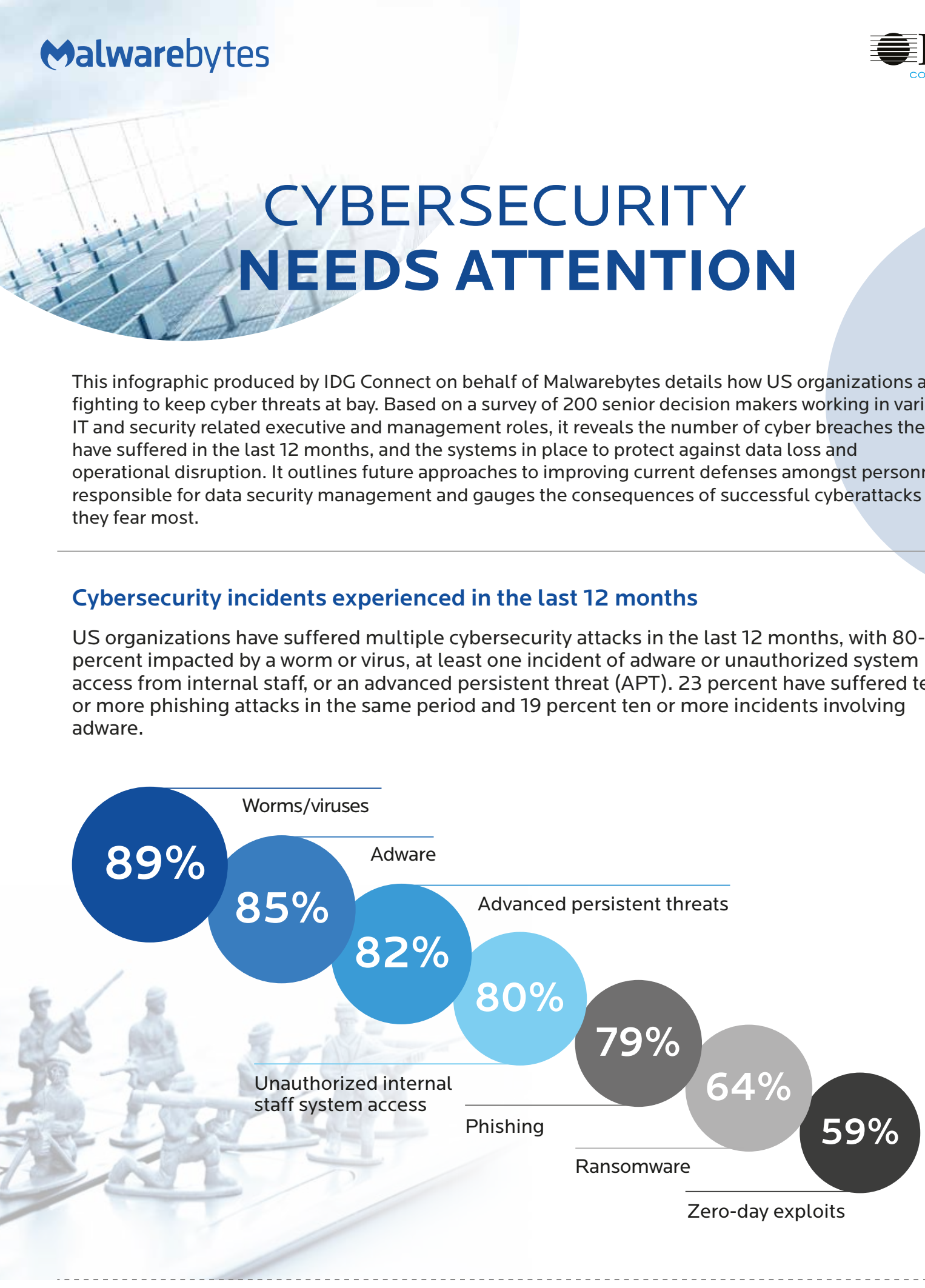
# CYBERSECURITY NEEDS ATTENTION

This infographic produced by IDG Connect on behalf of Malwarebytes details how US organizations are fighting to keep cyber threats at bay. Based on a survey of 200 senior decision makers working in various IT and security related executive and management roles, it reveals the number of cyber breaches they have suffered in the last 12 months, and the systems in place to protect against data loss and operational disruption. It outlines future approaches to improving current defenses amongst personnel responsible for data security management and gauges the consequences of successful cyberattacks they fear most.

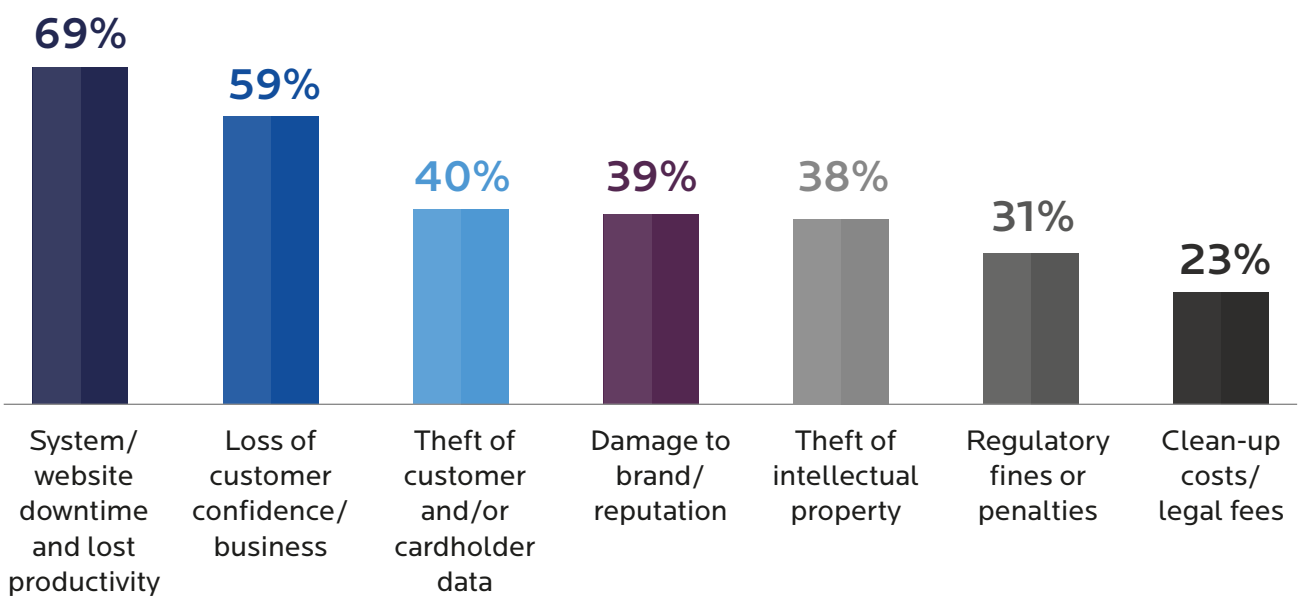
## Cybersecurity incidents experienced in the last 12 months

US organizations have suffered multiple cybersecurity attacks in the last 12 months, with 80-90 percent impacted by a worm or virus, at least one incident of adware or unauthorized system access from internal staff, or an advanced persistent threat (APT). 23 percent have suffered ten or more phishing attacks in the same period and 19 percent ten or more incidents involving adware.



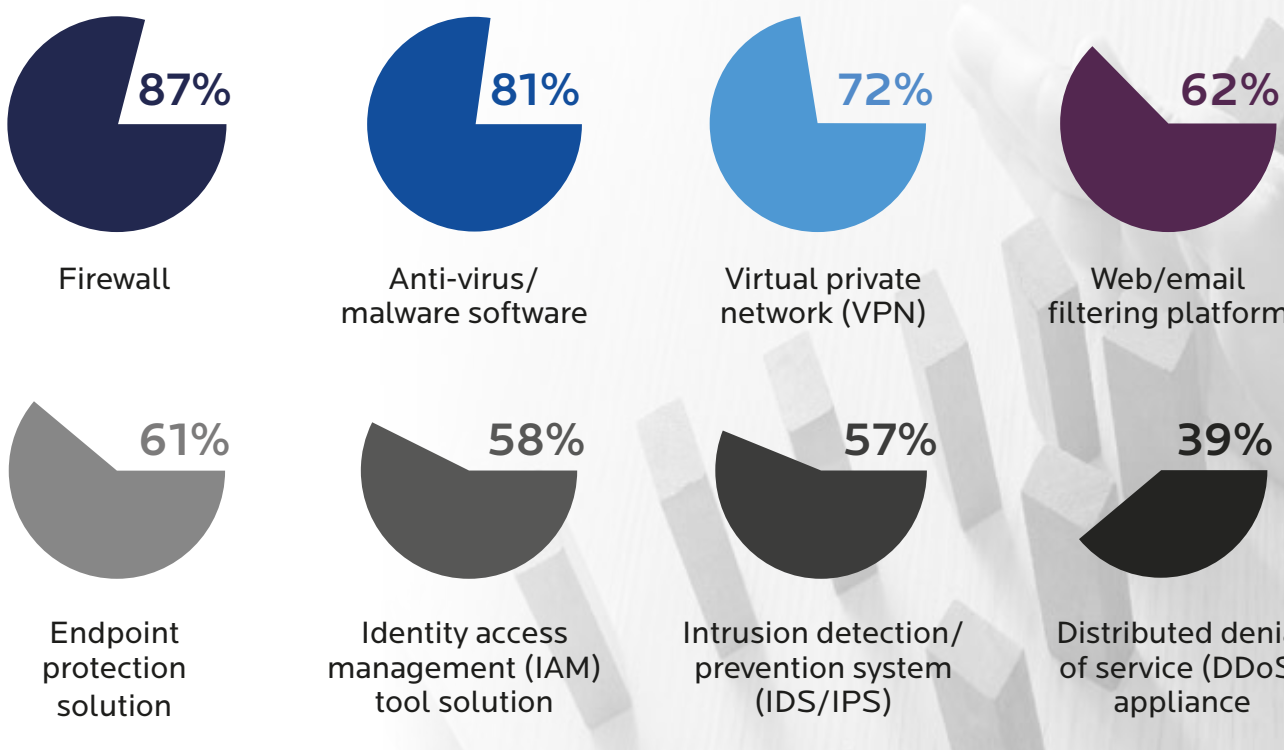

## Downtime and lost customers are expensive consequences

The fallout of successful cyberattacks can be severe, but the financial losses associated with system/website downtime, lost staff productivity and customer desertion cause more widespread concern. Organizations also fear that theft of customer or cardholder data will lead to fines from regulators, and worry about the commercial effects of their intellectual property falling into the wrong hands.



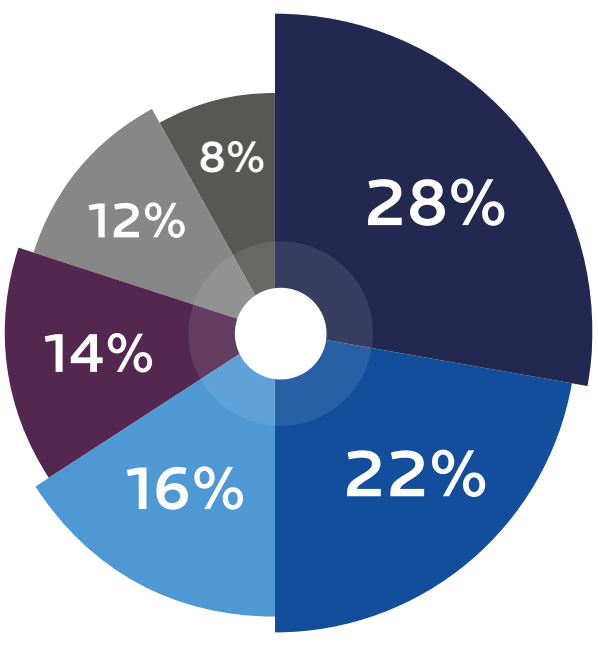

## Existing cybersecurity defenses are not bulletproof

Multiple and successive layers of cybersecurity defenses have been added to most organizations' infrastructure over time, but they still fail to stop every incident impacting the business. Managing an intricate mesh of different security solutions from different vendors can be complex and time consuming for IT departments tasked with their ongoing configuration and maintenance.




## Focus on updating existing systems risks overlooking proactive solutions

Organizations identify different ways to improve their current cybersecurity defenses. Yet given a binary choice of investment, more will spend money on updating and patching applications, hardware and services already being used rather than bringing in additional systems, a course of action that risks overlooking new, proactive approaches like threat hunting.




- Upgrade current security systems
- Investment in additional security hardware/software/services
- Spend more time application/ system vulnerability testing
- Allocate more staff to cybersecurity maintenance/management
- Proactively engage in threat hunting to identify undetected threats
- Increase or improve security awareness training for end users

## Security management begins with IT managers and CISOs

Responsibility for cybersecurity management most often rests with IT managers and CISOs. Staff holding these roles face a difficult task in maintaining adequate protection against cyberattacks and meeting regulatory requirements whilst simultaneously keeping the financial and administrative overheads involved down to a manageable level.