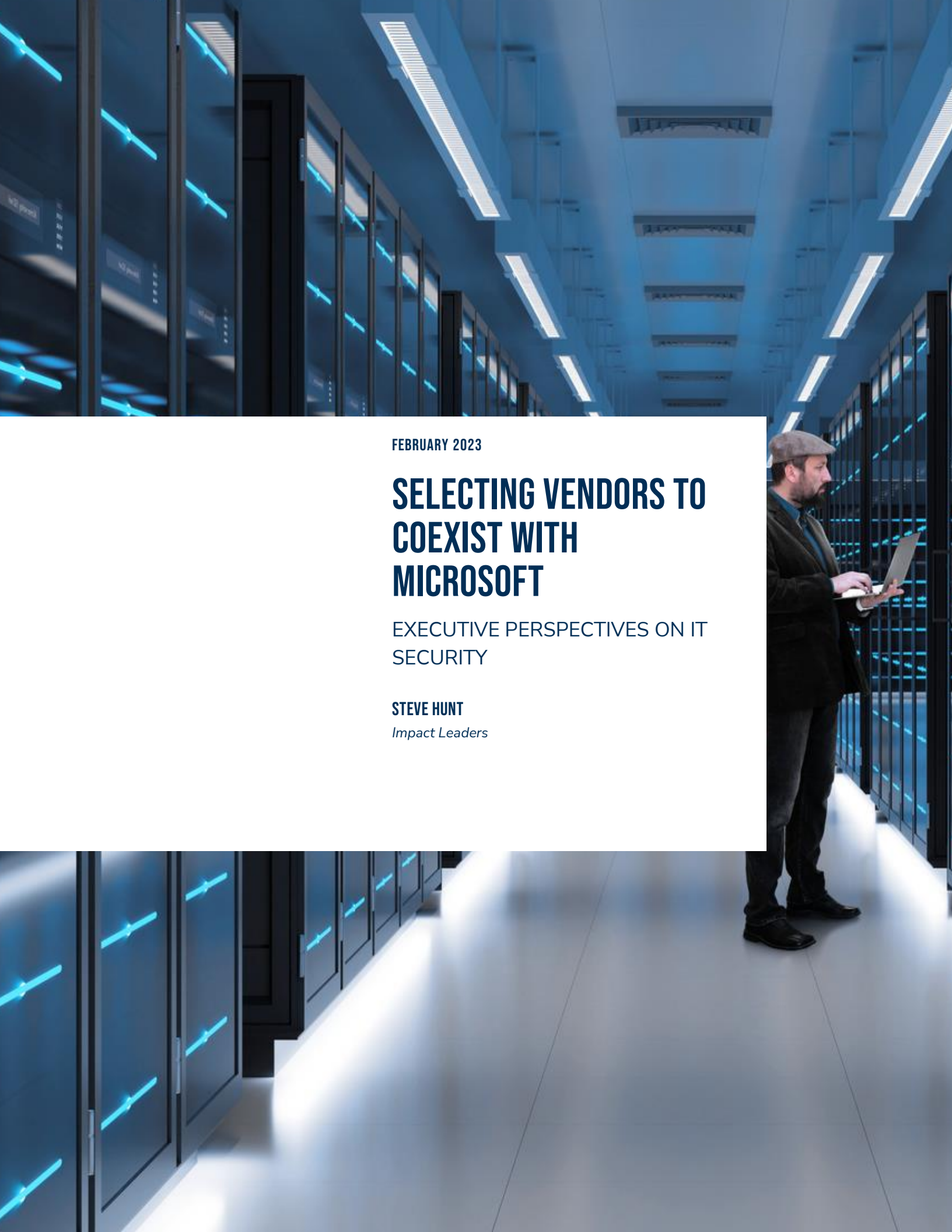

FEBRUARY 2023

SELECTING VENDORS TO COEXIST WITH MICROSOFT

EXECUTIVE PERSPECTIVES ON IT SECURITY

STEVE HUNT

Impact Leaders

INTRODUCTION

Microsoft is upping its game in identity and access – and security in general. However, some highly informed CISOs avoid relying on Microsoft for security. How should CISOs make the most responsible decisions for security, while also taking advantage of Microsoft's security features?

Impact Leaders interviewed 25 executives in large enterprises on their plans for 2023 and their perceptions of the current state of identity management, multifactor authentication (MFA), and the role of Microsoft in an identity and access management (IAM) strategy.

- Respondents were senior leaders: 21 CISO/CSO/CTO, 4 IAM executives
- Companies were large, with an average annual revenue of US$42bn
- Industries were diverse, with 11 in financial services and 14 in a mix of high tech, consumer products, services, and other industries

In this report, we share

- CISOs' key concerns on MFA, identity management, and Microsoft
- Logical and emotional approaches to selecting an IAM solution
- How CISOs decide between an independent IAM solution or Microsoft
- How most large-enterprise CISOs seek IAM solutions to complement Microsoft

HOW CISOS PERCEIVE MICROSOFT SECURITY

Microsoft is leveraging its ubiquity and claiming comprehensiveness in its offering – every major organization interviewed for this report invests heavily in Microsoft infrastructure,

Microsoft 365 E5 is Microsoft's newest and most powerful suite of applications and includes state-of-the-art security capabilities. Although it doesn't come cheap: compared to the standard workforce suite of applications (Microsoft 365 Business, @$6/user), E5 is a tough pill to swallow at $57 per month per user.[1]

On the other hand, Microsoft does security well. Since the launch of Microsoft Defender in 2006, the security suite has gotten better and earned respect of the security profession with a seemingly comprehensive security offering (Table A).

TABLE A: SELECT FEATURES OF MICROSOFT SECURITY PORTFOLIO

Cloud access security broker	Information protection	Privileged access management
Security analytics and reporting	Endpoint and app management	File and disk encryption
Multifactor authentication	Identity verification	Endpoint protection
Anti-malware	Firewalls	Threat protection
Cloud app security	Data loss prevention	Passwordless login

[1] See Microsoft price comparison page. https://www.microsoft.com/en-us/microsoft-365/compare-microsoft-365-enterprise-plans

When ransomware was the talk of the town, Microsoft beefed up its identity and access capabilities in Azure and strengthened endpoint detection and response (EDR). At the same time, corporate executives were wowed by Windows Hello for Business, almost entirely removing passwords from day-to-day morning logins. It is no wonder that CFOs would ask “why can’t we replace CrowdStrike with Microsoft's EDR? Why don’t we replace Cisco Duo with Microsoft’s MFA?”

> *“Why can’t we just use Microsoft for everything? After all, we are paying a lot of extra money for CrowdStrike, where we get EDR within E5 for no extra money.”*

"**But that's not entirely true," says one Fortune 100 CISO**. "**The devil is in the details**" of Microsoft licensing. While it appears that Microsoft Defender provides a suitable solution, Microsoft makes the licensing very challenging to understand.

> **“It would be more expensive for us to switch to (Microsoft) E5 entirely because the license only secures the files, not the servers. But in our case, when we have more servers than workstations, that makes Microsoft more the twice the cost of [our current solution]” (emphasis added).**

Cost is one part of the equation, and quality the other. Just how good is the security of Microsoft E5 really? CISOs interviewed by Impact Leaders reported a consensus: CISOs are more confident in, for example, Crowdstrike’s ability to deliver the control they want from an EDR solution. In fact, they are more confident in many non-Microsoft solutions than the solutions of E5. 91% said they routinely seek products to complement Microsoft’s offering.

However, just like when Microsoft introduced Defender’s first antivirus solution and CISOs decided to run it in parallel with their own preferred solutions, like McAfee or Symantec antivirus, the same holds true today. CISOs will use their preferred vendor for, say, EDR or identity and access management, and they will activate the analytics and logging of the Microsoft solution. They believe Microsoft’s telemetry to be second to none since it is baked into the operating system.

That’s the current state. CISOs continue to respect and appreciate Microsoft security solutions and use them as complementary to their preferred vendor solutions.

“Marrying the two gives us an overall better solution.” – CISO, financial services

HOW CISOS FEEL ABOUT MICROSOFT MFA

The crown jewel of any identity and access management (IAM) fabric is the strong authentication of users. Multifactor authentication nowadays integrates with single sign-on, traditional applications, mobile devices, and of course, Microsoft. 19% of CISOs interviewed say strong authentication is used across all their workforce passwords. Over half of CISOs (57%) estimate usage at 75% of all logins or higher. However, the quality of popular MFA solutions is not a reason to rejoice. Only 30% feel very confident in the protection of their workforce credentials.

Moreover, getting everything to work together is where some IAM providers fall short. Two-thirds of large organizations have more than one IAM provider. Some have as many as six. While fewer than 20% of CISOs say they are aggressively pursuing a migration of their infrastructure to the cloud, nearly all say they are attracted to hybrid security solutions that bridge on-premises applications with their counterparts in the cloud.

That explains why CISOs are clearly trending toward FIDO Alliance open authentication standards, such as WebAuthn, to ease integration challenges across applications. In the last two years, CISOs went from 10% favoring FIDO to over 60%. Over half say they believe FIDO represents the future of authentication.

Nevertheless, most CISOs – and probably all CFOs – fail to understand what Windows Hello for Business (a product that uses WebAuthn) does behind the scenes. To get full functionality of both in a Microsoft environment there is more than a little bit of wizardry involved.

To create a passwordless MFA experience – as Windows Hello for Business claims it can – administrators must configure registration and authentication settings to require user verification to prove that a person is who they claim to be.

For example, with a standard USB physical token, like Yubikey by Yubico, the user touches it, and it activates. The system recognizes that the key is present, but it doesn't identify the user. Anyone could touch that key to activate it. Therefore, if an administrator has required user verification, a basic Yubikey will not work, because it won’t provide necessary proof, or identity verification.

Windows Hello for Business is essentially a Yubikey. The physical "token" is the PC itself with a Trusted Platform Module (TPM). In fact, one can only turn on a higher level of verification in Windows Hello when the computer has a TPM. A FIDO authenticator generated inside the TPM chip is tied through Windows Hello to either a personal identification number or biometric reader. So, at its heart, Windows Hello for Business is a Yubikey with identity verification built-in and tied to a piece of hardware in one's laptop.

Therefore, it's no surprise that Microsoft requires a TPM for its Windows 11 computers; it is critical to the company's strategy of growing passwordless MFA.

When an administrator configures Windows Hello alongside user verification with a particular authenticator (using WebAuthn), then the user essentially gets a passwordless experience at the front end.

You are you, and you have the device = two factors of authentication

However, there are still things that Microsoft cannot support. For example, traditional (legacy) applications that cannot support the tokenization of credentials are not supported. And herein lies the rub for most organizations. Traditional applications still make up the bulk of large enterprise infrastructures.

Microsoft Windows Hello for Business tries to solve this in a clunky workaround. Administrators may run a PowerShell script that causes Azure to "stand up" a read-only domain controller that can issue partial Kerberos credentials.

When a user uses Windows Hello for Business, they receive a Kerberos ticket from the read-only domain controller. Then, the user's machine connects to a full-featured domain controller where the previously issued ticket is exchanged for a full-featured ticket. At that point, the user can access anything on the secure internal network, like a file share.

Take note that there is a lot about this that is very recent – just in the last few months. One can assume that most CISOs will not take time to understand this bleeding-edge capability for quite a while, and many will be reluctant to be early adopters – not to mention the time and expense to implement and configure it.

"For native Azure Active Directory organizations, it's one thing, but for most organizations with on-premises Active Directory, it's a mess." –CISO, consumer services

Key Costs When Choosing Microsoft

Costs of using Windows Hello for Business for its full capabilities are myriad. (Table B)

TABLE B: FULL FUNCTION FINANCIAL IMPACT OF WINDOWS MFA

COST	IMPACT
Upgrading Operating Systems on Every Machine	Windows 10 or 11 required
Upgrading Servers	Windows 7 and 8 are not supported, neither are older Active directory 2016 servers nor print servers
Limited to Microsoft	Windows Hello for Business does not work on Mac or Linux
Upgrading PCs	To activate identity verification, all PCs need a Trusted Platform Module (TPM) chip. New Windows 11 machines also need a TPM
Implementing MFA	Turning on Windows Hello for Business as a simplified login experience to the laptop is one thing. Getting it to work across non-Microsoft applications and workflows is entirely another. Rolling out MFA to the enterprise is a major integration project
Integrating Traditional Applications	RDP, VPN, offline devices, airgap servers for critical infrastructure, and custom legacy applications all require workarounds to function with Microsoft. Some workarounds will be very complex, for example RADIUS does not support FIDO2 and Jira only supports LDAP. Neither will accept Windows Hello for Business authentication

COST	IMPACT
Building Out PKI	Full features depend on a public-key infrastructure
New Domain Controllers	One step to activating full features requires setting up a read-only Azure domain controller to produce one-time Kerberos tickets
Changing Code	Organizations with in-house developers will have to invest in retraining developers and rewriting code to support WebAuthn
Remote Users Limited	User biometrics cannot map to non-Microsoft remote user authentication. Remote users do not have an easy experience accessing corporate systems on hand-held devices and tablets
Partners Not Compliant	It is difficult to ensure that contractors and suppliers have hardware support for full capabilities

Source: Impact Leaders

CONCLUSION

- CISOs respect and appreciate Microsoft security solutions and use them as complementary to their preferred vendor solutions.
- Executives interviewed view Microsoft as a platform on which they commonly overlay complementary products and functionality.
- Few CISOs feel very confident in the overall protection of user credentials.
- Microsoft does not provide high security IAM and ease of use out of the box and will not without heavy lifting. Therefore, CISOs commonly seek IAM solutions from security-focused vendors that integrate well with Microsoft and the cloud.

ABOUT IMPACT LEADERS

Impact Leaders is an advisory firm providing insights on leadership, strategy, and operations to hundreds of IT executives—as well as to the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives as well as experienced researchers and consultants, our experts provide actionable advice to our client base, leveraging deep insights developed via our extensive network of clients and other industry contacts.

CONTACT

For all inquiries, contact Steve Hunt, Principal:
steve@impactleaderscoaching.com