Making the right decisions for IT security can safeguard your devices, data and reputation. Discover how robust hardware and services can keep your organization protected.
In today’s ever-evolving digital landscape, organizations are under a growing risk from sophisticated cybercrime. From the changing ways employees work to the rising number of serious threats that take aim at endpoints, there are plenty of areas where an organization’s IT security can be left vulnerable.

The stakes are high. But there are ways to strengthen your defenses.

To avoid becoming the next name in the news because of a cyberbreach, organizations need to focus attention on security features at the device level and start to move towards services that can help tackle current security risks, and the unknown threats of the future.
Over the next few pages, we’re going to take you through some of the most dominant cybersecurity trends and threats to today’s endpoints. But first, ask: what is your organization doing to stay protected? Do your PC purchasing decisions include these three key aspects? We’ll give you more information about how to ensure your IT incorporates these features in a later section.

IS YOUR ORGANIZATION PRIORITIZING THESE THREE AREAS?

1. Resilient hardware
   that protects firmware and applications, and can reimage and recover the BIOS quickly, so you can get back to business fast.

2. Layers of protection
   to proactively defend against threats below, above and in the OS, and prevent impact to the network – from hardware to threat prevention technology.

3. Proactive management
   to enforce your security policies, and actively monitor and respond to threats.
85% of businesses say productivity is better with flexible working, but as employees move outside the office, so can sensitive data.
“People can work on the go – they work in coffee shops, hotels and planes. A lot of people are connecting to random wireless networks, they have no idea of credentials. And then they go back to the office, plug back into the environment and that system has been compromised, thus putting the whole company at risk.”

Michael Calce, a.k.a. ’MafiaBoy’, Chairman of HP’s Security Advisory Board

**FOUR THINGS TO CONSIDER**

The following questions can help you begin to assess the current status of your hardware and services, and whether your organization can sufficiently guard against potential attacks.

- Does your organization have a patch management process to systematically fix software vulnerabilities?
- Would your organization benefit from regular insights into the status and effectiveness of your security position?
- What type of technology does your organization currently invest in for endpoint security?
- Do you have end-user security training, and if so, how effective is it?
The internet is fundamental to how we do business today. But as the internet and digital world grows in complexity, so does cybercrime and its threat to security. Threats are growing in number and intricacy, and are fast to infiltrate the wider organization once they’ve made their way into a system.

Organizations have decisions to make and features to look out for when acquiring new services and devices, to safeguard against the rising risks. By looking towards hardware and services that can respond to threats quickly, users stay up and running, and organizations stay productive and avoid the long-term financial consequences that come with cybercrime.

68% of business leaders say cybersecurity risks are increasing.\(^4\)

The average cost of a cyberattack is $13m, up 12% in a year.\(^4\)

Cyberattacks and data fraud are two of the top five risks CEOs are likely to face.\(^4\)
A LOOK AT DATA BREACHES IN INDUSTRIES
Over the last few years, stories of data breaches and computer fraud have become more commonplace across the media. Cybercrime doesn’t discriminate. From hospitality firms and social media giants to municipalities and healthcare providers, even the biggest organizations from around the world can make the headlines for losing control over its customer, employee and company data.

FACEBOOK
In April 2019, Facebook was once again under scrutiny as millions of user records had been exposed. The popular social networking site allowed two apps access to the personal information of its users – and the data had been stored on insecure servers. A total of 540 million records, including Facebook IDs, comments and likes, could be found.\(^5\)

This comes less than a year after Facebook announced the largest data breach in its history, which exposed personal information of up to 50 million users – an incident that was followed by the social media’s stock falling by more than 3%.\(^6\)
US CITIES OF BALTIMORE AND GREENVILLE

According to Verizon’s 2019 data breach investigation, 16% of breaches involved public sector entities – the highest percentage of sectors investigated. In May 2019, a ransomware attack hit Baltimore, Maryland, infecting around 10,000 government devices with a new strain of ransomware called RobbinHood, which blocked essential city services such as the payment of water bills and property taxes. Hackers initially demanded the city pay 13 bitcoins, approximately $100,000, to restore access to the systems. The city didn’t pay the ransom, and the resulting costs reached millions of dollars.

Baltimore was the second city to fall victim, after Greenville, North Carolina, which experienced the same strain of malicious cyberattack in the month previous. And it doesn’t end there. Many other cities around the world have been attacked, but have remained unannounced to the public.

AUSTRALIAN NATIONAL UNIVERSITY

The university confirmed that an estimated 200,000 people, including staff and students, had been affected by a major data breach, discovered in May 2019. In a message to the university body, the vice-chancellor stated that personal information, going back 19 years, such as names, addresses, payroll and bank account details had been accessed by an unauthorized, malicious actor.

“The reality is we’re getting to a point where most cities are facing a million of these attacks every week – this is now what local municipalities are up against.”

Nicole Perlroth, cybersecurity reporter, New York Times
04 WHAT THREATS SHOULD BE ON YOUR RADAR?

“We have been seeing a rise in firmware attacks, which are attacks on the software embedded in hardware, that can provide an attacker with control over an entire system. To address this degrading threat environment, HP has been leading the industry in designing systems and devices with security built-in from the hardware up, to help protect, detect and remediate attacks, with minimal interruption to users.”

Boris Balacheff, Chief Technologist for System Security Research and Innovation, HP, for HP Innovation Journal, Cybersecurity special edition

Threats are lurking. And they come in many different forms. But with every threat there’s a way to stay protected. Here are several ways you could be compromised, and what to do about it.
<table>
<thead>
<tr>
<th><strong>CURRENT OUTLOOK:</strong></th>
<th><strong>WAYS TO RESOLVE:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The threats on the rise</td>
<td>Features to look out for to protect against the threats</td>
</tr>
</tbody>
</table>

**Unsecure devices for remote workers**
More and more employees work across different devices, locations and connections – and not all will be secure.

Real-time monitoring and analytics give an oversight of device health and can see where attacks are coming from to ensure prompt response to the security event.

**Advanced malware attacks**
Malware that has a specific target – modified with different ways and techniques to infiltrate a system – can avoid detection by traditional security controls and antivirus.

Deep-learning AI can identify and protect against new, never before seen malware.

**Firmware attacks**
Firmware security, particularly in the BIOS, can be vulnerable to malware and exploited by hackers.

Self-healing BIOS protection can detect threats and automatically recover the BIOS from attacks or corruption, without intervention from IT.

*Windows 10*

Take the lead with Windows 10 Pro devices.
CURRENT OUTLOOK:
The threats on the rise

Ransomware
The second most common type of malware incident — up 15% in the first half of 2019 — ransomware is designed to lock, encrypt and deny access to data until a ransom is paid.

Cryptojacking
A form of cyberattack where a hacker hijacks a target’s processing power to mine cryptocurrency. Cryptomining malware soared by 4000% in 2018, McAfee found and can be costly in electricity, network performance and vulnerability to other attacks.

Human error and endpoints
Endpoints are common attack vectors. Pair this with employee susceptibility to cybersecurity attacks, threats to the endpoint can be common and, ultimately, successful. Email is the most common point of entry for malware and accounts for 94% of delivery.

DECISIONS TO MAKE:
Features to look out for to protect against the threats

Hardware-enforced protection can help protect PCs from ransomware and facilitate fast recovery to minimize impact and reduce downtime.

Management services can ensure you’re equipped with the latest devices, up to date software and sophisticated protection.

Want to know more about cryptojacking? View our Cryptojacking Guide to discover how to keep jacks at bay.

Advanced malware protection with isolation technology contains email, browser and file attacks to prevent the spread from victim 0.

Security policies and antivirus software alone are insufficient — and organizations should be considering additional layers of protection and services for the final line of defense.
Endpoints are a target for cyberattacks, and it’s with growing frequency that breaches are traced back to starting at the endpoint. From the decentralization of the workplace – where devices can be difficult to keep track of – to the pressure from attacks that antivirus miss, a lack of endpoint security can mean huge disruption to an organization, to productivity and to the bottom line.

64% of organizations reported a major breach that started at the endpoint.
### CURRENT OUTLOOK:
Endpoints represent a weak link in security

**Zero-day attacks are four times more likely to compromise organizations.**¹²

57% of successful attacks are missed by traditional antivirus.¹²

Over half of breaches take months or longer to discover.⁷

The frequency of new or unknown zero-day attacks has increased from 24% to 37% in 2018.¹²

48% of malicious email attachments are Office files.¹³

---

### WAYS TO RESOLVE:
Considerations that protect endpoints against threats

Managed security services can protect against zero-day attacks through real-time threat protection and analytics services.

Going beyond traditional antivirus protection with deep-learning-based artificial intelligence can further protect devices.

Services that give a full overview of device health and insights reporting can help organizations uncover issues and protect devices.

With new types of malware appearing every day, deep learning AI can protect against never before seen attacks, before they happen.

Real-time threat isolation technology traps malware from email attachments and file download attacks, preventing them from impacting the device and network.

---

**Windows 10**

Take the lead with Windows 10 Pro devices.
**THE HUMAN ELEMENT**

Where there are endpoints, there are employees. And where there are people, there’s inevitable human error, and fraudsters poised to take advantage. Verizon’s 2019 data breach report found that 21% of breaches were caused by human error, up 5% in 5 years. Could this be due to a lack of security awareness? Research from Proofpoint found that employees are answering almost a quarter of security-related questions incorrectly, including categories related to mobile encryption, actions to take following a suspected breach and identifying phishing attacks.

Social engineering, from spear phishing to pretexting, can trick employees into visiting and entering sensitive information into fraudulent sites, or into downloading and installing malware onto their devices. Although the frequency of breaches caused by phishing is moving in the right direction, organizations have certainly not seen the end of socially-engineered attacks.

- 32% of breaches involved phishing
- 65% of groups use spear phishing as the primary infection vector
- Almost 25% of people will click a phish each year
- The more phishing emails people click, the more likely they are to click again
“Statistically speaking, employees are often the weakest link. But they’re not necessarily at fault. Employees need to be equipped with the right technology. They need built-in security on their systems to help them navigate this never ending, vast space of potential breaches and attack vectors.”

Michael Calce, aka ‘MafiaBoy’, Chairman of HP’s Security Advisory Board

When human error brings vulnerability, decision makers need to explore new ways to protect the rest of the network. And although internal training and policies can work to cut down susceptibility, introducing security-enforced hardware, threat protection solutions and managed services can bolster defenses and fill in the security gaps.

GOING BEYOND THE BOTTOM LINE
The cost to organizations goes further than dollars. Trust, loyalty and reputation are impacted when an organization experiences a data breach. In fact, employee morale and business relations are the two top forms of damage caused by cybercrime.

Level of impact

- 47% employee morale
- 38% business relations
- 36% reputation/brand strength
“A lot of the traditional technology for security today is signature-based detection, and that’s just not sufficient anymore. I’m really excited with what HP have been developing with HP Sure Sense, which is essentially a behavioural type of detection versus signature based. So, there is a lot of defense being made to respond to attackers.”

Michael Calce, aka ‘MafiaBoy’, Chairman of HP’s Security Advisory Board

The forecast for today’s threats, vulnerabilities and risks may seem cloudy, but asking the right questions can equip your organization with the right protection. Your hardware and service requirements should reflect the changing face of cybersecurity and support your IT department in addressing the current and future risks — so prioritizing security features when acquiring new resources is a must. Think resilient hardware, layers of protection and proactive management.
TODAY’S RFP REQUIREMENTS
When completing a request for proposal and choosing an IT provider, explore these five crucial areas to help you meet the rising tide of security threats.

1 HARDWARE
Don’t allow malware or ransomware to take down your fleet and stall important projects. Choose hardware that’s designed to detect and recover from attacks, keeps you alerted to changes and limits the spread of breaches, so if an attack gets in your users can be back to business quickly.

Solution: HP Sure Start, HP Sure Run and HP Sure Recover for resilient hardware that can self-monitor and self-heal.

• HP Sure Start secures your PCs with hardware-enforced, self-healing protection that automatically recovers the BIOS, even before the PC boots into the OS.
• HP Sure Run keeps critical security protections up and running to prevent unwanted changes to settings.
• HP Sure Recover ensures fast, secure and automated recovery of your OS, with embedded reimaging, with only a network connection.

2 THREAT PROTECTION
When one in ten URLs leads to malware, your organization needs to keep endpoints protected against malicious websites and attachments. Look for resilient hardware features that can recognize new risks and secure your systems, in real time, against the advanced malware that employees and traditional antivirus can miss.

Solution: HP Sure Click for isolation technology that learns AI of HP Sure Sense, you’re protected against never before seen attacks.

HOW TO PLAN FOR ENDPOINT SECURITY AGAINST EVER-EVOLVING CYBERTHREATS
3 ANALYTICS AND INSIGHTS
Staying informed of device health and protection status can help IT to resolve issues before they affect users. Get access to analytics and reports around security incidents to identify threats, support security policies and give you the information and insights to protect devices and data.

Solution: HP Proactive Management with HP TechPulse for unique predictive analytics that gives a holistic view of device protection status, plus additional reports and alerts about unprotected devices and attempted threats – helping you monitor security and mitigate issues.

4 MANAGED SERVICES
IT security teams are faced with a complex, busy workload and little time for other priorities. Work with a provider that offers managed services to keep an eye on device health.

There’s a global talent shortfall. Given the 2.93 million unfulfilled cybersecurity jobs worldwide – predicted to reach 85 million by 2030, a figure equal to the population of Germany – could your IT team do with additional support?

Solution: HP Proactive Security for the world’s most advanced isolation security service for real-time malware protection on Windows 10 PCs. Plus, HP Service Experts can enforce security policies and perform daily management to monitor the health of your multi-OS environment – lightening the load on IT teams.

5 DEVICE REFRESH
Today’s landscape means the security goalposts frequently change. Organizations need to ensure their device refresh cadence allows for new technology with up to date security features to face the evolving cyberthreats.

Solution: HP Services for assistance at every stage of the device lifecycle to optimize your IT assets and resources, equip users with up to date technology, and ensure safe decommissioning and retiring of devices to help keep data secure.
07 ASKING THE RIGHT QUESTIONS TO STRENGTHEN SECURITY

How to Plan for Endpoint Security Against Ever-Evolving Cyber Threats
To help precisely identify your security expectations, delve deeper into the important hardware and services areas, and direct any questions you have to all potential providers. This will help you ensure it’s a partner you want to work with and will be able to sufficiently protect your organization. Use the following ten questions to explore your requirements, and inspire new queries and considerations.

1. **Can your hardware self-protect and recover from today’s malware threats?**
   Ask about hardware-enforced protection, including what can be recovered and restored, and how long it will take, when a threat hits.

2. **Will we be able to actively monitor malicious activity?**
   Find out if you have access to insights, reports and analytics to identify and respond to threats.

3. **What details will we get about attempted attacks?**
   Discover the type of information and analytics you’ll receive, and whether it will help you better understand the attacks targeting your organization.

4. **What are your capabilities in predictive analytics?**
   See if you’ll have access to analytics technology that can spot issues early to help safeguard against attacks.

5. **What technology do you have to recognize and stop never before seen threats?**
   Find out whether you can harness deep learning AI that recognizes malware instinctively and works in real time.
What additional privacy options can you offer?
Ask about features such as data erase, privacy screen or remote lock to protect sensitive data.

How can you prevent the spread of viruses?
Isolation technology can contain and protect against malware that enters through URLs, attachments or files – find out if this is something you can benefit from.

Will you be able to help us enforce our policies, and will there be experts available to support?
Make sure you can access specialized expertise to help you strengthen your security position and support the workloads of your internal IT teams.

What are your terms for fleet refresh?
Find out how frequently you’ll be able to update devices to ensure the strongest level of security.

How do you dispose of decommissioned devices?
Ensure that processes are in place to protect data for end-of-use devices.

Although attacks are growing with frequency and sophistication, there are opportunities for organizations to challenge the threats with strong security. With HP, you can explore a whole range of hardware features and services to meet your organization’s needs.

See why the HP EliteBook 840 G8 and the HP Elite family of laptops, desktops, and convertibles are HP's most secure PCs.27
SOURCES AND DISCLAIMERS

5 Telegraph, April 2019, Millions of Facebook user records exposed in data breach. https://www.telegraph.co.uk/technology/2019/04/03/millions-facebook-user-records-exposed-data-breach/
6 Fortune, Facebook loses around $13 billion in value after data breach affects 50 million of its users. September 2018
8 CISO Mag, June 2019, Baltimore hackers leak data on Twitter after no ransom was paid. https://www.cisomag.com/baltimore-hackers-leak-data-on-twitter-after-no-ransom-was-paid/
14 Proofpoint, 2019, Beyond the phishing report. https://www.proofpoint.com/uk/resources/threat-reports/beyond-phish
17 HP Sure Start Gen5 is available on select HP PCs with Intel processors. See product specifications for availability.
18 HP Sure Run Gen2: See product specifications for availability.
19 HP Sure Recover Gen2: See product specifications for availability. Requires an open, wired network connection. Not available on platforms with multiple internal storage drives. You must back up important files, data, photos, videos, etc. before using HP Sure Recover to avoid loss of data. HP Sure Recover (Gen1) does not support platforms with Intel® Optane™.
20 HP Sure Click is available on select HP platforms and supports Microsoft Internet Explorer, Google Chrome™, and Chromium™. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files in read only mode, when Microsoft Office or Adobe Acrobat are installed.
21 HP Sure Sense requires Windows 10. See product specifications for availability.
24 HP Proactive Security available as a separate purchase for Windows 10 devices, regardless of manufacturer. See www.hpdaas.com/requirements for additional system requirements. Requires HP TechPulse, which is included in any HP DaaS or HP DaaS Proactive Management plan. Security Experts available in the Proactive Security Enhanced plan only.
25 Based on HP's internal analysis of isolation security services that offer SaaS and managed services that include on-board and configure, compliance enforcement ad malware threat analytics. Most advanced based on hardware VM isolation enforced protection with individual browser tabs and apps in isolation as of March 2019.
26 HP Service Experts who conduct threat analysis and monitor isolation activity for HP Proactive Security are available for the Enhanced plan only.
27 Based on HP's unique and comprehensive security capabilities at no additional cost and HP Manageability Integration Kit's management of every aspect of a PC including hardware, BIOS and software management using Microsoft System Center Configuration Manager among vendors with >1M unit annual sales as of November 2016 on HP Elite PCs with 7th Gen and higher Intel® Core® Processors, Intel® integrated graphics, and Intel® WLAN.