efficient iP™
DEFINING SMART DDI

2017 Report

The Global DNS Threat Survey

Methodology

This DNS attack study was conducted for EfficientIP, a leading provider of DNS, DHCP and IPAM (DDI), by research firm Coleman Parkes from a survey of 1,000 respondents, including 300 from North America, 400 from Europe and 300 from APAC.

The approach of this study was to look at the technical and behavioral causes for the rise in DNS threats, their potential business effects and suggest straightforward and rapid remedies.

Sectors covered include **Communications, Education, Finance, Healthcare, Manufacturing, Public Sector, Retail, Services, Transportation, and Utilities.**

1,000 respondents

3 regions (North America, Europe and APAC)

Breakdown of organizations

1,000-2,999 employees	47%
3,000-4,999 employees	19%
5,000-9,999 employees	18%
10,000+ employees	15%

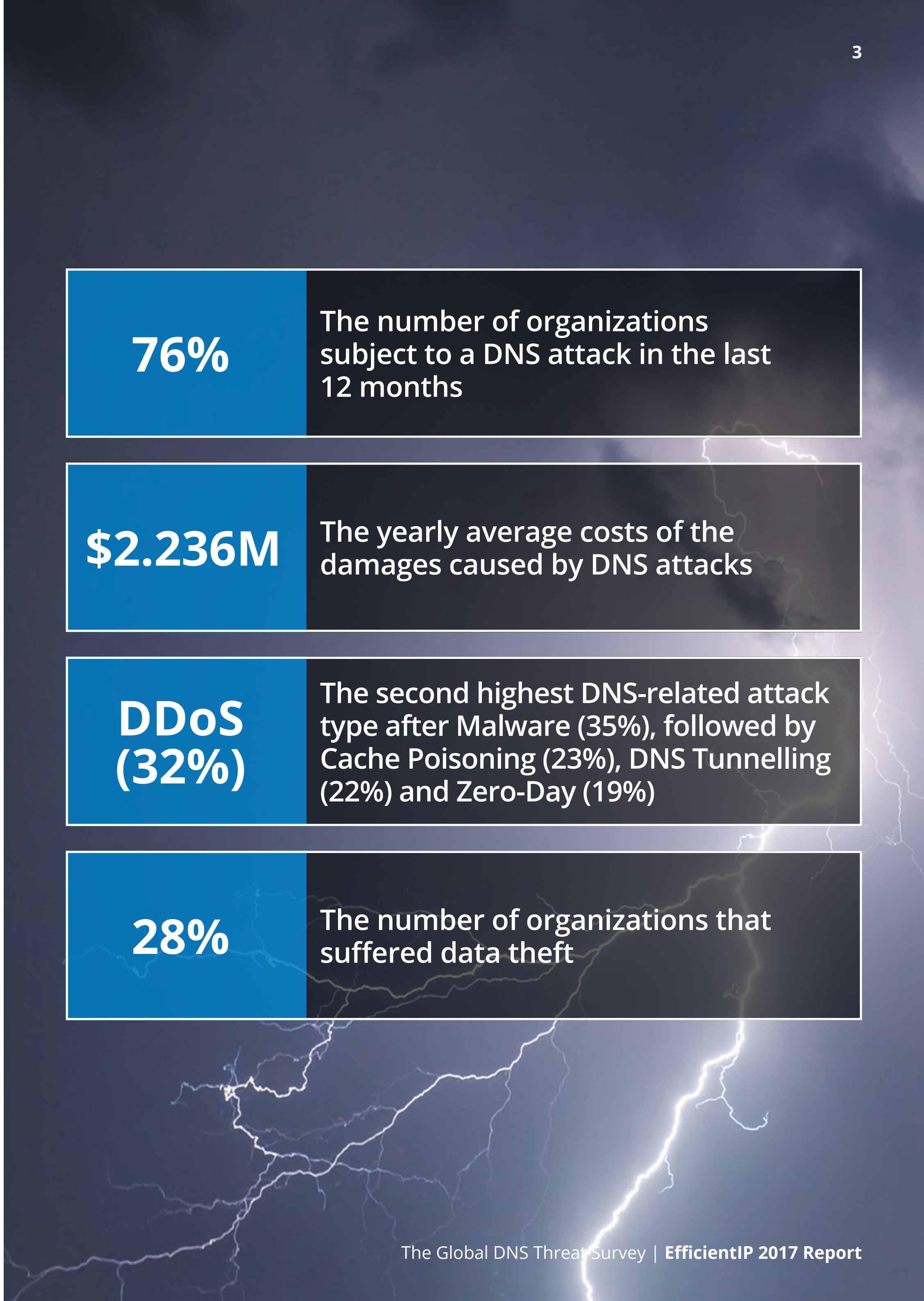
Executive Summary

Being one of the critical elements to deliver IT services, the DNS is increasingly a target of cyberattacks designed to cause downtime or simply cause business damage.

Additionally, the DNS is being used by attackers as a vector to, for example, exfiltrate data or launch a DDoS attack.

The threat landscape is constantly evolving; therefore, the way organizations manage, use, deploy and secure DNS services needs to evolve in response.

> “Worryingly, **76%** of organizations have been subject to a DNS attack in the past year according to our survey. Organizations must ensure they have the right solution in place to prevent business damage such as a loss of sensitive information, downtime or a compromised public image.”
>
> David Williamson, CEO of EfficientIP



76%	The number of organizations subject to a DNS attack in the last 12 months
$2.236M	The yearly average costs of the damages caused by DNS attacks
DDoS (32%)	The second highest DNS-related attack type after Malware (35%), followed by Cache Poisoning (23%), DNS Tunnelling (22%) and Zero-Day (19%)
28%	The number of organizations that suffered data theft

Today's Threat Landscape

As organizations are becoming more secure, attackers have had to become more creative. As DNS is mission-critical, but open by design and typically not monitored, it has become the perfect target to exploit it in as many ways as possible. Despite the reality of risks, companies are not sufficiently aware of the diversity of the menace.

It is clear that today's traditional security solutions do not efficiently protect DNS- they are not smart enough to effectively identify threats and have not been designed to defend it properly.

76% **of organizations surveyed have been subject to a DNS attack in the past year**
(74% in our 2016 survey)

49% **OF BUSINESSES ARE STILL UNAWARE OF DNS BASED MALWARE**
(91% of malware are using DNS - Cisco 2016 Security Report)

DOWN from 66% last year (2016)

Only **41%** of businesses were aware of **DNS DDoS attacks**
(38% in our 2016 survey)

- **The Utilities sector was the least aware (32% aware), Services the most aware (54% aware)**

Only **26%** of businesses were aware of **DNS Zero-Day vulnerabilities**
(24% in our 2016 survey)

- **The Finance sector was the least aware (16% aware), Services the most aware (35% aware)**

Only **38%** of businesses were aware of **Data Exfiltration through DNS**
(24% in our 2016 survey)

- **Manufacturing was the least aware (34% aware), Utilities, Retail and Services the most aware (43% aware)**

What You Should Be Worried About

The survey found 76% of organizations surveyed have been subject to a DNS attack in the last 12 months. It also shows they are facing a great variety of attacks. Here are three main attack types you should be worried about today:

DNS DDoS

32%
of respondents subject to attack
22% in our 2016 survey

"Recent massive DDoS attacks such as Dyn have highlighted the risks compromised Internet of Things (IoT) devices can pose as a new vector used by attackers to stop organizations from doing business online. This type of new threat can also come from inside the network so IT teams must quickly protect their internal DNS infrastructure."
David Williamson, CEO of EfficientIP

DNS Zero-Day

19%
of respondents subject to attack
13.1% in our 2016 survey

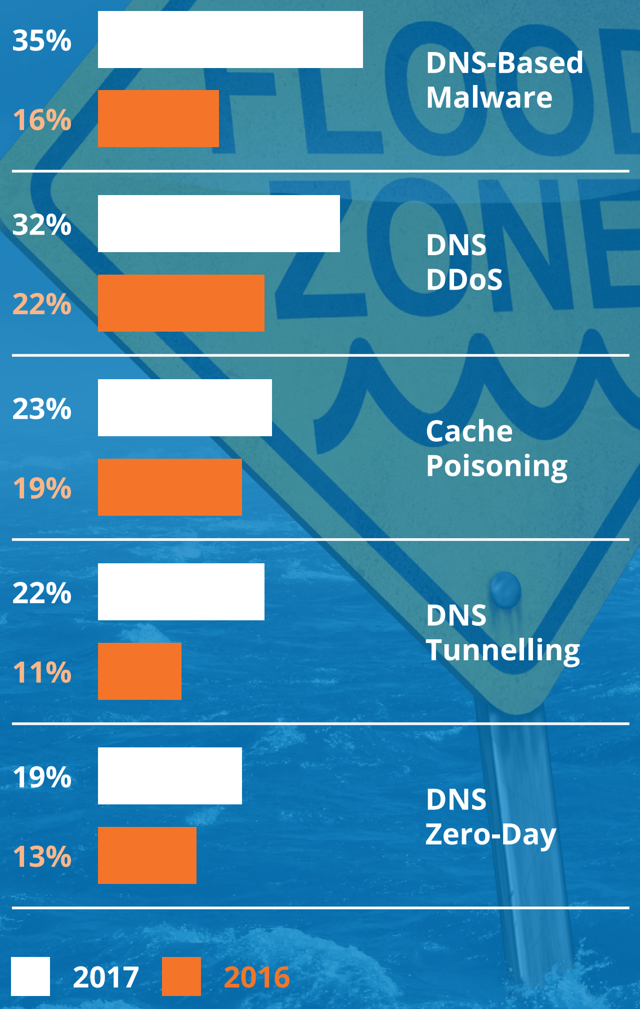
"Being one of the easiest attacks to execute, the increase of DNS Zero-Day vulnerabilities is not surprising. With one specifically-crafted DNS query only, an attacker is able to crash DNS servers and take down a business. The time taken by organizations to apply patches to BIND vulnerabilities is also helping attackers reach their goals."
Jean-Yves Bisiaux, CTO and Founder of EfficientIP

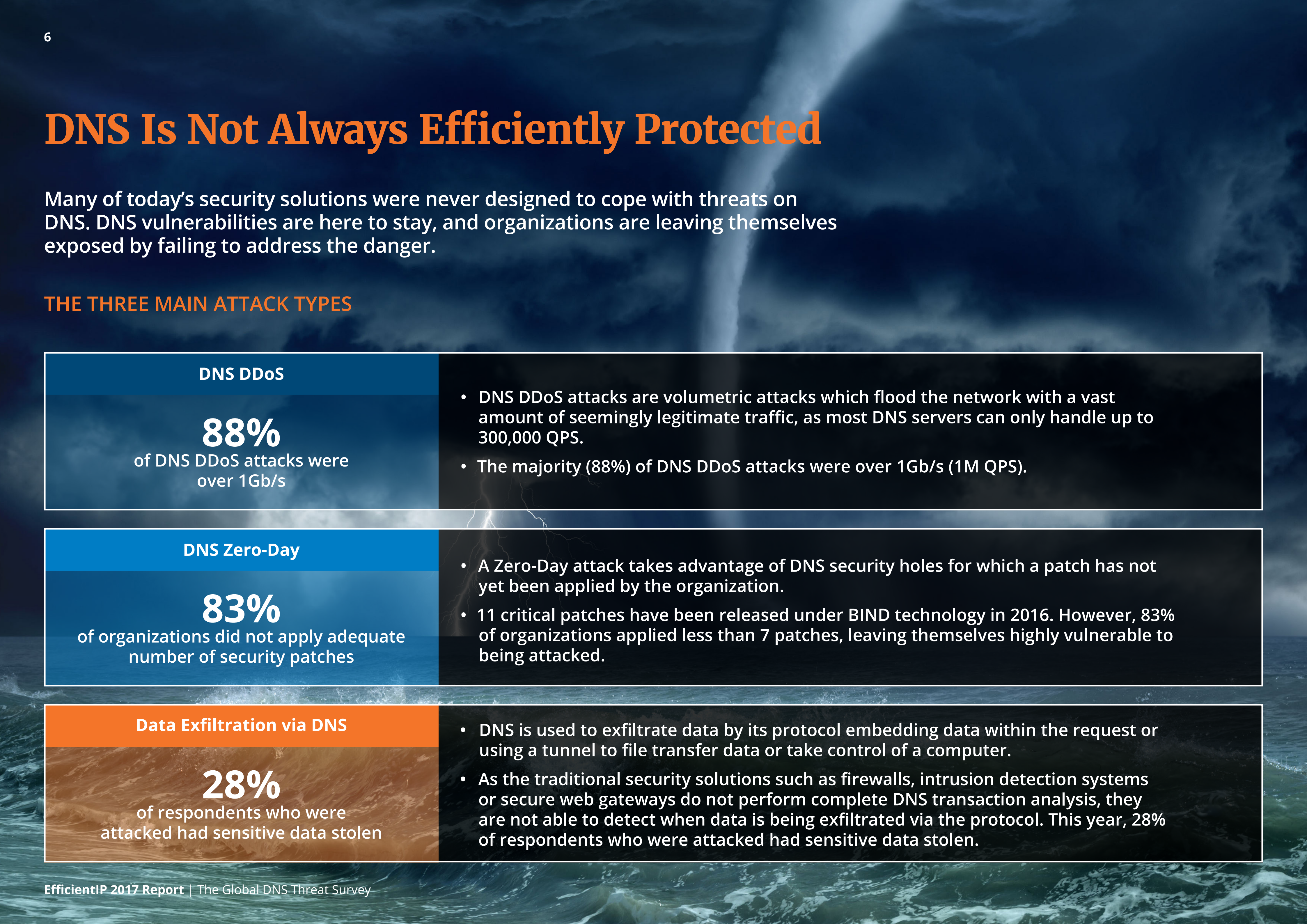
Data Exfiltration via DNS

28%
of respondents subject to attack
24% in our 2016 survey

"Organizations must therefore protect against attacks that attempt to exfiltrate data from their companies. Many organizations have security processes and technologies in place to guard against this. However, there are often gaping holes in protection due to the fundamental workings of the Internet."
IDC Technology Spotlight: Dealing with DNS-Based Data Breaches to Avoid GDPR Non-Compliance, 2017

Types of attacks organizations surveyed have suffered from





DNS Is Not Always Efficiently Protected

Many of today's security solutions were never designed to cope with threats on DNS. DNS vulnerabilities are here to stay, and organizations are leaving themselves exposed by failing to address the danger.

THE THREE MAIN ATTACK TYPES

DNS DDoS

88%
of DNS DDoS attacks were over 1Gb/s

- DNS DDoS attacks are volumetric attacks which flood the network with a vast amount of seemingly legitimate traffic, as most DNS servers can only handle up to 300,000 QPS.
- The majority (88%) of DNS DDoS attacks were over 1Gb/s (1M QPS).

DNS Zero-Day

83%
of organizations did not apply adequate number of security patches

- A Zero-Day attack takes advantage of DNS security holes for which a patch has not yet been applied by the organization.
- 11 critical patches have been released under BIND technology in 2016. However, 83% of organizations applied less than 7 patches, leaving themselves highly vulnerable to being attacked.

Data Exfiltration via DNS

28%
of respondents who were attacked had sensitive data stolen

- DNS is used to exfiltrate data by its protocol embedding data within the request or using a tunnel to file transfer data or take control of a computer.
- As the traditional security solutions such as firewalls, intrusion detection systems or secure web gateways do not perform complete DNS transaction analysis, they are not able to detect when data is being exfiltrated via the protocol. This year, 28% of respondents who were attacked had sensitive data stolen.

The Cloud Effect

Organizations are putting more and more trust into using hosted/cloud-based services.

IT infrastructures are rapidly shifting to a hybrid private/public cloud model. Cloud services are widely used in some form, with **93%**[1] of organizations utilizing Software-, Infrastructure-, or Platform-as-a-Service offerings.

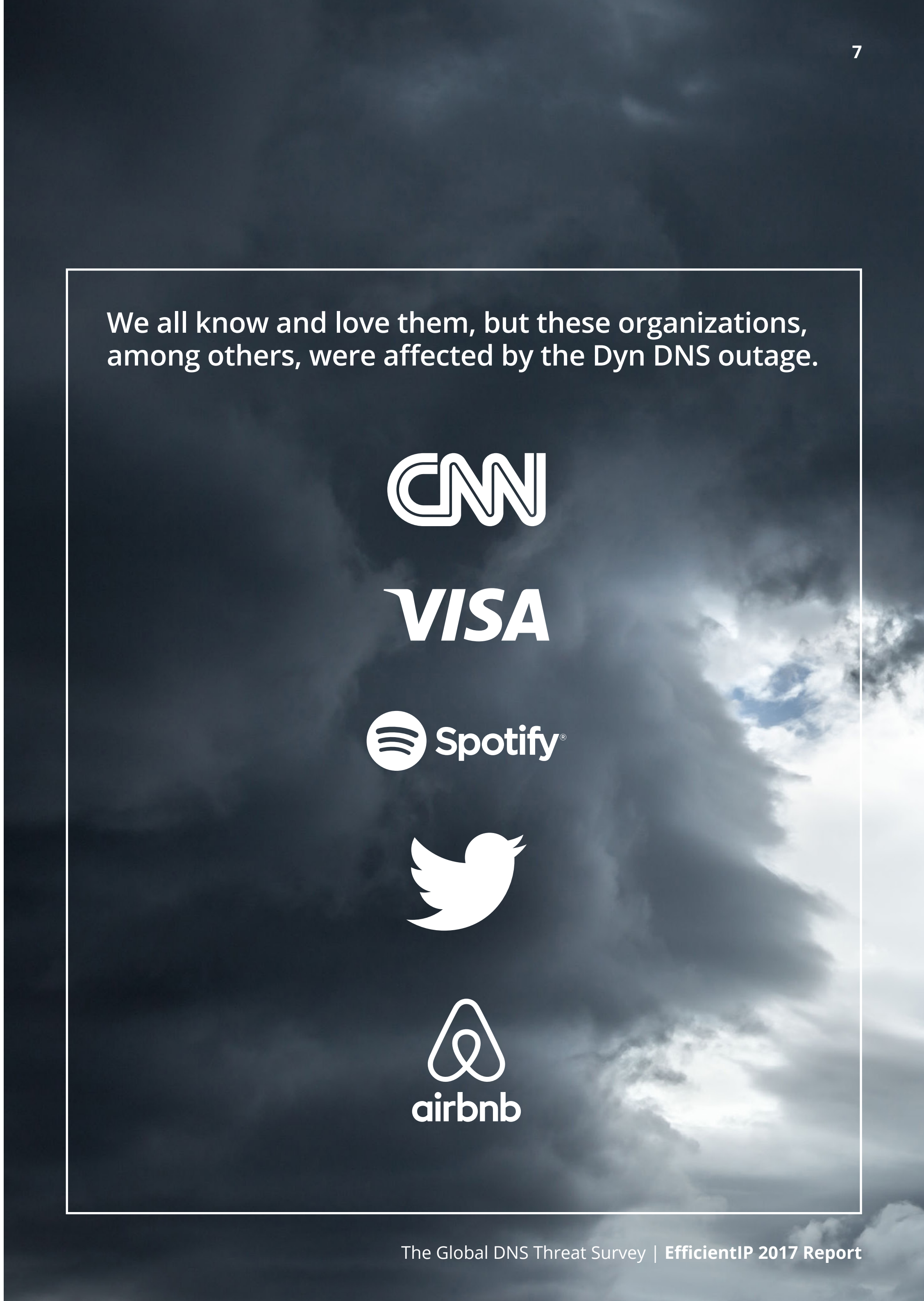
According to the Deloitte Technology, Media and Telecommunications Predictions, by 2018, **IT spending for IT-as-a-Service for data centers, software and services will represent 35%.**

However, whilst cloud services undoubtedly bring many benefits, they do also bring their own risks. According to our survey, **42% of organizations had suffered Cloud App Downtime** (includes private as well as public clouds) due directly to DNS attacks.

When cloud DNS provider Dyn was attacked and went down in 2016, those affected included some of the largest and most sophisticated e-commerce organizations on the planet. As they solely relied on Dyn for DNS services, they did not stand a chance.

Organizations should therefore not rely solely on hosted/cloud offerings when it comes to DNS services, but instead take a more hybrid approach. This entails setting up a mix of in-house and hosted /cloud DNS architecture for both public and private services to ensure business continuity.

[1] McAfee, Building Trust in a Cloudy Sky Report



We all know and love them, but these organizations, among others, were affected by the Dyn DNS outage.

CNN

VISA

Spotify

airbnb

What About Sectors?

The growing DNS threat means no sector is safe. When looking at the average cost of one single attack, the highest was for Communications organizations ($622K), followed by Financial Services ($588K). The lowest was for Healthcare organizations ($282K).

While some sectors had a higher cost of attack than others, the loss of intellectual property or data was equally as damaging for sectors such as Financial Services.

15% of **Financial Services organizations** were subjected to 5 attacks in the last 12 months. The impact of the attacks included sensitive customer information stolen **(17%)** and intellectual property stolen **(20%).**

24% of **Healthcare organizations** had sensitive customer information stolen, e.g. social security numbers. This was similar for Communications organizations **(25%).**

37% of **Retail organizations** experienced a DNS-based malware attack in the last 12 months. **47%** of attacks resulted in cloud service downtime and **37%** resulted in a compromised website.

20% of **Public Sector organizations,** including Universities, had intellectual property stolen and **19%** had sensitive customer information stolen, e.g. social security numbers, job assignments, performance ratings.

39% of **large Manufacturing organizations** suffered from a DNS DDoS attack in the last 12 months. Major consequences for manufacturers included loss of business **(20%).**

The Business Impact Of DNS Attacks Around The World

The yearly average costs of the damages caused by DNS attacks for organizations with 3,000+ employees:

$2,236,000

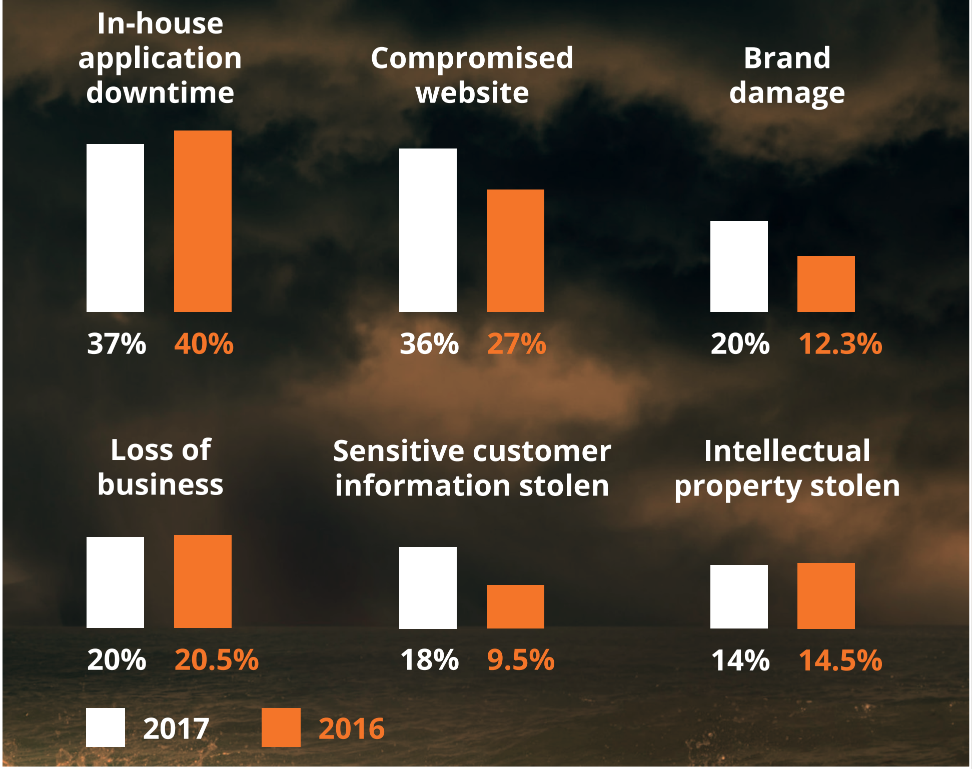
IN 2017

Despite the dangers to business, organizations are still not taking the right measures to respond. While actions might have been taken to mitigate the effects of attacks, they were still unable to stop them.

As an example, the cost of the damages caused by a DNS attack for a small organization (1,000 to 2,999 employees) is $277k, while the total yearly cost is $983k.

The time to mitigate DNS attacks is also significant - on average more than 5 hours. 45% of all organizations surveyed spent more than half a day resolving an attack.

Effects of DNS attacks in 2017 vs 2016



The best of the worst mitigating actions:

1. Shutdown server or service
2. Disabled some applications
3. Closed down specific affected processes and connections

Organizations Of All Size Are Affected

Nobody is safe. Hackers seem to attack any organization, regardless of their size or industry. The frequency and impact of attacks is becoming more and more important, as shown by the following table.

Company size Cost of attack	1,000-2,999	3,000-4,999	5,000-9,999	10,000-49,999
$500k -$5M	12%	26%	34%	30%
5-10 Attacks	24%	31%	41%	37%

Medium size organizations, with 5,000-9,999 employees, such as a large university or a retailer, will be most affected. While an attack can cost a lot to a large organization, they are typically able to recover based on overall revenue and resources. For a smaller size organization, however, it is much harder to recuperate financially.

34%

of attacks on medium size organizations cost between $0.5M to $5M

What EfficientIP Recommends

THE RIGHT APPROACH: A DNS SERVER THAT SECURES ITSELF

An unsecured DNS architecture is an invitation to attackers that can result in data exfiltration, loss of business and application downtime.

It is critical that any security solution is designed and deployed to ensure continuity of service and data protection. To do so, here are five steps you can take today:

	STEPS	HOW	BENEFITS
1	**Simplify your DNS architecture and add high-performance capability**	Replace useless firewall and load balancers with purpose-built DNS security technology	Increased resiliency, lower TCO. Absorb large volumes of traffic, protect against extreme attacks
2	**Eliminate single points of failure**	Deploy Hybrid architectures combining different DNS engines	Mitigate zero-day attacks by switching in real-time from one DNS engine to another
3	**Enhance your threat visibility**	Use real DNS transaction analytics	Detect Stealth attacks, prevent data theft, ensure GDPR compliance
4	**Apply adaptive countermeasures**	Provide graduated security measure according to threats: block, RRL, quarantine and rescue mode	Ensure business continuity, mitigate risks of false positives
5	**Keep your DNS Security up to date**	Implement efficient industrialized process to patch your DNS servers as often as required	Comply with security best practices and limit vulnerabilities

Protect Your Business Today

Having looked at the findings, do you still think your DNS infrastructure is really secure?

Although preventing all attacks cannot be solved by just the previous actions, it is a good start to help pave the way to the creation of a more versatile and secure solution.

Read what IDC is saying about DNS-based data breaches

www.efficientip.com/resources/white-paper-idc-gdpr

Check out our customer successes

www.efficientip.com/resources

Request a DNS security demo

www.efficientip.com/request-a-free-trial

efficient iP™
DEFINING SMART DDI