jos

An HKBN Group Company

ENDPOINT SECURITY FOR THE HYBRID WORKPLACE

As businesses increasingly adopt cloud-based collaboration platforms to connect teams across the globe, they will eventually need to expand their entire technology infrastructure and ecosystem, including SOCs, IoT, Cloud Computing, and SASE, to accommodate this digital transformation.

It is crucial for businesses to keep in mind that traditional endpoint security methods are no longer sufficient to ensure their endpoint security. In fact, with cyber threats increasingly becoming more sophisticated and rapid, businesses must adopt a proactive instead of reactive stance so that they can respond and prevent incoming attacks from reaching vulnerable endpoints.

The Cyber Threat Landscape

47K .sg

47,000 unique Singapore-hosted phishing URLs (with a ".SG" domain) were observed in 2020

39%

39% of Organisations admitted to suffering a security compromise involving a mobile device in 2020

67%

67% of IT professionals say endpoint misuse grew in their organisations in 2021

44%

44% are worried that more liberal BYOD policies will see personal devices used for work without risk assessment in 2021

Remote and hybrid working arrangements result in employees accessing company data and resources through their personal devices at various locations and networks of their choosing, leaving them highly vulnerable to cyberattacks.

When users and devices are off-network, antivirus and traditional security solutions are insufficient measures in combating advanced threats which are becoming increasingly challenging for IT personnel to foresee. It is highly recommended that businesses adopt a proactive stance through routine scans to identify potential incoming threats before they reach vulnerable user endpoints.

The Evolving Hybrid Work Landscape

83%

Employees prefer a hybrid work model and to work remotely between 25% and 75% of the time

63%

High-growth companies have already adopted a "productivity anywhere" workforce model in 2021

More than ever, IT and cybersecurity decision-makers have to contend with a wide variety of operating environments and endpoints to secure – increasing the number, variety, and sophistication of cyberthreats the company faces. Without an evolving cybersecurity strategy, many IT and security departments may quickly find themselves struggling to secure networks and data.

Endpoint Vulnerabilities

Only 37% of users in 2019 use two-factor authentication

54% of 3,000 workers in 2021 use their work device for personal purposes including sharing work equipment and connecting to home devices

28% of respondents in Singapore had experienced at least one cyber incident in the past 12 months in 2019

47% respondents in Singapore installed security applications in their mobile devices in 2019

55% of users in 2019 said they wouldn't even bother changing their passwords following a data breach

Only 34% of users in 2019 change their passwords regularly

80% of reported security incidents in 2020 are phishing attacks

How Secure Is Your Business Data?

While there are many endpoint threat detection and response solutions out there, one key criterion is compatibility with the multitude of endpoints operating systems and environments.

This is critical to provide unified visibility across an organisation's entire technology ecosystem, with automation and enforcement at every control point.

The Loopholes In Traditional Cybersecurity Solutions

The cyber landscape has evolved from an on-premises world bounded by a manageable network perimeter into a cloud-powered infrastructure that supports remote working, 5 billion monthly teleconferences, and a constantly increasing rate of cyberattacks.

Traditional cybersecurity solutions were not designed to handle today's fast pace of cyberthreats like:

- Data Breaches
- IP Theft
- Phishing
- Ransomware Attacks

Companies who solely depend on these traditional tools and do not evolve their cybersecurity measures may quickly find themselves dealing with alert fatigue, staffing shortages, and an increasing number of successful attacks.

How An Endpoint XDR Can Strengthen Your Security

XDR, Extended Detection and Response, is the evolution of EDR, Endpoint Detection and Response. XDR extends beyond the endpoint to make decisions based on data from more products and can take action across your stack by acting on email, network, identity, and beyond.

MAXIMISE value from your existing cybersecurity measures

REVEAL blind spots with cross-stack visibility

DETECT stealthy attacks with cross-stack correlation

AUTOMATE threat responses across different domains

MANAGE your operations from one intuitive console

CUSTOMISE multi-site architecture tailored to your organisation

EXECUTE full functionality with unlimited device and firewall control

INCREASE efficiency and productivity in your SOC

Enhancing Your Security in 3 Steps

1 Seamlessly Manage Data From Any Source

- Collect structured, unstructured, and semi-structured data in real-time from any technology product or platform
- Defend against any threatening data in real-time
- Automate the process of assigning policies, mitigating threats, and defining actions for every rule

2 Single Out Incoming Attacks With Cross-Stack Correlation

- Provides real-time, automated machine-built context and correlation across the enterprise security stack to transform disparate data into actionable information
- Analyzes attack causes and incidents
- Integrates threat intelligence for detection and enrichment from leading 3rd party feeds

3 Rapidly Neutralize Attacks With Actionable, Automated Responses

- Resolves threats automatically on all devices
- Highlights benign findings as threats for real-time, automatic remediation
- Offers custom threat detection capabilities
- Integrates leading SOAR tools to streamline SOC workflows

Are You Ready To Prevent Tomorrow's Threats With HKBN JOS?

Implement a singular platform for a unified visibility across your entire technology ecosystem. Automate and take back full control at every point.

Get in touch to see how HKBN JOS can help you **protect every endpoint** of your business environment.

GET IN TOUCH

HKBN JOS sg-enquiry@jos.com +65 6551 9611 67 Ubi Avenue 1, #02-01, Starhub Green, North Wing, Singapore 408942

Sources:

1) https://www.csa.gov.sg/en/News/Press-Releases/ransomware-incidents-online-scams-and-covid19-related-phishing-activities-dominated-cyber-landscape-in-2020
2) https://www.accenture.com/us-en/insights/consulting/future-work?c=acn_glb_talentandorganimediarelations_12163686&n=mrl_0521
3) https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf
4) https://securitybrief.com.au/story/remote-work-continues-and-endpoint-security-cited-as-a-must
5) https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html
6) https://www.csa.gov.sg/news/press-releases/csa-public-awareness-survey-2019
7) https://enterprise.verizon.com/resources/reports/2020-msi-report.pdf
8) https://about.att.com/story/2021/att_cybersecurity_survey.html

jos