SPONSORED CONTENT | WHITE PAPER

Market Pulse

Secure device access: The missing key to your security strategy

CIO

SPONSORED BY okta

A growing problem

The proliferation of portable devices has magnified the cybersecurity challenges facing organizations of all sizes. Globally, the average person now uses 3.6 personal and work-related devices, and in North America, the figure is a stunning 13.4.[1] The challenges of managing and securing IT assets have been amplified by "bring your own device" policies at 85% of organizations, accelerated in part by shifts to remote and hybrid work arrangements.[2] As a result, IT organizations often no longer manage — or are even aware of — every device that accesses corporate resources.

To better understand device access and management challenges facing organizations of all sizes, Okta commissioned Foundry to survey 150 IT security decision-makers across a spectrum of small, mid-sized, and large businesses.

Struggle to control

The results indicate that IT groups need help with this issue. An overwhelming 94% said their businesses have been negatively impacted by unauthorized devices or system access, with ransomware being their top device-related security concern. One in five security incidents originates from a lost or stolen asset. This indicates that the inability to fully lock down or block access to employees' and contractors' devices poses a severe security risk.

Over 40% worry about unauthorized access to corporate-issued devices, and nearly as many are concerned about access to personal devices used at work. Large organizations expressed more significant concerns about this issue than small ones, probably because of the volume of endpoints in use.

1 Statista. Average number of devices and connections per person worldwide in 2018 and 2023. https://www.statista.com/statistics/1190270/number-of-devices-and-connections-per-person-worldwide

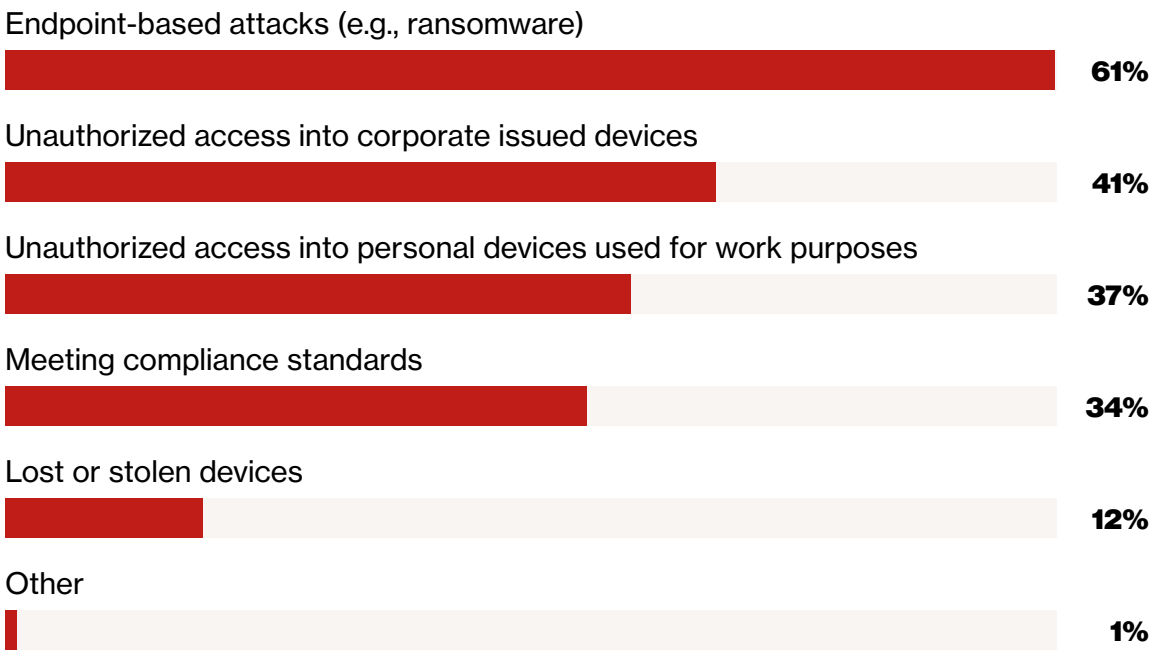
2 Balcik, C. Mobile devices and your employees: To BYOD or not to BYOD? May 31, 2023. https://insights.samsung.com/2023/05/31/mobile-devices-and-your-employees-to-byod-or-not-to-byod/

Over half of those responsible for access management said tracking, managing, and securing device inventory is a top pain point.

Other top concerns include inconsistent application of security policies across devices and time-consuming password reset and recovery processes. Over half of security decision-makers said access violations cause downtime, and nearly half have experienced data loss. About one-third also cited increased help desk hours, lower productivity, and reduced revenue.

The wide range of these challenges illustrates the broad-based risk created when organizations fail to prioritize device access management.

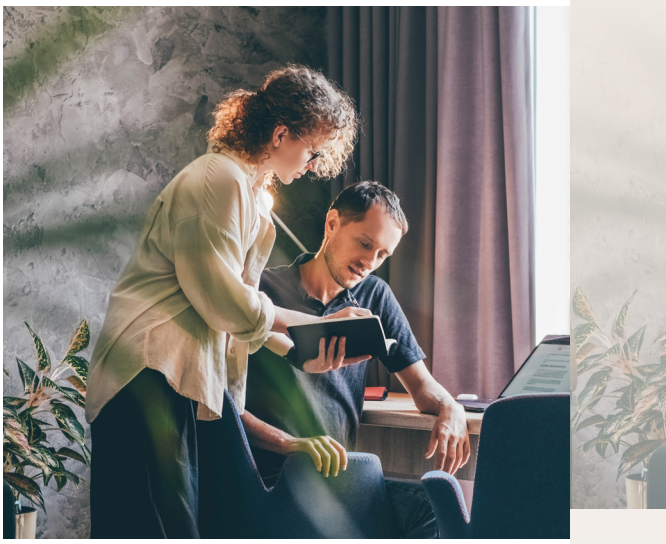
Top concerns regarding device security (select two)



SOURCE: FOUNDRY MARKETPULSE SURVEY FOR OKTA, SECURE DEVICE ACCESS, FEBRUARY 2024

Permissive device usage needs to be accompanied by robust visibility and controls. Security leaders know this. Two-thirds of their organizations use Identity and Access Management (IAM), a solution for ensuring that the right users have appropriate access to the technology resources they need. A slightly smaller number (61%) employ Endpoint Detection and Response (EDR), a technology that continuously monitors devices for threats. With the average cost of a data breach now nearly $4.5 million, it is unsurprising that big companies opt to combine multiple protection methods to enhance security.[3]

Smaller organizations lag behind their large peers in deploying these technologies, a finding that is not surprising given their limited resources. For example, nearly three-quarters of enterprises use IAM compared to only 52% of small businesses. The only area in which small companies lead their enterprise counterparts is a dubious one: the use of manual processes.



Businesses that rely on spreadsheets and paper records for device access management are easier targets for attackers.

Solutions are being adopted slowly

Three device access features are gaining wider acceptance.

- Desktop multi-factor authentication (MFA) requires two or more verification factors from different categories: something known (like a password), something possessed (like a mobile phone), and/or something they are (like a fingerprint).

3 IBM, Cost of a Data Breach Report 2023. https://www.ibm.com/reports/data-breach

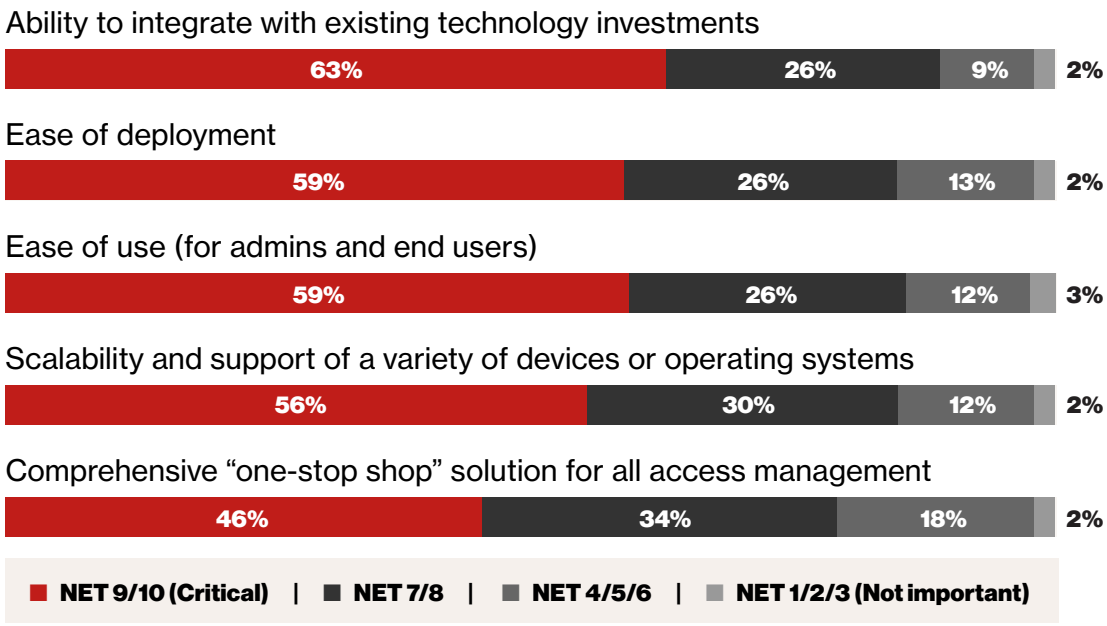
- Passwordless login may piggyback on desktop MFA technology but uses only passwordless verification forms such as biometrics or a mobile authentication app.

- Device single sign-on (SSO) allows a user to initiate a session that starts at device login and enables access to downstream resources without reauthentication unless required by security policies.

Although more than 90% said their organizations plan to adopt or use at least one of these measures, less than 30% have deployed any across the company. About half are using desktop MFA and/or passwordless login, but only roughly 25% have deployed either enterprise-wide. For both technologies, 21% confine usage to a single business unit, and 28% are in the investigation phase. Device SSO is in enterprise-wide use at 29% of organizations and within a single business unit at 28%, with 19% investigating and 21% planning to adopt.

Respondents said multiple factors are important when choosing a device access management solution. This is evident from the 85% to 89% who rated four factors as critical or very important: the ability to integrate with existing technologies, ease of deployment, ease of use, and adaptability across various devices or operating systems. Smaller organizations that lack enterprise-scale resources rated deployment simplicity and ease of use as important to a greater degree than their larger peers.

Important factors when choosing a device access management solution



SOURCE: FOUNDRY MARKETPULSE SURVEY FOR OKTA, SECURE DEVICE ACCESS, FEBRUARY 2024

Recommendations

Mobility is an essential part of business today. Companies that want to optimize the productivity benefits of always-on connectivity need to do so in the context of effective and unobtrusive security solutions.

Look to IAM solutions that protect applications and devices with consistent security policies and integrate with existing endpoint solutions to ensure visibility and comprehensive threat detection.

Those capabilities are ideally paired with native, passwordless protection that provides identity-based secure access to all resources, from apps to devices with a choice of authenticators, including phishing-resistant options. The combination of these technologies addresses the most common security concerns and provides an extensible foundation for addressing whatever new challenges may emerge.

Visit Okta to learn more about **secure access to devices.**