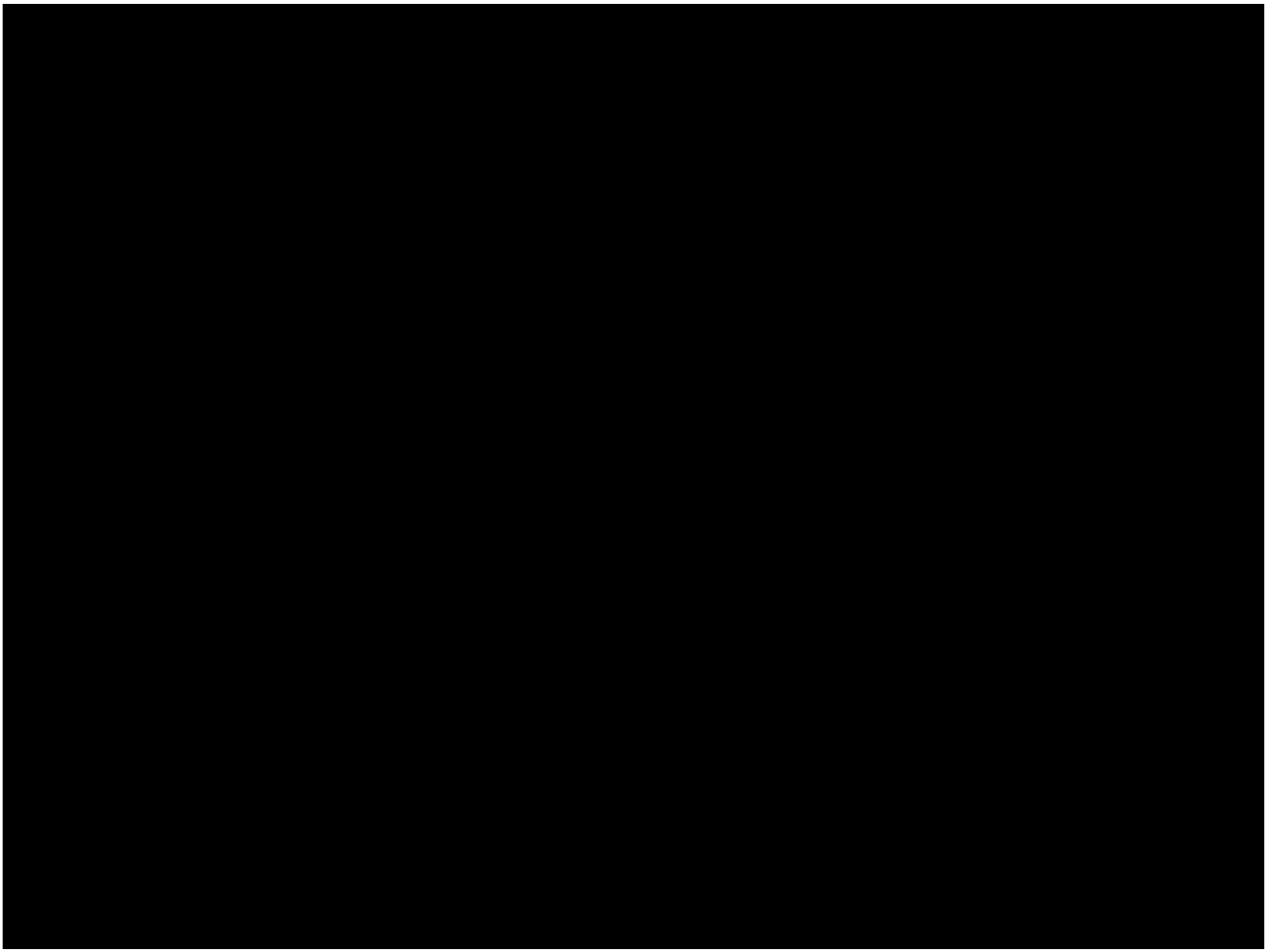
Secureworks®

VMw ⊨ tqsO
⊦• '

x 9 s ° º w ⊨0 b hwJqx



近年、職場の構造は急速に変化しており、しばしば前触れもなくに進化しています。在宅勤務やBYOD（Bring Your Own Device）ポリシーが多くの組織で一般的になるにつれ、サイバーセキュリティの新たな課題が発生しています。ビジネスリーダーにとって、これらの課題にどのように対処し、サイバーリスクを軽減する方法を理解することは、企業の重要なポリシーです。

83%

の米国の雇用者がCOVID-19に対応して調整を行わなければならなかった

進化

過去10年間で、ビジネスの世界では多くの働き方がトレンドとなって形成されました。リモートワークの成長に加え、BYODポリシーを採用している組織は増加傾向にあり、2011年には60%強だったBYODを導入しているとを報告している米国の組織が、2018年には80%近くに達していました[1]。BYOD 市場の期待値は、2025 年までに 4,300 億ドル以上になると推定されています。

70%

の雇用主がリモートワークへの適応に苦慮するのにしていると述べる

近年浮上したのもうひとつのトレンドは、多世代労働力の増加です。定年退職を先延ばしにしている人たちやZ世代が就職市場に参入したことで、現在の労働力の大部分を占めるのは4世代となっています。この幅広い年齢層は、多様なスキルと考え方をもたらします。その結果、多くの企業ではこれを考慮して意識的なビジネス上の意思決定を行ってきました。LinkedInのGlobal Talent Trendsレポートによると、56%の企業が多世代の従業員に対応するためにポリシーを更新しています2。

このような世代間の違いは、急速な働き方の変化により浮き彫りになっています。Society for Human Resource Management （SHRM）の調査によると、18～34歳の従業員の70%近くがリモートで効率的に仕事をすることに自信を持っていると回答しているのに対し、55～64歳の従業員では44%にとどまっています3。

ビジネスの成長とグローバル経済は、従来の職場の構造にも影響を与えています。企業が新たな市場に進出する際には、現地の労働力をサポートするために、世界各地に新たな拠点を開設します。このような拡大に伴い、監視すべきアクティビティやセキュリティを確保すべきエンドポイントも増えています。

COVID-19パンデミックの発生により、多くの組織はリモートワーク環境への迅速な適応を余儀なくされました。調査によると、米国の雇用者の83%がCOVID-19に対応するために調整を余儀なくされ、そのうち75%以上が一定期間リモートワークに移行しました。さらに、70%以上の雇用主がリモートワークへの適応に苦慮していると答えています4。rk.[4]

Risk Management Considerations

As companies manage their evolving workforce, they must confront the new risks involved and implications for their cybersecurity programs.

While securing a BYOD workforce initially created hurdles for some companies, the fact that most of the devices' usage was taking place on an internal network from the same physical location minimized some level of risk. However, with people's personal devices

increasingly being used from unique home networks, the attack surface for potential threats has greatly expanded. Now a threat actor merely needs to compromise one device on a home WiFi connection – a tablet or smart TV, for example – in order to access the specific device with company data.

Managing hundreds or even thousands of remote workers only further expands the attack surface. Not only are employee devices at risk of exposure, but cloud-native platforms like Zoom are being implemented to virtually connect employees, often rapidly and without security risk considerations. As a result of this rapid deployment to remote work, more than half of organizations recently surveyed said that their cloud usage would be higher than initially planned.[5] What used to be an in-person meeting or conversation around the water cooler is now a digital file; this adds a layer of complexity to the already huge amounts of data a company must secure.

As attack surfaces increase, many companies are often challenged with scaling their security preparation and response to match. Even as some organizations expected increased security budgets prior to the 2020 recession, many cybersecurity teams have been left scrambling to secure a new workforce with the same, or fewer resources than they previously had.[6]

Adapting to the New Environment

As organizations adjust to the ongoing workplace changes, there are several practical steps business leaders can take to ensure they are prepared.

1. Evaluate your security posture to know where you stand

Do you know what information or data is accessible via your internal network or VPN? Knowing where your valuable assets are and having the security controls already in place to protect them is a fundamental first step.

2. Assess and address your perimeter

Perimeters used to mean a dotted line around an office building; these borders have now expanded around the entire planet, and can include systems hosted by third-parties and the cloud.

3. Consider changing work patterns and user behavior in this environment

A remote and global workforce means activity on your network will no longer take place from only office locations or during the same set of hours. Understanding these types of changes to user activity will help security teams identify potential anomalies.

4. Ensure you are implementing the basics of network defense

Once you have assessed your perimeter, having the right telemetry – such as firewall and endpoint detection and response – in the right places is critical to establishing a baseline level of security to prevent the most basic intrusions.

5. Implement companywide employee education

Every employee has a responsibility to a company's security. It's important to spread awareness that it's not just on IT to secure company data. All it takes is one misconfigured system for a malicious threat actor to hack into.

6. Employ multifactor authentication (MFA)

MFA – a security measure that verifies a user's identity by requiring multiple credentials – is a critical and non-negotiable part of a layered defense strategy.

Preparing for a New Normal

The workplace today is vastly different than ever before, and it appears that changes that may have seemed fleeting are likely the new "business as usual." How can your organization prepare for this reality?

For starters, it's prudent to take a close look at your security investments. What may have worked 10 years ago is not the same as what today and tomorrow's security organization requires. Staying up to date with futureproof solutions is critical to keeping your company's assets protected. For example, organizations should consider software and artificial intelligence as a way to help contextualize the vast amounts of data being processed by a security team. "Always on" endpoint security is another imperative to address the changing, 24/7 workforce of today.

From a cultural perspective, it's time for organizations to embrace, rather than resist, these changes. At a minimum, companies must be ready to support and enable a majority of their workforces to work remotely, while implementing the right measures to ensure security.

Finally, IT and security functions should welcome the opportunity to prove to the larger organization how security can enable business growth and safeguard data in times of rapid change. This evolution has also demonstrated that every business strategy should incorporate cybersecurity measures into their business continuity plans. In order to prepare for the unexpected, security teams should have the tools and resources to be nimble and ready to adapt to what's next. For better or for worse, this new, modern workplace is here to stay. Organizations must keep up or get left behind.

Source

[1] Frost & Sullivan, Bring Your Own Device (BYOD)—Key Trends and Considerations

[2] LinkedIn, 2020 Global Talent Trends Report

[3] Society for Human Resource Management, *Majority of Employees Embrace Remote Work*

[4] Society for Human Resource Management, Tips and Tools to Engage Your Remote Workers

[5] Flexera, 2020 State of the Cloud Report

[6] ESG, 2020 Technology Spending Intentions Survey

Secureworks

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp