
hmd.
Holistic Security
in a Hybrid
Working World

How a comprehensive enterprise solution keeps businesses secure in a post-pandemic world

SECURITY MUST ADAPT WITH THE TIMES

Accelerated by the Covid-19 pandemic, the working world has transformed into one where hybrid work and increased digitisation are the norms, not the exceptions. The pace of change can be seen across the board. There is increased personal mobility among the workforce as Monday-Friday in the office becomes a thing of the past and high-revenue growth companies embrace hybrid workforce models at an accelerated rate[1]. What's more, Internet of Things (IoT) deployment is expanding rapidly to accommodate industries from healthcare to manufacturing – just two examples of industry verticals embracing digital solutions to boost productivity and efficiency while maintaining company and mission critical systems security.

With the hybrid personal mobility trend the new norm, and enterprises rapidly adjusting to manage their operations, the technology used is often not in line with human behaviour and there is a disconnect between how technology expects end-users to behave (changing our passwords regularly, restricting device use to work items only, etc.) and what the end user actually does. This creates a culture gap when it comes to understanding the security and privacy risks associated with new ways of working. For instance, research shows 68% of business leaders feel their cybersecurity risks are increasing, and two-thirds (66%) of CISOs do not believe their organisation is prepared to cope with an attack[2].

Device and network security measures must move with the times as the landscape evolves so they can protect against increased cybersecurity threats and adhere to privacy legislation as we move towards three-quarters of the world being covered by some form of privacy law by 2023[3]. A holistic approach that complies with strict privacy legislation surrounding data collection and is built on reliable foundations is the best way for organisations to protect themselves against security and privacy threats posed by the 'new normal' now, and in the future.

[1] https://www.apollotechnical.com/hybrid-working-statistics/
[2] https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf
[3] https://www.zdnet.com/article/gartner-predicts-privacy-law-changes-consolidation-of-cybersecurity-services-and-ransomware-laws-for-next-4-years/

We live in a 'want it now' culture where if things don't happen instantly, we get frustrated. We are all driven by experiences and it is human nature to look for a solution with the least friction.

Work devices and applications are no exception. If given the freedom to do so, employees are likely to try out different options and explore new apps or connection methods to get tasks done. This can expose new entry points to cybercriminals, or break important privacy rules, which is why enterprises must ensure they have the appropriate employee education and IT capabilities in place to manage these threats while enabling effective work and user-friendly devices.

Andrej Sonkin
GM, Enterprise Business, HMD Global

More personal mobility, more risk?

52% of employees globally work remotely at least one day of the week[4] and mobile workers are predicted to count for almost 60% of the U.S. workforce by 2024[5]. Working from home – or from anywhere – has reached unprecedented levels since the pandemic began. The transition has taken place at such a rapid pace, however, that the lines between personal and professional have become blurred, and security compromised as companies have struggled to properly equip employees – and decision-makers – with the right technology.

Smartphones and tablets are now integral to business success. They help ensure collaboration, communication, and access to important company data wherever an employee may be. However, this hybrid working environment also leaves businesses vulnerable to heightened security threats as enterprise security protocols fight to keep up with the pace of change.

[4] https://resources.owllabs.com/state-of-remote-work
[5] https://www.checkpoint.com/downloads/resources/mobile-security-report-2021.pdf

In 2020 alone, 97% of organisations experienced mobile threats[6] and enterprises must now contend with an increasing level of risk and data leaks as employees move outside the jurisdiction of the office and use typically less secure home or public Wi-Fi.

Using the same device for both work and personal use is an important user requirement – and 55% of workers globally are already doing so[7]. However, this isn't advised without having effective boundaries in place between personal and work apps and related data. Without these boundaries and an ability to manage enterprise devices appropriately, there is an increased risk that if your device is stolen or infected with malware your personal data and valuable company information may be exposed and you could incur additional phone bill costs.

The technology and devices used must be able to prevent such personal and company data breaches at source. Official app stores such as Google Play are becoming increasingly capable of detecting and removing Potentially Harmful Applications (PHA) through in-built malware detection tools such as Google Play Protect which scans over 100 billion apps every day. This makes it more likely that PHA's are downloaded from 3rd party stores or other unknown sources. As well as ensuring enterprise devices get regular (ideally monthly) security updates by selecting devices from manufacturers that offer a clear update promise, one of the benefits of an enterprise mobility management (EMM) solution is that it can be used to block users from using these unknown sources for app downloads.

> *Cybercriminals don't discriminate between small or big business and they're always looking for new ways to attack. The impact of malware ranges from causing additional expenses to your mobile subscription to ransomware attacks and leaks of personal data, and security is always as strong as its weakest link. Therefore, enterprises large and small are increasingly looking at taking necessary precautions and deploying EMM solutions to define policies on what is and is not allowed to be done with enterprise devices.*

Ari Heikkinen
GM, Global software security, HMD Global

[6] https://www.checkpoint.com/downloads/resources/mobile-security-report-2021.pdf
[7] https://www.gartner.com/en/newsroom/press-releases/2021-04-26-gartner-survey-finds-1-in-5-workers-consider-themselves-digital-technology-experts-since-covid-19

HMD Global's EMM solution – HMD Enable Pro – lets businesses optimise enterprise devices for specific use cases, whether for personal or IoT use. Organisations can manage and monitor a fleet of Android devices remotely, install needed applications, define various connectivity and security settings, and benefit from features like Android SafetyNet to quickly identify devices that are potentially compromised on security. Meanwhile, those using Android smartphones or tablets can use Work Profile to allow employees to have their work and personal life in a single device while keeping company and personal data separate. Work Profile can be enabled for both company owned and BYOD devices with a compatible EMM solution. This is increasingly vital in a world where 70% of employees use company-issued tablets to download personal apps[8].

Over-the-air commands for remote lock and remote wipe mean IT can rapidly respond when devices are lost or stolen so long as they are enrolled to an EMM solution. Compatibility of devices with EMM solutions is ensured through the underlying Android OS and Android Enterprise capabilities, which are part of the latest Android versions. This is another reason organisations should target devices that are regularly updated and upgraded and are part of the Android Enterprise Recommended program that mandates at minimum of one Android OS upgrade and two years of quarterly security updates.

[8] https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/the-case-for-making-byod-safe

HMD Global's Android Enterprise Recommended Nokia device range goes beyond even the strict criteria set out by Google to make the gold-standard of security available regardless of budget. All Nokia smartphones in the Android Enterprise Recommended program receive at least two Android OS upgrades and three years of monthly security updates.

Andrej Sonkin
GM, Enterprise Business, HMD Global

Nokia G, X-series devices and the Nokia XR20 and Nokia T20 tablet receive monthly security updates, rather than the minimum Android Enterprise Recommended requirement of quarterly updates, so all price points from $150 are constantly equipped to tackle new cybersecurity vulnerabilities.

Standout statistics

- In 2020, 97% of organisations experienced mobile threats[9]
- Secure access is the top cybersecurity challenge when supporting remote workers[10]
- 55% of workers globally use their personal smartphone or laptop for some work tasks[11]

[9] https://www.checkpoint.com/downloads/resources/mobile-security-report-2021.pdf
[10] https://www.cisco.com/c/en/us/products/security/future-secure-remote-work-report.html
[11] https://www.gartner.com/en/newsroom/press-releases/2021-04-26-gartner-survey-finds-1-in-5-workers-consider-themselves-digital-technology-experts-since-covid-19

IMPORTANCE OF SECURITY FOR INDUSTRY VERTICALS AND IoT DEPLOYMENTS

While personal mobility has been the main trend of enterprise smartphone and tablet use, other significant trends we have identified include use of commercial off-the-shelf (COTS) devices and enterprise solutions in industry vertical and IoT use cases. As COTS device capabilities and performance has increased over recent years, the need for specialised devices has decreased. This has allowed devices originally intended for consumer use to be transformed via an EMM into ones that fit specific purposes and use cases.

As most of the industry vertical use cases require mobility, and all IoT use cases only require data and occasionally SMS, enterprises prefer mobile connections over WLAN connectivity. Mobile data connections provide security for the connection and the possibility to centrally manage connections, as well as less risk of connectivity issues which can arise when, for example, WLAN passwords are changed.

Let's take a look at three specific industry examples to see where security threats can emerge and how HMD Global devices and services alleviate them.

Healthcare

Examples of mobile device use in this space include the collection and management of patient data, at-home monitoring and data entry by patients, and as part of clinical trials. Healthcare is also increasingly taking advantage of IoT to improve connectivity, collaboration and caregiving. These advances are revolutionising the industry but also mean providers are being targeted, as seen when the Irish NHS suffered a crippling ransomware attack in 2021[12]. Making sure patient data is kept secure is, therefore, paramount. Nokia phones and tablets and HMD Global's enterprise services offering are making this possible. The end-to-end solution incorporating HMD Connect Pro for IoT data roaming connectivity supports healthcare providers by providing

[12] https://www.bbc.com/news/world-europe-57184977

access to the most reliable and lowest latency network in the world. And HMD Connect Pro's management console also gives medical providers the power to oversee their fleet of SIM cards in real-time, so they always know how they are being used and where they are. This is a beneficial feature for shared equipment without identifying any individuals.

With HMD Enable Pro Kiosk mode, healthcare professionals can fully manage devices to ensure only the applications they want are installed on the device, limiting risk of ransomware attacks in waiting room tablet use, shift work where devices change hands among employees, or telehealth devices used by outpatients.

Manufacturing

Industry 4.0 – the fourth industrial revolution where traditional manufacturing becomes automated using modern technology – has only been accelerated by the pandemic. This acceleration has ushered in faster, more efficient processes as the number of connected devices has increased. However, this rapid adoption has left a traditionally manual industry struggling to keep pace. For instance, one in five manufacturing enterprises admit IoT devices are their most poorly supervised assets[13]. And a lack of culture around IoT cybersecurity means proactive device and solution protection is critical.

With HMD Global, a manufacturer can now oversee entire workflow processes using mobile devices as IoT terminals to retrieve data. Worries over weak entry points around the edge of the WLAN network are reduced using HMD Connect Pro which lets users route data securely from SIM to platform no matter where in the world their devices are. And the ability to activate or deactivate SIM cards with one click and receive notifications when a SIM card is used in a different device lets enterprises regain control over their IoT device connections.

[13] https://panaseer.com/wp-content/uploads/2019/09/20190919-Peer-Report.pdf
[14] https://www.3plstudy.com/ic3pl/ic3pl.ic3pl.home
[15] https://hornetsecurity.com/data/downloads/reports/document-cybersecurity-special-logistics-en.pdf
[16] https://www.websiteplanet.com/blog/bergen-leak-report/

Transport & Logistics

From route optimisation to supply chain organisation - where 81% of shippers see big data becoming central to success[14] – transport and logistics enterprise is embracing digital to improve efficiency. The data that is needed for shipping can contain personal data such as names, phone numbers and addresses, making then subject to privacy laws and regulations and a potential target for criminals. Indeed, the logistics industry was the second-most targeted by cyberattacks in 2019[15] and there are regular examples of companies exposing customer data due to weak security practices[16]. Data privacy is, therefore, an important consideration for any enterprise expanding their digital options.

> *As the transport and logistic industry embraces data-led solutions, and as data privacy laws continue to strengthen around the globe and privacy becomes an expectation, it is important for organisations in these industries to maintain reputation and credibility by adhering to the highest security and privacy standards.*

Ari Heikkinen
GM, Global software security, HMD Global

Company device policies undoubtedly facilitate efficient services when used correctly but make individual and company data vulnerable without the right protections. HMD Enable Pro's Fully Managed profile can make sure only work-related applications are accessible on company-owned devices for delivery drivers – and unlock the possibility to see where the device is to assist with delivery planning and accuracy.

Standout statistics

- In November 2020, individual healthcare organisations experience an average of 632 cyberattacks per month – with ransomware the most common[17]

- 60% of companies say that mobile devices are their biggest security risk[18]

PRIORITISING PRIVACY

The pressure to protect personal data is intensifying. Mobile devices have been pinpointed by cybercriminals as gateways to attack and steal personal data, with 0.12% of all devices worldwide infected each month with malware[19]. And, globally, the introduction of data privacy laws is accelerating. It took 41 years to go from eight laws in 1970 to 89 in 2011[20]. In the decade since, 39 countries have introduced their own legislation[21] and, by 2023, over 80% of companies worldwide will be facing at least one privacy-focused data protection regulation[22]. Whether a manufacturer, healthcare provider, or working in another industry altogether, organisations are responsible for maintaining the privacy of the personal data they collect and process.

HMD Global takes this responsibility extremely seriously. Proudly Finnish, proudly European, and truly global, our Nordic heritage means that enterprises can trust that GDPR regulations are the foundation of our security and privacy policies.

We prioritise privacy in our services and nothing we design is done without a privacy risk assessment. It is important to us to clearly communicate our privacy policies to enterprises and end-users in a transparent and open manner and we do so via the Privacy Portal[23]. This is the online home for the latest privacy policies and supplemental material. It is available 24/7, 365 days a year and is where you can find comprehensive answers to questions like what data is collected to provide HMD Connect Pro and HMD Enable Pro services. Plus, by including links to privacy documents on the first page of every enterprise device setup, it is easy for businesses to remain compliant.

[17] https://blog.checkpoint.com/2021/01/05/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/
[18] https://www.verizon.com/business/resources/reports/mobile-security-index/2021/cheat-sheet/
[19] https://pages.nokia.com/T006US-Threat-Intelligence-Report-2021.html
[20] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034
[21] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
[22] https://www.gartner.com/en/newsroom/press-releases/2021-09-30-gartner-says-digital-ethics-is-at-the-peak-of-inflate
[23] https://www.nokia.com/phones/en_int/privacyportal

A final privacy precaution we take is to collect, analyse and approve the critical security configurations of every phone and tablet model we manufacture before any public software releases. This scanning process is carried out by the HMD Security and Enterprise team located in Finland utilising cloud testing and physical device testing for total clarity.

At HMD Global, European values meet global innovation for security and privacy in mobile solutions. We are committed to adhering to GDPR in all that we do, and this shows at many levels in our operations: we have strict privacy requirements for our mobile solutions, we do continuous privacy risk assessments for them all, and our policy is to store phone activation and performance data in Google Cloud servers in Hamina, Finland so it is protected by European and Finnish laws which are some of the strictest in the world.

Jari Koljonen
Data Protection Officer (DPO), HMD Global

A VIEW FROM THE INDUSTRY

Ronald van Loon is a Top 10 Global Influencer in artificial intelligence, machine learning, digital, digital transformation, business intelligence, and predictive analytics. Below, he explores the comprehensive, holistic security solutions being used across industries as organisations implement digital transformation technologies and enable remote work.

Cybersecurity is a challenging landscape for organisations to traverse as they navigate digital transformation in a hybrid remote work world.

However, most businesses are taking a reactionary approach to security instead of being proactive in the face of new evolving threats. Out of every 100 companies across various industries, only 10% of businesses aim to reduce security risks, while 70% are trying to implement security measures as threats occur.[24]

Companies must ensure that cybersecurity becomes an integral part of their business models, ensuring end-to-end holistic security across the value chain. In addition, as digitisation advances, they have to ensure that their cybersecurity teams are improving risk management strategies, and uniting business objectives with IT.

Securing a Connected Enterprise in the Era of Remote Work

Enterprises have many moving parts in their connected digital business environments, from increasing IoT touchpoints, ecosystem interactions with partners, affiliates, acquisitions, enterprise-wide technology platforms, and cloud and edge adoption. The workforce is embracing these new digital tools and capabilities in the workplace and at home in order to become resilient in the face of disruption, such as that seen from Covid-19.

Businesses need to build cybersecurity capabilities into new operating models as the stages of their digitisation advance. To reduce enterprise security risks, organisations have to develop and align security and privacy controls and measures with their enterprise risk management strategies and involve the entire organisation in the process across stakeholders, C-level, management, and IT.

[24] https://www.mckinsey.com/~/media/mckinsey/email/leadingoff/2021/07/19/2021-07-19b.html

Building a Risk and Security Framework

If organisations are to achieve holistic security, they have to embed security protocols into their processes, products, and services and involve customers and partners. Their strategy must be built on a design framework that lays out its steps to implement enterprise-wide holistic security.

This involves uniting the workforce culture around security by educating, training, and recruiting new talent. People can then integrate cybersecurity across business processes, using risk metrics to improve incident response and run threat and response planning simulations and scenarios.

Now the organisations can be prepared to integrate security into technology across the network, cloud, mobile, applications, infrastructure, and data, including enhancing identity and access management. It's also important to consider policies, regulations, and compliance to enhance asset protection.

Finally, a business is prepared to activate defense mechanisms that can proactively detect anomalies and potential threats before they occur and continuously monitor the company using analytics.

This type of framework helps companies progress from their initial stages of reactive security management to building a proactive, holistic security environment.

Enabling a Profitable Enterprise with Holistic Security

The future of work will be a hybrid remote work environment. Therefore, organisations need to ensure that as they enable digital transformation technologies, they also locate and measure business areas to improve security.

Additionally, businesses should keep in mind that there is a direct correlation between the level of cybersecurity maturity in the organisation and the organisation's profitability. If organisations can secure their critical data, manage remote access, communicate cybersecurity policies and requirements across the organisation and existing partnerships, update cybersecurity protocols regularly, and continuously scan IT landscapes for potential gaps in security, they will enhance profitability and create a proactive holistic security environment across the enterprise.

About HMD Global

Headquartered in Espoo, Finland, HMD Global Oy (“HMD”) is the home of Nokia phones. HMD’s mission is providing accessible connectivity for everyone. HMD designs and markets a range of Nokia smartphones and Nokia feature phones and an expanding portfolio of innovative HMD service offerings. With an ongoing commitment to security, durability, reliability, and quality across its range, HMD is the proud exclusive licensee of the Nokia brand for phones and tablets. For further information, see www.hmdglobal.com.

hmd.