HPE GreenLake

Best practices from high-performing security teams

How are businesses defending against threats in today's edge-to-cloud environments? The Ponemon Institute surveyed more than 1,800 cybersecurity professionals to find out.[1] Here are some responses from participants who reported that their organization is highly effective:

01

56%

recognize the potential damage from attacks that have reached inside the network

But only 45% of non-high-performers say they recognize this as a threat. 47% of high performers are confident that their organizations have not experienced a persistent threat below the platform software that has resulted in data stolen, modified or viewed by unauthorized entities. However, only 30% of non-high-performers say the same.

02

88%

say backup and recovery is key

And 68% of high performers say their organizations make server decisions based on the security inherent within the platform.

03

64%

utilize a Zero Trust model

25% chose a Zero Trust model because government policies required it, and 24% for other reasons. 15% say they selected elements from the Zero Trust framework to improve security.

04

78%

say a key benefit of automation is its ability to find attacks before they do damage or gain persistence

In addition, 74% of high performers identified a reduction in false positives as an important benefit. 71% said automation is critical when implementing an effective Zero Trust model.

05

85%

say identifying and authenticating IoT devices on the network is critical

But only 55% of non-high-performers agree. 40% of high performers say their IoT devices are appropriately secured, vs. 15% of non-high-performers.

06

94%

say it is not possible to have privacy without a strong security posture

87% of high performers believe a strong cybersecurity posture reduces the privacy risk to employees, business partners and customers. High performers are less likely to believe human error is a risk to privacy.

07

59%

say they get full value from their security investments

Only 42% of non-high-performers say the same. However, both groups agree that the IT infrastructure has gaps that allow attackers to penetrate defenses (60% of high performers, 61% of non-high-performers).

08

77%

say security technologies are important or highly important for digital transformation

35% say these technologies are important for transformation strategies; 42% say they are highly important. In contrast, only 53% of non-high-performers say they are important or highly important.

Make the right purchase decision. Contact our presales specialists.

Chat now (sales)

Call now

Get updates

Learn how HPE can help you manage cybersecurity risk—wherever your apps and data may live

greenlake.hpe.com/security

[1] The 2022 Study on Closing the IT Security Gap: Global, Ponemon Institute, January 2022

a50006309ENW