imperva 2019 Cyberthreat Defense Report

INTRODUCTION

In November 2018, over 1,200 qualified IT decision makers and practicioners — from 17 countries and 19 industries — responded to an online survey intended to guage their perception of cyberthreats and evaluate how their organizations are working to defend against them. Here's what we learned...

CYBERTHREAT HEADACHES

Some of the leading cyberthreats keeping IT security teams up at night.

- Accout takeover attacks
- Denial of service attacks
- Web application attacks
- Insider threats

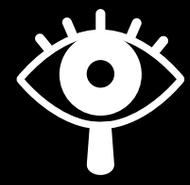
SECURITY'S BIGGEST OBSTACLES

These obstacles inhibit IT from defending cyberthreats.

- Too much data to analyze
- Lack of skilled personnel
- Low security awareness among employees

PROCESS INSECURITIES

One of the IT security processes organizations struggle with the most:



Detection of rogue insiders / insider attacks

APP & DATA SECURITY FOUNDATIONS

The most commonly used technologies for protecting applications and data:

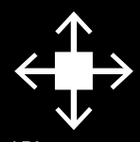
Web application firewall (WAF)

Database firewall

Data activity monitoring (DAM)

APP & DATA SECURITY ACQUISITIONS

Two of the top application and data security technologies targeted for acquisition in 2019 are:



API gateway/ protection

Runtime application self-protection (RASP)

SECURITY MANAGEMENT ACQUISITIONS

The top security management and operations technologies targeted for acquisition in 2019 are:

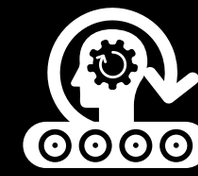
Advanced security analytics

Threat intelligence service(s)

MACHINE LEARNING MATTERS

Machine learning and artificial intelligence technologies are here to stay.

94%
Organizations already using them



81%
Believe they are making a difference

DDOS PROTECTION PLANS

Defending against denial of service attacks remains a top priority.

55%
Already deployed

DDoS Prevention

32%
Plan to acquire in 2019

DOWNLOAD THE FULL REPORT AT:
www.imperva.com/cdr2019

CYBEREDGE GROUP