HP WOLF SECURITY

OUT OF SIGHT & OUT OF MIND REPORT

HP WOLF SECURITY

EXECUTIVE SUMMARY

The workplace has evolved, ushering in the age of hybrid working. Digital and workplace transformation have both been accelerated, and work has forever changed. Workforces will become increasingly distributed and less visible to IT and security teams. The number of freelancers will also grow exponentially, reaching 50% of the US workforce by 2027. As a result, it has never been more challenging for IT teams to deploy, manage, and secure their IT ecosystem.

This is the new reality for organizations, and they have no choice but to adapt and evolve.

Any major transformation comes with a period of adjustment. Yet when such transformation is suddenly accelerated, it often comes with pain points. Many organizations were unprepared to support such a mass workforce shift. From onboarding users with secure devices, to triaging threats, the time and complexity involved in delivering IT security support remotely has been a huge challenge.

Cybercriminals have been quick to capitalize on the chaos. They are targeting distributed workers more frequently. They are compromising more machines and triggering more alerts. Furthermore, they are taking advantage of the fact that organizations have less visibility, which is allowing them to go more unnoticed. They are counting on the fact businesses are struggling to keep up.

In this HP Wolf Security Out of Sight & Out of Mind report, we gather data from a global YouGov online survey of 8,443 office workers who shifted to Working from Home (WFH) during the pandemic and a global survey of 1,100 IT decision makers (ITDMs). The report examines how recent workforce transformation is changing user behavior and its impact on the manageability of IT security.

In this HP Wolf Security report, we will explore:

- **The New Shadow IT:** Since working more from home, users have been cutting IT out of the loop. They are buying, installing, and using IT equipment unsanctioned – without considering security. They are also clicking on potentially harmful links without reporting it to IT.
- **Attackers are getting in:** Risk is increasing. IT teams say they are seeing a rise in employees opening malicious attachments resulting in higher rebuild rates on compromised machines. This is just the tip of the iceberg – it's likely there are many more unknown compromised devices out there.
- **Something's got to give:** Compounding these issues, the IT onboarding and support cost is increasing and becoming more complex. From triaging threats to provisioning and onboarding employees with secure devices, rebuilding and patching IT security is increasingly unmanageable. This is making it harder than ever to protect the enterprise.

HP WOLF SECURITY VIEWPOINT:

IAN PRATT, GLOBAL HEAD OF SECURITY, PERSONAL SYSTEMS, HP INC.:

"This report highlights the harsh reality facing businesses today. Threat actors are increasingly adept at bypassing endpoint defenses. Users are acting autonomously, equipping themselves with tools outside of IT's purview. People are less sure about what they can and can't trust.

While many of these issues existed long before the pandemic, the tectonic shifts in behavior driven by the rapid rise of hybrid working has exacerbated these problems. We can't keep doing the same things we have always done. IT and security need to evolve. We need a new security architecture that not only protects against known and unknown threats, but that helps to reduce the burden to liberate cybersecurity teams and users alike."

KEY STATS

YOUGOV SURVEY OF OFFICE WORKERS SHOWS THAT:

68% who purchased devices to support WFH say security wasn't a major consideration

43% didn't get their new PC or laptop checked or installed by IT

49% of 18–24-year-olds clicked on malicious emails more often since WFH

70% who clicked on suspicious links didn't report it to IT

TOLUNA SURVEY OF ITDMS SHOWS THAT:

74% saw a rise in employees opening malicious links or attachments

79% say rebuild rates have increased

77% say triaging alerts is more time-consuming

62% of alerts relating to the endpoint are false positives

A NEW SHADOW IT IS EMERGING AS USERS DRIFT FURTHER OUTSIDE OF IT'S PURVIEW

Research suggests 70% of employees globally want **flexible working options to continue** post pandemic, and nine out of ten organizations will be **combining remote and on-site working** in the future. As a result, the face of work is changing. People are setting up home offices. They are shifting to anytime working models that enable working at different times of day. They are also working in more isolated environments without their colleagues on hand for a second opinion. This is leading to shifts in user behavior which present new challenges for IT and security teams.

'Shadow IT' is a concept that has typically referred to non-IT departments – such as finance or marketing – deploying software outside the purview of IT. The increasing popularity of cloud, in particular Software-as-a-Service, has been a key driver for this – now, any department can simply download and use new software within their own operational budget, enabling them to bypass IT. This trend has created many headaches for security and IT departments. It has clouded visibility of what is being used or how such services may impact data security, compliance, and governance.

Our research shows that the 'shadow' is now being cast even wider. Individuals are increasingly purchasing IT equipment and using these devices to connect to the corporate network, without being checked by IT. 45% of office workers surveyed purchased personal IT equipment to support home working in the past year, with 29% buying a PC/laptop and 16% buying a printer (fig. 1).

Figure 1 – Office workers by country that have purchased IT equipment to support home working

	GLOBAL	CANADA	MEXICO	USA	GERMANY	UK	JAPAN	AUSTRALIA
PC OR LAPTOP	29%	35%	45%	31%	21%	14%	20%	34%
PRINTER (WITH OR WITHOUT AN INTEGRATED SCANNER)	16%	19%	27%	17%	14%	8%	9%	18%
INTERNET ROUTER	15%	16%	22%	18%	11%	4%	9%	19%
TABLET / IPAD	11%	13%	19%	12%	10%	5%	6%	13%

Of those that purchased a new device, just 32% said security was a major consideration – a figure that drops further to 16% in the UK (fig. 2). Cost and functionality were deemed more important: 69% said functionality was a major consideration, and 51% said cost was. Further to this, 43% didn't get their PC or laptop checked or installed by IT, while 50% said their printer wasn't checked or installed by IT (fig. 3). When you consider that such devices could be used as a backdoor into business networks, this is a worrying trend.

Figure 2 – Office worker purchasing considerations when buying a new device for home working

	GLOBAL	CANADA	MEXICO	USA	GERMANY	UK	JAPAN	AUSTRALIA
COST	51%	52%	47%	51%	45%	54%	52%	54%
FUNCTIO-NALITY	69%	64%	77%	70%	80%	62%	43%	69%
SECURITY	32%	32%	33%	32%	33%	16%	37%	34%

"INDIVIDUALS ARE NOW PURCHASING IT EQUIPMENT AND USING THESE DEVICES TO CONNECT TO THE CORPORATE NETWORK, WITHOUT IT TEAM'S KNOWLEDGE."

HP WOLF SECURITY VIEWPOINT:

IAN PRATT, GLOBAL HEAD OF SECURITY, PERSONAL SYSTEMS, HP INC.:

"People often don't know if they have clicked on something malicious, so the real numbers are likely much higher. Threat actors don't always announce themselves, as playing the 'long game' to move laterally and infiltrate higher-value infrastructure has proven to be more lucrative. Limiting what an attacker can do if an endpoint is compromised is therefore essential -- containing the threat mitigates harmful impact."

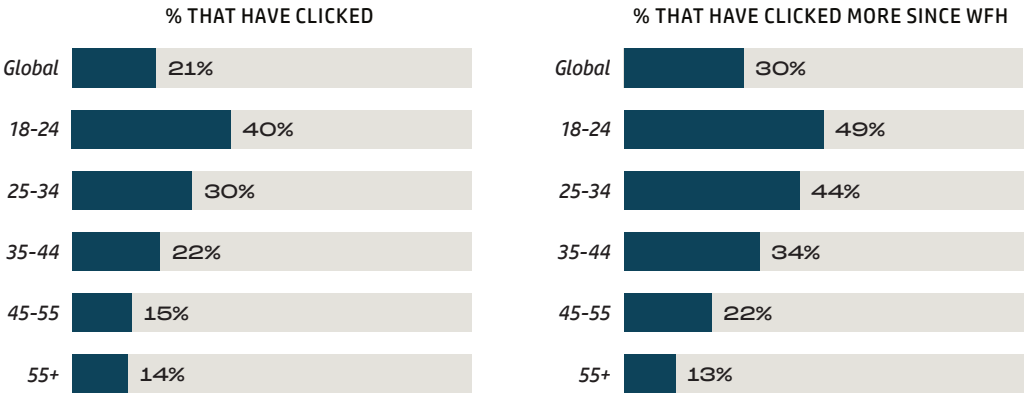
JOANNA BURKEY, CHIEF INFORMATION SECURITY OFFICER (CISO), HP INC.:

"With increasingly distributed teams, there are fewer informal networks for people to sanity check: 'does this look a bit strange' before they click. Education helps, but it can only get you so far. While we should encourage and make it easy for people to report incidents, we can't rely on self-reporting alone. Having layered security in place that can provide the right level of visibility is key."

Figure 3 – Office workers that said their new equipment for home working was checked or installed by IT

The findings also indicate that people are being less vigilant or finding it harder to determine what is and isn't safe to click. 21% of office workers say that they have clicked on a malicious link since working from home; 30% of whom said they have done so more often since WFH (fig. 4). These figures rise significantly for 18-24-year-olds: 40% clicked on a malicious email and 49% have clicked more often since WFH. This figure is likely to be higher too, as it only accounts for people who know they have clicked on something – many don't.

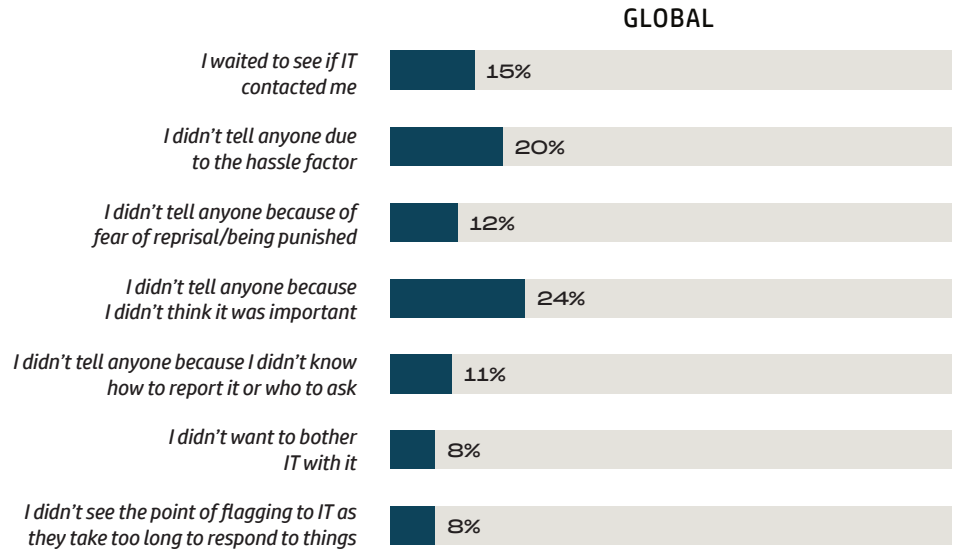
Figure 4 – Office workers by age that clicked on a malicious email while working from home



Of office workers that clicked when working from home, or nearly clicked, just 30% reported it to IT. Of those that reported it, 38% said they only did so because they had no choice, as their machine was broken. Of the 70% that didn't report it to IT, 24% didn't think it was important, 20% cited the "hassle factor" of reporting, and 15% said they just waited to see if they would be contacted by IT. However, 12% didn't tell anyone for fear of reprisal (fig. 5).

"35% OF OFFICE WORKERS USED TO "POP TO IT" WITH PROBLEMS WHEN IN THE OFFICE, BUT NOW THEY WFH IT'S TOO HARD TO CONTACT IT SUPPORT."

Figure 5 – Office workers' reactions after clicking on a malicious email



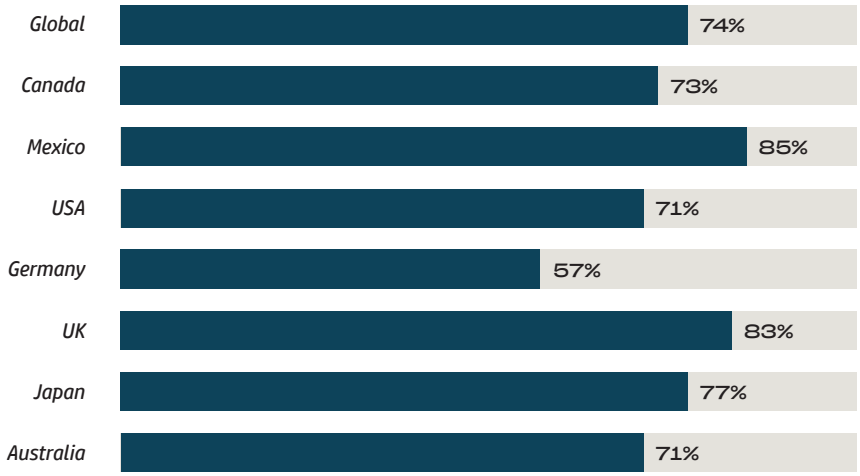
When considering the potential reasons for users not informing IT, the research suggests that remoteness may be a contributing factor. 35% of office workers "popped to IT" with problems when in the office, but now they WFH it's too hard to contact IT. A further 60% of 18–24-year-olds feel "a bit stranded" when WFH, and worry that if something went wrong, they'd be on their own. This compares to 48% of all office workers.

PERFECT STORM FOR IT AS THREATS RISE, COMPLEXITY INCREASES, AND IT SECURITY BECOMES MORE UNMANAGEABLE

The supercharged shift to home working made it more difficult than ever to deliver IT security support, a trend set to continue in the hybrid workplace. Exacerbating the issue is the fact the threat level is rising. By their own admission, users are finding it harder to decipher what they can and can't click on and are keeping IT out of the loop on potential issues as well as purchases. At the same time, hackers are more inventive in their approach to tricking users.

74% of IT teams saw a rise in employees opening malicious links or attachments – a figure that increases significantly in Mexico and the UK (85% and 83% respectively) (fig. 6). When you consider that only 21% of office workers surveyed admitted to clicking on a link, this suggests IT sees more of those than employees are aware of.

Figure 6 – Percentage of IT teams by country that have seen a rise in employees opening malicious links or attachments



It comes as little surprise, therefore, that rebuilds on compromised machines are rising too. 79% of IT teams say their rebuild rate has increased (fig. 7). This indicates the number of compromised machines is increasing. But the true figure of compromised machines is potentially much higher: 80% of IT teams worry employee devices might be compromised without their knowledge.

Figure 7 – The average number of devices being rebuilt per month

	GLOBAL	CANADA	MEXICO	USA	GERMANY	UK	JAPAN	AUSTRALIA
AVERAGE	61.9	67.1	56.3	67.1	57.3	61	61.7	61.3
INCREASED	79%	79%	86%	81%	69%	86%	79%	72%

As the tide of threats rises, Security Operation Centers (SOCs) are being flooded with alerts. Respondents estimate that SOC teams receive an average of 4,200 alerts each day – 23% get 5000-10000 (fig. 8).

"80% OF IT TEAMS WORRY EMPLOYEE DEVICES MIGHT BE COMPROMISED AND THEY DON'T KNOW ABOUT IT."

HP WOLF SECURITY VIEWPOINT:

IAN PRATT, GLOBAL HEAD OF SECURITY, PERSONAL SYSTEMS, HP INC.:

"As IT continues to grow in complexity, security support is becoming increasingly unmanageable. HP's 2021 Q3 threat report shows that attackers are quick off the mark when it comes to exploiting newly found vulnerabilities, counting on the fact emergency patching is too complex and time consuming for most organizations."

JOANNA BURKEY, CHIEF INFORMATION SECURITY OFFICER (CISO), HP INC.:

"For hybrid working to be a success, we need to find a path forward that frees IT and security teams to focus on tasks that really add value. This means releasing teams from mundane and manual tasks that could easily be embedded or automated – such as spending hours provisioning and fielding user access requests."

Figure 8 – The average number of alerts received by SOC teams each day

	GLOBAL	CANADA	MEXICO	USA	GERMANY	UK	JAPAN	AUSTRALIA
LESS THAN 2,000 PER DAY	12%	5%	22%	11%	21%	5%	7%	13%
APPROX 2,000 - 5,000 PER DAY	65%	63%	59%	64%	68%	72%	73%	58%
APPROX 5,000 - 10,000 PER DAY	23%	32%	19%	25%	11%	23%	20%	29%
AVERAGE	4236.4	4710	3916.7	4367.5	3643.3	4326.7	4200	4446.7

While many of these will be Firewall alerts, requiring minimal intervention, on average 14% of alerts are directly related to the endpoint. Respondents estimated that they triage an average of 816 endpoint security alerts each week[1]. However, 62% of alerts relating to the endpoint are false positives with no malicious impact, leading to a lot of wasted time.

Yet it is not just the volume of threats that is creating headaches for IT and security teams. The distributed nature of work is creating a logistical nightmare that is driving up the cost, time, and complexity to secure the workplace.

79% of IT teams say that the time to rebuild machines has increased by an estimated 47%, taking an average of 4 hours each time. Similarly, 77% say triaging events has become more time-consuming.

Furthermore, 74% of IT teams have spent more time fielding queries related to accessing websites, applications or documents that have been blocked by security policies/tools.

It is a similar story across the IT security support spectrum:

- 64% of IT teams say that securely recovering Operating Systems (OS) and users is more time-consuming and difficult
- 65% say patching endpoint devices is more time-consuming and difficult
- 64% say the same of provisioning and onboarding new starters with secure devices

It is perhaps no surprise that IT teams estimate the cost of IT support in relation to security has risen by 52%. When coupled with a severe industry skills shortage, 57% of cybersecurity professionals say their organizations have been impacted by the global cybersecurity skills shortage, teams are being stretched to breaking point.

83% of IT teams say the pandemic has put even more strain on IT support because of home worker security problems and 77% of IT teams say they fear teams will burnout and consider quitting.

"62% OF THE ALERTS RELATING TO THE ENDPOINT END UP BEING FALSE POSITIVES, LEADING TO A LOT OF WASTED TIME."

SUMMARY

HP Wolf Security: Out of Sight & Out of Mind summary:

- The new Shadow IT – made up of individual employees working from home – is buying and connecting devices outside of IT purview.
- This is introducing new risks, as potentially insecure devices and networks are being connected to the wider business.
- Users are increasingly clicking on potentially harmful links and downloads, opening the door for would-be attackers.
- When mistakes are made, users are less likely to report it to IT.
- IT and security teams are seeing an increase in user-initiated threats, leading to more compromised machines, putting company data and operations at risk.
- Compounding this increased threat, it is becoming much harder, costlier, and time-consuming to manage and deliver IT security support.

FINAL THOUGHTS FROM HP WOLF SECURITY

Today's hybrid working environments are fluid. There is no defined perimeter. The user and the endpoint are on the front line.

Organizations that try to force a change in natural workflows and WFH behaviors are fighting a losing battle. While security education is very important, it's not enough on its own.

Increasingly well-funded and sophisticated threat actors at the door, innovating new ways to trick users. People are more isolated. They are under pressure and working at speed. It is very easy to make a mistake.

At the same time, IT security support is becoming increasingly unmanageable. From patching to triage and provisioning users, IT teams are constantly firefighting. They are not being given the headspace they need to think and innovate.

In this context, endpoint security has never been more important. But trying to detect and prevent malicious activity in real-time is untenable in today's hybrid, hyper-digital world. The shocking increase in rebuild rates is testament to this.

Organizations need IT teams focused on driving innovation. Security teams focused on preventing the next big breach. But they can't do this if they are flooded by alerts and tied down by necessary but mundane tasks.

There needs to be a new way.

SECURING THE FUTURE OF WORK REQUIRES A NEW SECURITY ARCHITECTURE APPROACH

We must embrace a new way of managing security threats to enable hybrid working. This requires an architectural approach to security that helps to mitigate risk, while limiting the impact of failure through segmentation.

A user should not be a single point of security failure. To secure the future of work, security systems and strategies must be designed for resilience, to ensure that the compromise of one device does not result in the compromise of critical assets.

By applying the key principles of Zero Trust – least privilege, strong isolation, mandatory access control and strong identity management – organizations can reduce the addressable attack surface. This enables quick recovery in the event of compromise and reduces pressure on IT security support teams.

An example of this approach in action is the use of isolation to protect against common attack vectors. By executing 'risky' tasks – such as clicking on links, attachments and downloads, or visiting potentially harmful web pages – in a disposable, isolated virtual-machine (VM), separated from the operating system, malware is rendered harmless. If a user does initiate a malicious document, the attacker is trapped. They have nowhere to go and nothing to steal.

Isolation relieves pressure on IT and security teams in several ways. It ensures the endpoint stays protected from the most common threats, helping to reduce or even eradicate rebuilds on compromised machines and keep data and systems safe.

It also adds a layer of protection against many vulnerabilities. This helps to ease the pressure of emergency patching by allowing teams to take a slower, more managed approach. IT and security teams can also lift user restrictions put in place to reduce security exposure, reducing help desk calls. Moreover, as IT and security teams are equipped with data on each attack, there are no false positives. This helps to reduce the number of alerts the team must investigate.

HP WOLF SECURITY VIEWPOINT:

IAN PRATT, GLOBAL HEAD OF SECURITY, PERSONAL SYSTEMS, HP INC.:

"The leading technology of the future will be secure-by-design and intelligent enough to not simply detect threats, but to contain and mitigate their impact, and to recover quickly in the event of a breach – which could happen at any time, to any one of us. This protection should extend below and above the Operating System and deliver protection to both known and unknown threats – even zero days. By building securing in from the hardware up, we can alleviate pressure on support teams while also ensuring users are free to do their job uninhibited."

Beyond this, by isolating malware in a safe, disposable VM, the malware can play out in full without any risk. This provides unique insights for threat analysts. The intelligence gathered can be utilized by the IT and security teams to hunt down APTs and other serious threats to the organization. This helps to turn a traditional weakness – the endpoint – into an intelligence gathering strength.

SECURING THE FUTURE OF WORK – A CALL TO ACTION

Hybrid working is the future. Workforce and digital transformation offer huge benefits to businesses. But the risks that accompany the opportunity must be understood and addressed. Given the increasingly distributed nature of work, strong endpoint security is essential.

IT teams are in dire need of better endpoint security that equips them with greater visibility and management tools. Where possible, IT teams should provision users with devices that have security built into the hardware to reduce support strains. For example, remote recovery capabilities and self-healing firmware can help to recover devices in the event of compromise. This can help to transform the role of support in security and keep teams focused on delivering value to the business.

By doing so, organizations will be best positioned to:

- Confidently remove restrictions and say yes to more employee access requests, by providing transparent security that supports business innovation.
- Reduce the attack surface and render malware harmless through isolation.
- Enable remote recovery and reimaging of machines and operating systems to reduce pressure on IT support teams.
- Deliver a first-class user experience without sacrificing security by using devices that provide built-in security at the point of purchase to deliver a seamless user experience.
- Reduce false positives and stop teams chasing false leads; allowing them to focus on real threats by gathering threat intelligence from the endpoints.
- Eradicate rebuilds and endpoint remediation and reimaging due to malware infections by using threat containment and isolation to protect against the most common attack vectors.
- Avoid crisis patching and manage security patching for applications and operating systems in a controlled and planned way.

ABOUT HP WOLF SECURITY

From the maker of the world's most secure PCs[i] and Printers[ii], HP Wolf Security is a new breed[iii] of endpoint security. HP's portfolio of hardware-enforced security and endpoint-focused security services are designed to help organizations safeguard PCs, printers, and people from circling cyber predators. HP Wolf Security provides comprehensive endpoint protection and resiliency that starts at the hardware level and extends across software and services.

METHODOLOGY

The findings in this report are made up from two separate data sources:

01 A YouGov online survey of 8,443 adults in the US, the UK, Mexico, Germany, Australia, Canada, and Japan who used to be office workers, and worked from home the same amount or more than before the pandemic. Fieldwork was undertaken between 17th – 25th March 2021. The survey was carried out online.

02 A Toluna survey of 1,100 IT decision makers in the UK, the US, Canada, Mexico, Germany, Australia, and Japan. Fieldwork was undertaken between 19th March – 6th April 2021. The survey was carried out online.

DISCLAIMERS

[i] Based on HP's unique and comprehensive security capabilities at no additional cost among vendors on HP Elite PCs with Windows and 8th Gen and higher Intel® processors or AMD Ryzen™ 4000 processors and higher; HP ProDesk 600 G6 with Intel® 10th Gen and higher processors; and HP ProBook 600 with AMD Ryzen™ 4000 or Intel® 11th Gen processors and higher.

[ii] HP's most advanced embedded security features are available on HP Enterprise and HP Managed devices with HP FutureSmart firmware 4.5 or above. Claim based on HP review of 2021 published features of competitive in-class printers. Only HP offers a combination of security features to automatically detect, stop, and recover from attacks with a self-healing reboot, in alignment with NIST SP 800-193 guidelines for device cyber resiliency. For a list of compatible products, visit: hp.com/go/PrintersThatProtect. For more information, visit: hp.com/go/PrinterSecurityClaims.

[iii] HP Security is now HP Wolf Security. Security features vary by platform, please see product data sheet for details.

HP WOLF SECURITY