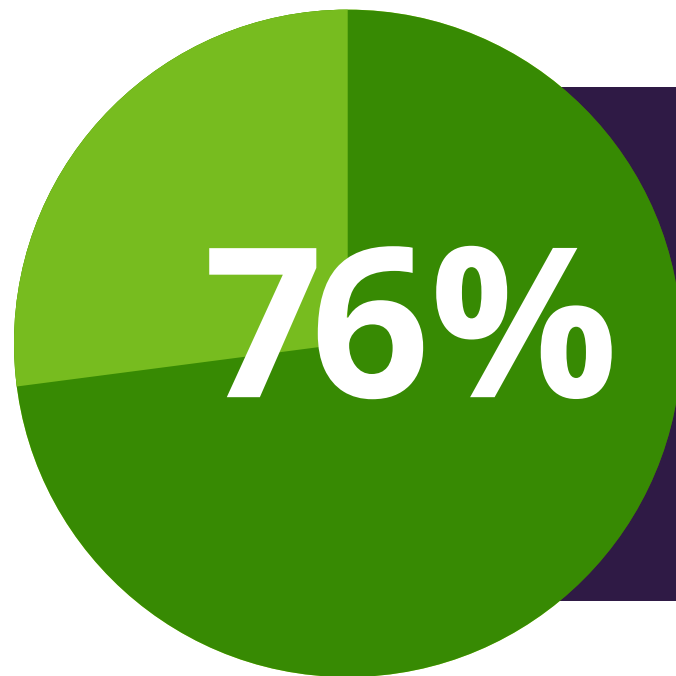
Reduced risk of successful cyber-attacks, data breaches and other incidents that can lead to substantial recovery and lost opportunity costs, erosion of customer confidence and potentially irreparable brand reputation damage

A more resilient, longer-lived and affordable cyber security infrastructure

An easier and more efficient way for ensuring and demonstrating compliance with an ever-growing set of data security regulations


Successful Attacks, Breaches on the Rise

Hardly a month goes by without another high-profile cyber-attack and corresponding data breach making the headlines. Major healthcare sites, leading entertainment companies, popular retail chains, government agencies and venerable financial institutions have all been hit hard, and repeatedly, over the past couple of years. And what we learn about on the web and in the popular press is only the tip of the proverbial iceberg. According to one report, 76 percent of organizations were victimized by cyber-attacks in 2015, up from 70 percent a year earlier.¹



of organizations were affected by a successful cyberattack in 2015 – low security awareness among employees is the biggest inhibitor to defending against cyber threats

¹ 2016 Cyberthreat Defense Report, CyberEdge Group, April 2016



As if the frequency of successful cyber-attacks is not enough, there is also the ensuing business impact to consider. The exposure of tens of millions of records containing sensitive employee, customer, or constituent data, the theft of countless credit and debit cards, disclosure of business-critical intellectual property and the loss of employment as “responsible” parties are invariably let go in the wake of such crises are only the beginning. Added to that are the direct costs associated with recovery – which can run into the tens of millions of dollars – as well as the loss of brand reputation and lost opportunity costs. For one retailer, profit for the quarter during which they announced a major breach dropped a crushing 46 percent compared to the same quarter a year earlier.

The bottom line is that no one is immune. Because it is not a matter of “if” you’ll be attacked but “when,” dealing with cyber threats and data breaches has become the new reality for organizations of all types and sizes worldwide.

For one retailer,
profit for the quarter
during which they
announced a major
breach dropped a
crushing

46%

compared to the same
quarter a year earlier.

Why Traditional Defenses are No Longer Sufficient

It's easy to attribute the prevalence of breaches to the presence of a determined and well-equipped adversary. After all, the industrialization of hacking over the past decade has put an arsenal of sophisticated attack tools and monetization capabilities in the hands of just about anyone who cares to look for them.

However, it doesn't help the situation that many of today's organizations make it easy for their foes - or insiders - to compromise business-critical information by relying too heavily on traditional network and endpoint defenses. Although network firewalls, intrusion detection and prevention systems (IDS/IPSs), antivirus software, personal firewalls and similar countermeasures still have a role to play, the simple truth of the matter is that there are too many ways around - or even through - such defenses.

For example, what happens when:

- Attackers use compromised credentials to steal data or cause damage in the corporate network;
- Insiders, with legitimate access to corporate data, perform careless actions with your enterprise data, or exploit privileges with malicious intent;
- Industrial hackers steal credentials to purchase goods or services with money stolen over time;
- Attackers gain entry into the corporate network by taking advantage of open communication paths intended to support legitimate business applications;
- Mobile users bypass perimeter defenses by bringing infected mobile devices into the office and directly connecting them to the corporate network;
- Attackers exploit input validation weaknesses or other vulnerabilities in custom web applications to trick systems into divulging records stored in connected databases; or,
- Adversaries use custom-crafted application requests to consume a disproportionate amount of back-end computing services, ultimately rendering business-critical applications unresponsive?

The problem is that traditional security strategies and technologies fail to adequately account for the lightning fast evolution of cyber threats and the attack surface area implications of user mobility and cloud delivery of IT services.



The Evolution of Cyber Threats

Once satisfied with door-rattling and other low-level attacks intended to boost their reputations, most hackers are now focused on stealing data that can be monetized, making a political statement or outright extortion. This has led to the industrialization of cyber crime and a corresponding explosion in the volume, diversity, and sophistication of the cyber threats that afflict today's organizations. Basic website defacement attacks and nuisance viruses continue to fade into the background as elaborate spear-phishing campaigns, credential-stealing malware and targeted attacks now command center stage. And once-dominant, network-layer exploits are now being joined by entire classes of new threats designed to target applications and data more directly. Furthermore, industrialization enables hackers to combine multiple, point exploits into highly sophisticated multi-vector attacks, and then launch these attacks at massive scale. The net result is the need for defenses not only that focus more directly on protecting data and applications, but that are also capable of counteracting multiple types of threats used in concert.

The Rise of User Mobility

User mobility poses multiple problems for traditional security models. When they are "in the field," mobile users and their devices often operate without the benefit of perimeter defenses. Upon returning to the office, they then connect to points behind the perimeter, easily spreading any malware picked up in their travels. Steadily growing adoption of bring-your-own-device (BYOD) practices compound this risk by taking the choice, implementation and configuration of client-side countermeasures out of the hands of IT and placing it into those of individual users. Restoring security effectiveness in this case depends on deploying defenses in the immediate vicinity of business-critical resources, rather than solely at the network perimeter.

The Journey to the Cloud

Greater flexibility and faster time to market are only two of the powerful lures driving the use of cloud computing as an alternative to traditional datacenter designs for delivering IT infrastructure and services. With essential data and apps often straddling both environments, the need is growing for defenses that provide consistent protection of key resources regardless of their location, in the cloud or on-premises.



A Better, More Secure Way Forward

Since being founded in 2002, Imperva has had a singular purpose and vision of enabling organizations to protect what matters most: business-critical data and the applications that serve as conduits to it. In contrast to traditional security strategies and technologies, the result of this focus is a portfolio of solutions that inherently accounts for ongoing changes to threat and technology landscapes, in addition to broader changes in the ways organizations architect and utilize their computing systems.

Beyond the fundamental principle of focusing on data and applications, other strengths of the Imperva approach to cyber security are revealed by exploring the details of how, where and when our solutions defend these all-important assets.

Imperva has had a singular purpose and vision of enabling organizations to protect what matters most: business-critical data and applications.



What Imperva Defends

Despite the never-ending changes to how cyber threats penetrate and propagate through a network, the end game remains constant: accessing valuable structured and unstructured information. By delivering web application, database, file, cloud application and DDoS protection solutions that directly attend to this end game, Imperva eliminates the need for organizations to explicitly adjust their defenses for every new “trick” or technique that attackers incorporate into their methods and wares. In addition, innovative technologies extend this advantage all the way to the application layer by enabling our security solutions to automatically learn application and user behavior changes over time.

How Imperva Defends

Equally important to what we defend is how we defend it. In this regard, the core capabilities of the Imperva solutions center on three functional requirements of an effective security strategy: discover, protect and comply.

- Multiple discovery engines work together to identify data and application assets throughout your computing environment, uncover associated vulnerabilities and generate a clear picture of the related risk to your organization. Ongoing monitoring further enhances both the asset inventory and risk pictures, for example, by providing insight into user behavior patterns and exposing network and system-level activity indicative of cyber threats.
- An extensive portfolio of protective mechanisms work to defend your organization’s web applications, databases, Big Data platforms, file systems and cloud-based assets from both known and unknown threats. Real-time alerting and blocking of bots, protocol exploits, SQL injection and cross-site scripting exploits.
- A powerful combination of automated data discovery and classification including the ability to monitor and audit access to virtually all sensitive data; and streamlined, regulation-specific reporting capabilities to help ensure compliance with industry mandates and regulations, such as SOX, HIPAA and PCI DSS.



A customer in the financial industry relies on Imperva SecureSphere to prevent—in real time—outside attacks from ever reaching sensitive data. With world-class deployment and operational support from Imperva, they placed all their production databases under its management in just one month.

Where Imperva Defends

Imperva safeguards data and applications both in the cloud and on-premises. The option to deploy essential security solutions on robust hardware appliances that deliver high performance and fail-open interfaces for high availability operations, is only a starting point. Virtual private, hybrid and public cloud initiatives are also enabled through support for many other deployment options and scenarios, including:

- Virtual appliances – for example, on the VMware ESX platform;
- Amazon Web Services (AWS) and Microsoft Azure – for protecting enterprise applications that leverage either of these popular infrastructure-as-a-service (IaaS) offerings;
- Data and application security as-a-service; and,
- Establishing protection for all of an organization's software-as-a-service (SaaS) applications.

When Imperva Defends

Imperva is committed to protecting what matters most to our customers: your data, applications and, in turn, your reputation. Accordingly, we will continue to enhance and expand our product lines – Imperva SecureSphere, Imperva CounterBreach, Imperva Incapsula and Imperva Skyfence – to stay ahead of ongoing and emerging trends. In addition, we will continue to invest aggressively in our most important asset, our people, especially the world-class security researchers at the Imperva Defense Center tasked with rooting out new attack methods and cyber threats before they impact your business.



Imperva is committed to protecting what matters most to you: your data, applications and, in turn, your reputation.

Conclusion

With the rapid evolution of cyber threats, increasing user mobility and key application and data resources migrating out of the datacenter and into the cloud, it is no longer sufficient to rely on traditional network and endpoint-focused security strategies and technologies. Instead, today's IT security and executive management teams need to consider shifting their investments in cyber-security solutions toward those that more directly and thoroughly protect the organization's business-critical data and applications, wherever they reside.

To learn more about the Imperva approach to cyber security and how our SecureSphere, CounterBreach, Incapsula and Skyfence solutions work to defend your organization's data, applications, infrastructure and reputation, please visit www.imperva.com, or [contact](#) an Imperva representative today.

