Publication date:
Nov 2020
Author:
Alan Rodger
Senior Analyst

Adam Holtby
Principal Analyst

Making the Future of Work Cyber-Secure and Sustainable

Best practices for a secure distributed workforce and a resilient business

In partnership with:

Brought to you by Informa Tech

Contents

Summary

The year 2020 has been one of unprecedented disruption, the effects of which will last for the foreseeable future. The dramatically increased need to support remote working has been a major challenge for many enterprises, bringing a structural change in security requirements for some. According to the results of a survey undertaken for NTT Ltd., 83% of organizations have needed to rethink their security to accommodate new ways of working during the pandemic. With most organizations planning for large parts of their workforce to have at least the option of remote working in future, leaders would be wise to choose a sustainable path that supports business requirements such as strong security protection, compliance, and operational efficiency.

At the same time, many may also look toward options to resolve long-standing deficiencies and inefficiencies in their broader security capabilities. Although disruptive, that path can be less problematic and more practical now the capabilities of modern solutions are available as packaged options with relevant expertise via services partners.

CISOs will want to address all doubt and questions about how resilient their organization would be in the face of possible further shocks in such uncertain times. For many, a plan to assess security-related maturity status will be advisable so that they can advance assuredly with

- Support for secure remote working locked in with formal business continuity plans
- A sustainable capability that links cybersecurity protection with stakeholder trust
- Support for already-strained IT and security teams

Key messages

- Supporting remote and mobile working securely should be seen as a strategic opportunity.
- As change brings greater risk diversity, organizations need a broader and flexible range of security protection.
- Implementing and managing new secure workplaces extends beyond the desired capabilities of most organizations.

Disclosure

Omdia has undertaken this white paper in collaboration with NTT Ltd., which offers advanced security solutions in conjunction with its strategic partner Palo Alto Networks.

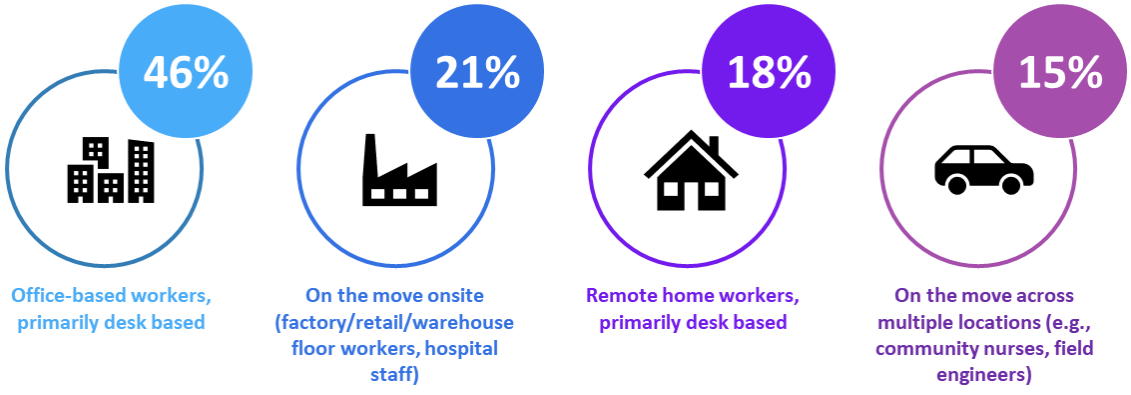
Supporting distributed working securely should be seen as a strategic opportunity

Organizations' work styles are at a key inflection point

Before the COVID-19 pandemic, a large proportion (67%) of employees were based onsite, working either primarily at a fixed desk location or on the move onsite. Only a relatively small number (18%) of employees were classified as remote home workers, as shown in **Figure 1**.

Figure 1: Prepandemic workplaces

Where did your employees work before COVID-19?
Please indicate what percentage of your workforce worked in the following locations:



Note: n=415

©2020 Omdia

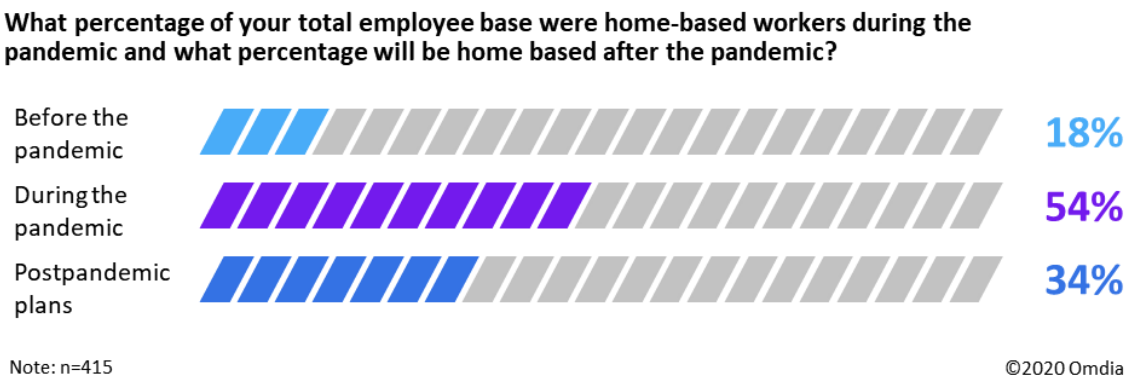
Source: Omdia Future of Work Survey 2020

A variety of different technological and cultural factors have historically slowed down the move by many businesses toward remote work. Concerns over employee productivity when away from the office, new security risks associated with mobile or remote ("distributed") working, and issues with the provisioning of software and hardware are examples of some common concerns. All these issues

are valid and need to be considered and managed, but the mass-home-working experiment brought about by the pandemic has shown how these challenges and others can be overcome and how new benefits can be realized as a result. Technologies to enable secure and productive flexible working have existed for some time now so are not a barrier in terms of scalability or reliability; however, ensuring appropriate breadth and depth of security is an absolute must.

Data from Omdia's recent 2H20 Future of Work survey, illustrated in **Figure 2**, draws some color around the scale of change businesses expect, with the number of home workers set to nearly double compared to work patterns before the pandemic. The increased number of home workers will previously have worked in any of the other three types of environment. In all of those workers' cases, numerous operational issues must be managed in order for them to continue successfully in their roles, with cost, risk, well-being, and cultural factors all being important considerations from the organizational perspective.

Figure 2: Remote and home working is set to be a long-term change for many

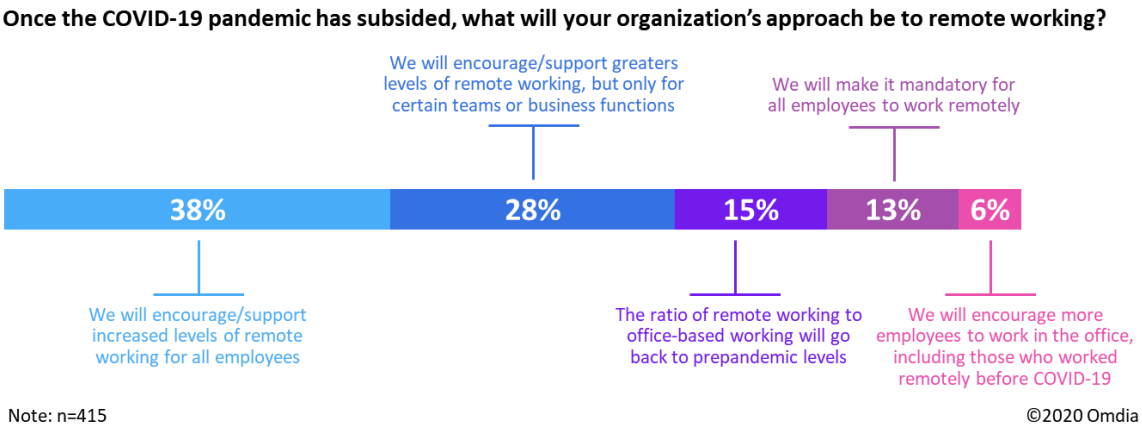


Source: Omdia Future of Work Survey 2020

Organizations are solidifying broader plans to support fluid work styles long term

This mass shift in work styles represents one of the most significant work-related changes the world has ever seen, specifically as it impacts global businesses at a technological, cultural, and economic level. The long-term business intent and direction is becoming clear: more employees will be working differently and away from the confines of a traditional office, more frequently. It is therefore important that businesses prepare with this longer-term view and perspective in mind. As **Figure 3** illustrates, organizations responding to a recent Omdia survey have reached a range of conclusions so far about their way forward. The most notable summary point from this part of the survey is that 79% of these organizations are planning for increased remote working to some extent, with the majority (51%) being highly committed to the approach.

Figure 3: A spectrum of postpandemic business approaches to remote working



Source: Omdia Future of Work Survey 2020

Investing in technologies and services that can help enable and secure a more mobile and fluid workforce is important. Solutions of note that are proving to be of interest to businesses include communication and collaboration tools, mobility management platforms and services, and security solutions. Whichever solutions are adopted, it is imperative that a long-term vision and strategic plan is guiding these investments.

Increased uncertainty must drive improvements in organizational sustainability

Robust business continuity plans require organizations to be equipped and operationally prepared to quickly recognize and respond to business disruptions and changing needs. One very strong lesson that businesses will have learned from the pandemic is that business continuity planning must extend beyond the traditional disaster recovery activities associated with IT infrastructure and systems. Rather, they must enable employees and customers to continue to engage with key business processes, thereby providing sustainability at an organizational level. Omdia's recent survey reveals that only 17% of businesses responding were fully prepared for the transition to remote working as part of their business continuity plans, as illustrated in **Figure 4**.

Figure 4: Only 17% of businesses were fully prepared to transition to remote work

Source: Omdia Future of Work Survey 2020

Given the scale and speed of change required to adapt to the remote-working needs brought about by the pandemic, it would be unrealistic to assume that the majority of businesses would be fully prepared to respond to further disruption in an ideal fashion. This is despite the need to enable distributed working being nothing new: it has been an important digital agenda item for many years now. However, it has undoubtedly now become a more important priority and focus of investment for businesses as they accelerate new capabilities to deliver it and improve employee experiences as a result. In doing so, it is critical that visibility and control is maintained over the business risks arising.

As change brings greater risk diversity, organizations need a broader and flexible range of security protection

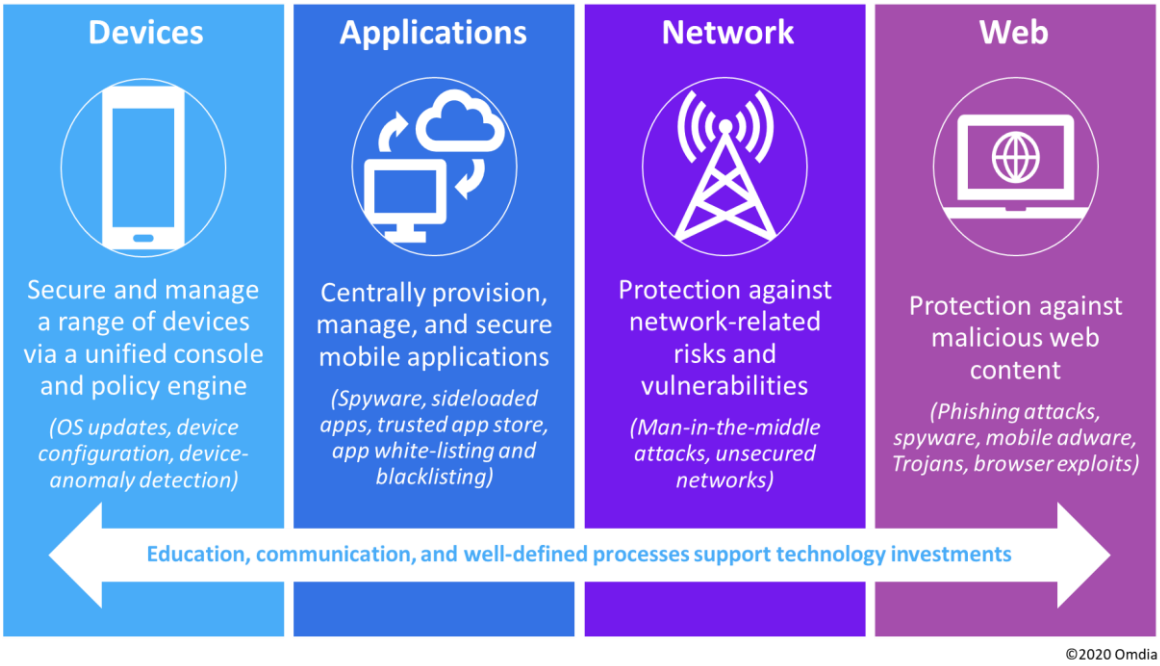
Cybersecurity and business dynamics both drive the need for flexibility and agility in enterprise protection

Digital transformation initiatives (the sudden rise in remote working being one that was uniquely accelerated because of the pandemic) are fundamental to most organizations' plans for successful sustainability and growth. Adequate and well-positioned cybersecurity protection is a critical element of this success, for example, in its key support of organizational compliance and stakeholder trust. Therefore, CISOs have a vital role as a business partner in planning for the implementation and ongoing support of initiatives. Other business leaders need to understand that a broader, deeper, and perhaps, more sophisticated digital footprint can result in increased levels of cyber-risk and could derail digital initiatives, causing investment to have been wasted and incurring other losses such as reputational damage.

While risks arising from the extension of enterprises into modern technology environments can be assessed and managed to an extent, malicious actors now mount unprecedentedly complex and varied types of attack and do so more frequently than ever. These can focus on weaknesses and vulnerabilities in any of the numerous technologies across now-broader organizational IT estates (e.g., cloud, Internet of Things, and mobile devices), which have provided extensions to the available attack surface.

The need to deal with a flow of innovative threat elements over time has driven the adoption of diverse security solutions. Combating attacks via vectors such as phishing, identity theft, hacking, and ransomware, sometimes as multiple modes of compromise, requires integration of people, processes, and these security solutions. The diversity of the threats (even just in the domain of remote working) and of the consequent protection measures necessary is illustrated in **Figure 5**.

Figure 5: Protection against diverse threats presented by the remote workforce



Source: Omdia

Much-needed transformation of security solutions is underway

While the pandemic has focused attention on the shift to remote working and the on security-related issues arising from remote working, the reality is that key security issues lie across a far broader scope.

Even in the domain of remote working, the virtual private network (VPN) systems that businesses have traditionally relied on to secure pockets of remote-working employees were not designed to effectively secure a large remote workforce, so new approaches and technologies are needed. New security methodologies such as zero-trust access (ZTA) and technologies including the likes of unified endpoint management (UEM), user behavior and analytics (UBA), and mobile threat defense (MTD) solutions can play an important role in securing remote work and in finding the balance businesses need. However, it is also important that organizations consider not just the technologies that can help but also changes to people and process practices.

But more broadly, the inability of enterprise security organizations to make meaningful gains in the past decade can be tied to a set of core challenges. Enterprises often need new solutions to address new threats or operational difficulties, but this has resulted in solution sprawl, with the average organization having at least 20 different security tools, which is more than most can manage successfully. In addition, organizations have too many sources of security telemetry, and analyzing it

all in real time (never mind correlating and learning from it) is nearly impossible. Add to this the reality that all these tools and datasets are only scantly integrated. This means coordinated, policy-driven response is extremely difficult, and orchestrated, automated processes are little more than a fantasy.

Consolidation and replacement of security tools is the kind of exercise that becomes focused on solutions rather than requirements. However, a real opportunity has arisen from the availability of enterprise-strength cloud-based capabilities that can support a vast scale of security data and allow it to be integrated and processed much more rapidly, resulting in much more timely insight that can drive faster reaction times to events. The legacy model of numerous security solutions with discrete roles, connected via point integrations, is becoming superseded by far greater abstraction from the concept of those solutions. This is happening as leading security vendors combine and transform legacy elements into cloud-enabled and far more automated capabilities that will genuinely redefine how enterprises purchase, deploy, and operate their cybersecurity architectures. Even one of the last bastions of physically positioned security hardware, the firewall, is beginning a journey to becoming cloud based, at least at the scale where the individual firewall protects a discrete organizational unit such as a branch.

Connecting insight and response is critical for high-strength protection

As threats have continued to mushroom and attacks have increased in number, sophistication, variety, and frequency, so the profile of incident response has risen. There is a need for swifter action on the part of responders to contain attacks, mitigate their impact, and subsequently remediate the damage done, to which end orchestration tools are required to streamline the response process. And, as with the scarcity of incident analysts driving the automation of producing insight, skilled responders too are at a premium in today's cyber-market. Consequently, there is also a requirement for at least the most basic, repetitive tasks within incident response to be automated, thus freeing up responders to focus on the tasks that really do require human intervention.

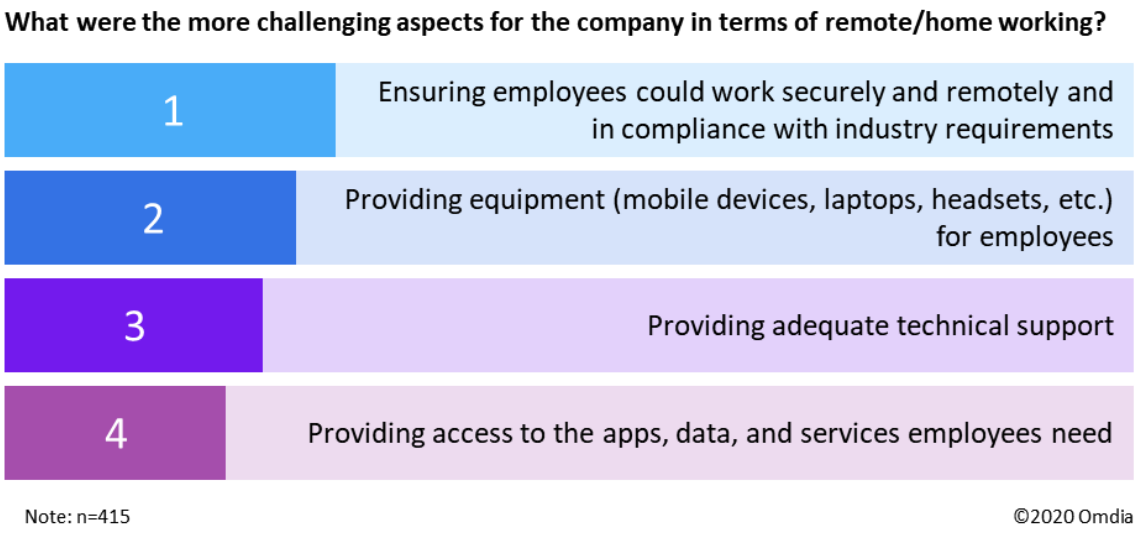
At the technical level, capabilities are needed to cover the three main areas of enterprise infrastructure (endpoint, network, and cloud) where response actions might be necessary. In the most advanced examples these are combined and integrated, a solution variant that Omdia labels xDR (*x* signifying the infrastructure element where response is needed; DR denoting detection and response). Where response is required at a process level, security orchestration and response (SOAR) operates defined workflows that can detail multiple actions (either automated or human operated) and that are triggered via integrations with other security solutions as appropriate.

Implementing and managing new secure workplaces extends beyond the desired capabilities of most organizations

Multiple challenges encountered in rapidly transitioning to remote working must be resolved sustainably

As we have seen, the transition to distributed work styles will be a permanent change for many employees, even in a postpandemic world. While remote working offers many benefits to employees and employers, there are also challenges that businesses must consider and overcome to ensure that remote work styles are successful over the long term, as illustrated in **Figure 6**.

Figure 6: Key challenges businesses are experiencing with remote working



Source: Omdia Future of Work Survey 2020

Some of the key challenges relate to ensuring that employees have easy access to the technologies, devices, data, and applications they need in order to work productively. People need access to different types of technology when they work remotely. For example, a laptop may be required in place of the desktop PC that an employee may have previously used in the office environment. There are also important logistical challenges that need to be considered: getting physical devices into employees' hands, initial device setup, and delivering remote troubleshooting/support. All these may have been well-defined and straightforward processes when the majority of employees were based in the office; however, as the workforce becomes more dispersed, new technical and logistical challenges and complexities emerge. Also, all of these processes must incorporate the right level of security to meet policies and protection requirements.

Extending in-house security/support capabilities is often a difficult option

Because security is such a complex and ever-evolving topic that incorporates many different tools, services, and competencies, businesses often have gaps in terms of what they can deliver in-house. While organizations must retain responsibility for overall governance over their own security technologies and strategy, the skills and technical resources required for complex operations represent considerable investments in noncore competencies, management capability, and setup time. Services partners are, therefore, an attractive proposition for businesses looking to plug these gaps or to adopt integrated services that can cover most or all of their requirements across a range of security-related capabilities.

While expertise in leading security solutions is one set of key capabilities that such partners can provide, their experience in making organizational security work as a whole is also important. This

can extend to cultural issues and matters such as HR and IT policies, all of which should be carefully considered by organizations as part of their commitment to better prevent, detect, and remediate security issues. Survey results detailed in NTT Ltd.'s *2020 Intelligent Workplace Report* found that many organizations have not yet updated their IT and HR policies since more employees started working remotely. Clearly, in both of these areas documents should guide employees on how to work securely and maintain compliance.

Security is not just a technology issue: the impact of people is vital in maintaining a strong security stance. Even if enterprises have the best mobile security technology and services on the market, just one bad decision or mistake made by an employee can have a significant impact on an enterprise's security; hence, it is very important to ensure that employee training addresses a broad range of practices and behaviors that can reduce the risk of causing such impact. With compliance requirements such as the EU's General Data Protection Regulation (GDPR) now being widespread in their reach, the rigor of privacy and security that is in operation in the office environment must also extend to remote working.

But because the risk always remains extant, there are always requirements for appropriate processes/tools and expertise to undertake investigative/remedial work and, sometimes, to address consequences such as data breaches and the resulting compliance reporting. These requirements are rising up the priority list: in a survey undertaken by NTT Ltd. during the early phase of the pandemic, 77% of organizations indicated that they have found it more difficult to spot IT security/business risk brought about by employees working remotely. Their need to address this difficulty is also flagged up by industry insight on the constantly changing approaches of threat actors. NTT Ltd.'s *2020 Global Threat Intelligence Report* highlights that adversaries are taking advantage of the current pandemic by repurposing their tool sets, deploying new infrastructure, and developing innovative campaigns to proactively target vulnerable organizations, very likely those that had to make haste to support remote working and may not have done so as sustainably as necessary. The report gives a very broad perspective of how attacks are being conducted and finds that some 21% of malware detected was in the form of a vulnerability scanner; this supports the premise that attackers are developing automated means of finding organizations' weaknesses.

Many services partners offer a range of cybersecurity consulting services that span strategic activities such as risk assessments and compliance considerations, through more day-to-day security-management-focused activities. Having the skills and resources needed to manage the many threats now faced is a huge challenge for businesses; the cybersecurity skills gap is very real. In its *Cybersecurity Workforce Study, 2019*, the research organization (ISC)[2] estimated a global gap in the cybersecurity workforce of 4.07 million people, which requires the cybersecurity workforce to grow by 145%. Clearly, enterprises that aim to recruit specialist cybersecurity skills for in-house positions are likely to encounter a scarcity and increased costs because lack of supply raises remuneration for cybersecurity staff.

A digital workspace platform can integrate siloed capabilities

As businesses look to rationalize and better integrate multiple security capabilities, Omdia believes that digital workspace platforms will increasingly be a key integration layer within an overall

workspace/workplace ecosystem that is “secure by design.” Different security capabilities can deliver more aggregated insights via such integration, and the platform can surface workflows that support actions such as remediation. Digital workspace platforms that leverage APIs in connecting security, productivity, mobility, and communication applications become a hub and single interface from which employees, including IT admins and security operation personnel, can more effectively carry out important tasks. Such platforms support the development of workflows to connect what may previously have been siloed enterprise solutions. For example, many CISOs are still having to manage legacy perimeter-based enterprises on top of newly developed architectures, further complicating the job of integration while migration to the cloud is ongoing. New automation and machine learning (ML) capabilities can also be developed to bring further efficiencies in a more unified ecosystem that may span productivity, mobility management, and collaboration capabilities as well as security.

Appendix

Methodology

Part of this publication analyzes and discusses results from Omdia's 2020 Future of Work survey, completed in August 2020. The survey draws on the insights shared by key business decision makers across different industries, including those in roles such as CIO, CTO, CFO, and HR director.

Results are also mentioned from two of NTT Ltd.'s publications:

2020 Global Threat Intelligence Report

2020 Intelligent Workplace Report

Skills gap estimates are referenced from (ISC)²'s *Cybersecurity Workforce Study 2019*, available at https://www.isc2.org/Research/-/media/6573BE9062B64FC7B4B91F20ECC56299.ashx.

Additional information and data referenced within the report and as part of the evaluations was gathered via vendor briefings, engagement with enterprises, and external sites such as vendor websites and from existing material and data sources published on the Omdia Knowledge Center.

Authors

Alan Rodger
Senior Analyst, Cybersecurity
alan.rodger@omdia.com

Adam Holtby
Principal Analyst, Digital Workplace
adam.holtby@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

About NTT Ltd.

NTT Ltd. (https://hello.global.ntt/) is a leading global technology services company. Working with organizations around the world, it aims to achieve business outcomes through intelligent technology solutions. Intelligent, in this context, means data driven, connected, digital, and secure. Its global assets and integrated ICT stack capabilities provide unique offerings in cloud-enabling networking, hybrid cloud, data centers, digital transformation, client experience, workplace, and cybersecurity.

NTT Ltd. and Palo Alto Networks are working together to enable a secure and connected future. By combining NTT Ltd.'s intelligence-driven security services and Palo Alto Networks' industry-leading technologies, we've created a secure access ecosystem that delivers comprehensive

and automated security solutions across head offices, branches and mobile workers, in line with your business objectives.

About Palo Alto Networks

Palo Alto Networks (https://www.paloaltonetworks.com/) is a leading global cybersecurity company, aiming to shape the cloud-centric future with technology that is transforming the way people and organizations operate. Its mission is to be the cybersecurity partner of choice, protecting society's digital way of life. It aims to address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, it positions itself at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Its vision is a world where each day is safer and more secure than the one before.

Copyright notice and disclaimer

investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.