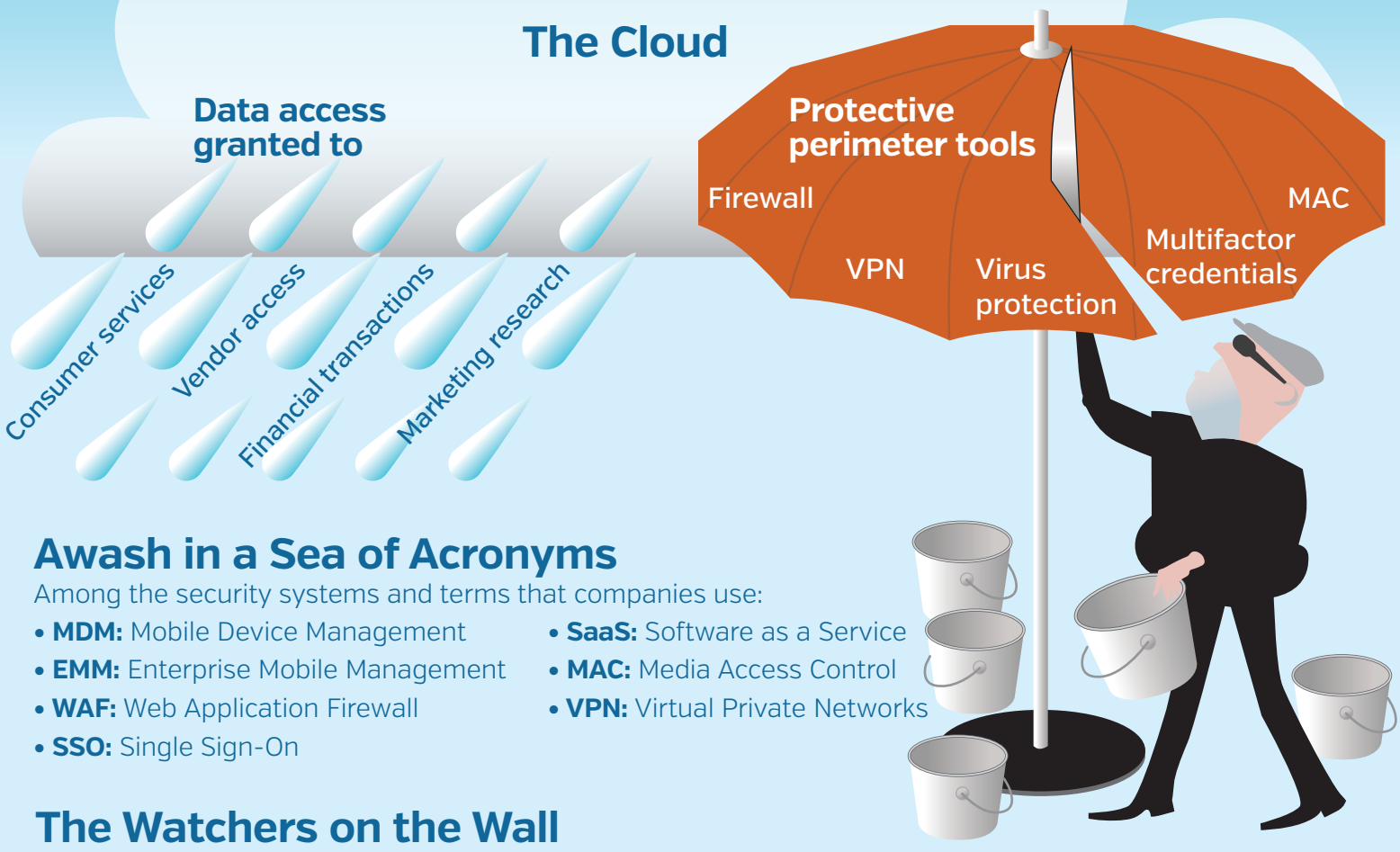
Compromised Credentials Can Cause Cloudbursts

Strong Perimeters Needed to Protect Data

The exposure of sensitive data can damage any size company. As consumers use more and varied digital devices, and as attacks become more sophisticated, companies must seek new security strategies. Controlling the cloud environment ensures that individuals only have access to the data they need, adding a security buffer.
A survey by the Cloud Security Alliance, a nonprofit that promotes best practices to safeguard information, looked at how companies address access management to gain a better understanding of enterprise security.



Awash in a Sea of Acronyms

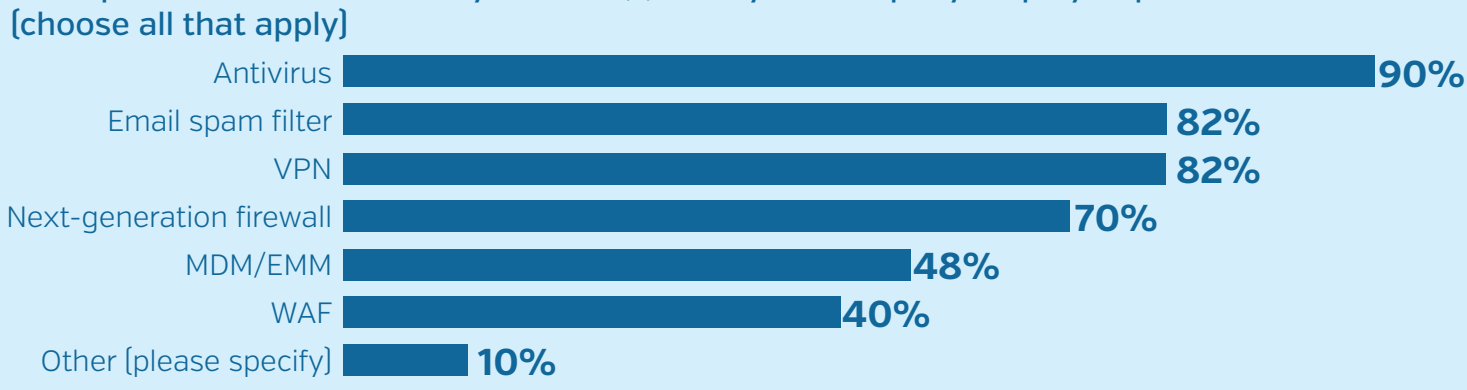
Among the security systems and terms that companies use:

- **MDM:** Mobile Device Management
- **EMM:** Enterprise Mobile Management
- **WAF:** Web Application Firewall
- **SSO:** Single Sign-On
- **SaaS:** Software as a Service
- **MAC:** Media Access Control
- **VPN:** Virtual Private Networks

The Watchers on the Wall

Perimeter-based security protects a company network along entry- and exit-access points. More than 70 percent of companies surveyed said they used such tools, and many use three or four.

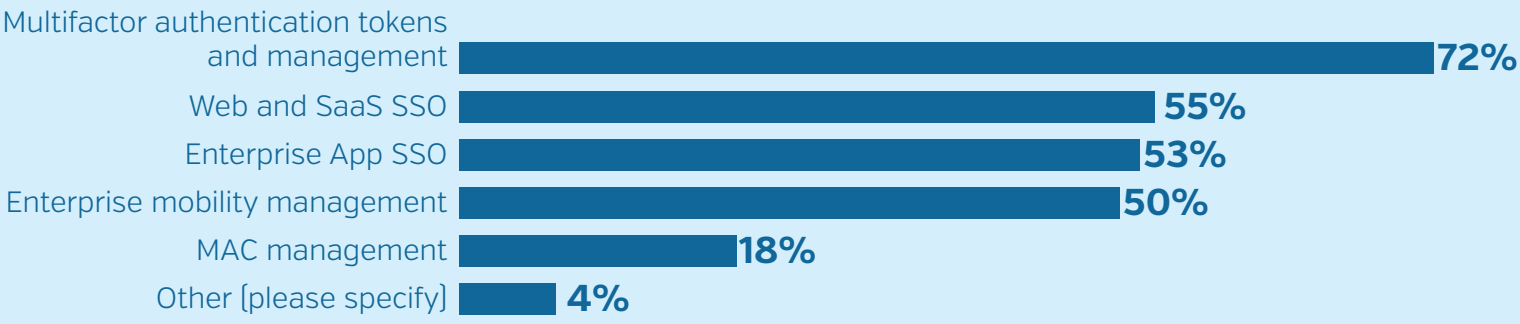
What perimeter-based security solution(s) does your company employ to protect its network? (choose all that apply)



Care for Consumers and Customers

About 74 percent of companies require users to access their data through multifactor authentication, the most commonly used safeguard. Many also use additional tools.

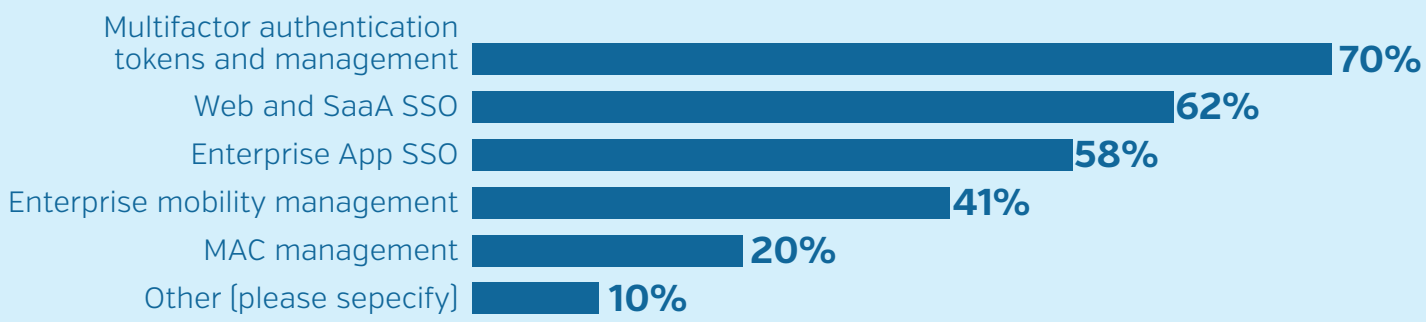
What access controls/processes does your company have in place to protect end users?



Big Data Needs Dense Defenses

Companies are adopting cloud services to process and analyze large volumes of data, which can process information faster and at greater volumes. Access to, and use of, such massive data stores requires increased security.

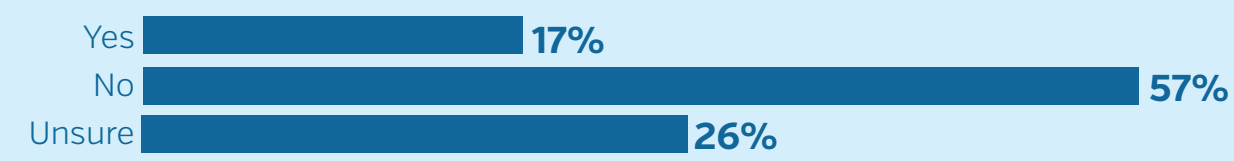
What big data access controls/processes does your company have in place to protect private users?



Cause and Effect

Nearly a quarter of those surveyed (22 percent) said a breach was due to compromised credentials, with 65 percent saying the likelihood of a future breach due to compromised credentials was medium to high.

Has your company ever reported a data breach?



Was the data breach your company experienced due to compromised credentials?

Source: Identity Solutions: Security Beyond the Perimeter, a study by the Cloud Security Alliance

IDT911