Considerations for Public Procurement

Cybersecurity Starts at the Device Level

Defining modern endpoint hardware, software, and services security requirements in procurement to identify the minimum baseline and understand the state-of-the-art

Many organizations, including the public sector, do not sufficiently consider endpoint security at the time of procurement. Endpoint security refers to protective measures focused on devices (including hardware and firmware) designed to prevent endpoint devices from being exploited to infiltrate an organisation's networked systems.

For PCs and printers, malicious actors increasingly seek to find ways to gain access to a computer or network (i.e., exploit attack vectors) through low level system vulnerabilities. These actors increasingly use AI to enhance and scale attacks, such as zero-day firmware, malware, and ransomware, as well as exploit vulnerabilities in AI systems. Modern endpoint state-of-the-art — security-by-design — should be evaluated at the time of procurement, with accompanying rationale and guidance to identify how hardware-enforced security capabilities make a difference in an organization's ability to manage its cyber resilience.

Public sector cyber resilience strategy should prioritize analyzing security and resilience capabilities in endpoint device hardware and firmware, including the ability to detect security events (that may even reach the magnitude of a breach) and recover from attacks. A public sector organization should always have a clear understanding and up-to-date articulation of both:

- **Minimal security baseline** requirements for the procurement of endpoint devices
- **Preferred consideration for state-of-the-art** requirements when endpoint security and resilience enhanced security are strategic priorities.

Critical Security Criteria

91% of IT decision makers globally view endpoint security as important as network security, spending more time on endpoint security now than they did two years ago.[1] Firmware attacks have been on the rise for the last decade, typically seeking to exploit embedded software (such as BIOS) which operates close to the hardware in an endpoint device, under the operating system. With the rise of hybrid decentralized work, endpoint challenges will continue to evolve, and organizations will need to adapt

[1] HP_Wolf_Security_Threat_Insights_Report_March_2025.pdf

© 2025 Copyright HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

security strategies for the new environment. Compromised firmware gives attackers the opportunity to hide from typical software-based detection, achieve persistence by avoiding removal, or take control of systems at a deeper level (such as with ransomware and destructive attacks).

For example, hackers can compromise printers to steal sensitive information and data, exploit vulnerabilities, insert malicious code, and gain access to corporate and home networks. In the past year, 68 percent of businesses reported a print-related data loss due to security shortcomings).[2]

Hardware and Firmware

Key device security capabilities should be considered a priority in setting requirements, such as hardware design for BIOS self-healing that can detect threats and automatically recover the firmware from attacks or corruption, without intervention from IT and while maintaining device availability. This allows users to get back to business quickly, keeps productivity high and downtime low. Such criteria should clearly define minimal requirements and also identify desirable state of the art device security capabilities that are recommended for consideration and may lead to future requirements.

Key capabilities to consider:

- Protection of device firmware code and settings integrity
- Detection of device firmware code and settings integrity security event
- Self-healing of device firmware code and settings upon a security event (that can potentially meet the threshold of being classified as a breach)
- Non-bypassable secure firmware update process
- Remote manageable recovery of entire device firmware, operating system, and configuration
- Password-less remote firmware settings management (secured using strong cryptography)
- In-memory firmware intrusion detection, prevention, and secure logging of suspicious events
- Secure erase capability
- Physical intrusion protection, detection, secure logging, and automated mitigation
- Internal and external port-based attack protection, detection, secure logging and remediation
- Protection from malicious third-party firmware (e.g. add-in cards) or boot loader code attempting to modify system behaviour and integrity, with secure logging of attempts
- The data security benefits of local AI EDGE environments versus cloud-based AI environments
- Passwordless access to devices and BIOS using biometry and/or MFA

Software

Attackers are skilled at avoiding intrusion detection algorithms by employing their own counter detection algorithms. Therefore, it is important that the device can scan frequently without calling attention to security sweeps. Enhanced isolation technologies prevent the attacked device from spreading the malicious code to other systems on the network.

Over 70% of security incidents start with a click on a document or browser. Isolation capabilities can drastically reduce the impact of advanced AI-driven phishing attacks and prevent malware and ransomware exploits.

[2] Quocirca Print Security Landscape 2024 Study, 4AA8-4243ENW.pdf

Detecting attacks, being alerted to changes, and recovering quickly is important not only during the boot process; but also during run-time when the device is most vulnerable.

Key capabilities to consider:

- Threat containment to protect host endpoint devices from potentially malicious end-user documents, email attachments and web browsing.
- Hardware-assisted isolation to protect critical business applications from potential malware on host endpoint devices.
- Secure internet browsing and email capabilities
- File-based malware detection and quarantining
- Protection and alerts for credential theft, to prevent users from entering login data into malicious websites
- Hardware enforced in-memory intrusion detection and remediation of suspicious activity

Security Management Solutions or Services

In today's dynamic threat environment, cybersecurity can no longer be an afterthought; it must be a vital component of any major project. Fleet management tools are powerful because they can configure many devices at once, saving administrators from contacting each device separately to apply configuration such as passwords and other credentials. Policies for security features such as device passwords, community names, ports, services, protocols, cipher suites, embedded web servers, and other credentials are used to secure the device and prevent unauthorized access. In the hybrid era, security remote management of endpoints devices is a pre-requisite, as well telemetry to keep them secure for working in less secure spaces. Devices are increasingly stolen and the ability for admins to find, lock and erase devices is essential to protect sensitive data and ensure compliance, such as GDPR.

Key capabilities to consider:

- Fleet asset- and configuration management monitoring
- Vulnerability management to ensure the endpoint is running the latest firmware and software
- Endpoint threat data reporting and analysis for SIEM and SoC integration
- Security threat and event monitoring to identify and timely remediate vulnerabilities and anomalous behavior on endpoints
- Identity and access management, using MFA, to the device, BIOS, OS, network, applications and data
- Remote capability to securely locate, wipe, or lock (stolen) devices, even when powered off
- Security (3rd party) risk assessment and ongoing management (helps to establish baselines to drive continuous improvement in cyber security posture (cyber hygiene))
- Security policy compliance and certificate management
- Assessment of endpoint security in the light of regulatory standards such as NIS2 / DORA / CRA or other regulatory security regulatory compliance standards

Supply chain security

Manufacturers must establish a clear process to manage supply chain risks. Manufacturers must ensure no malicious hardware or software is introduced into products during the sourcing and manufacturing processes by identifying and utilizing trusted suppliers, service providers, and components. Suppliers and service providers should be contractually obligated to develop and implement appropriate measures to meet the goals and objectives of the supply chain risk management program, with regular monitoring from the manufacturer through audits and technical inspections. An initial assessment should occur before engaging and hiring third parties to ensure security throughout the life of the device. Supply chain security controls should be in place to validate the origin of devices and components during transport and throughout their lifecycle.

Key capabilities to consider:

- Awareness of supply chain providers and purchase only from trusted sources to ensure the endpoint devices are not modified or tampered with (this mitigates against potential attacks). This should include evaluating supply chain security and governance processes, as well as understanding parameters that may influence a vendor's practices, such as jurisdiction or underlying company ownership structure.
- Supply chain risk management (SCRM) capability follows industry standards and best practices (i.e. NIST SP 800-161, NIS2)
- Supply chain and information security certifications (ISO/IEC 20243 (O-TTPS), ISO/IEC 27001), SOC 2 (Type2))
- Manufacturer-provided artifacts, such as Platform Certificates, should be considered to implement verification of device provenance and configuration integrity (see NIST 1800-34 practice guide)
- Third-party risk management to ensure security of hardware components, software, access to confidential company data or to a secured company network (ensure this starts before engaging and hiring the third parties).
- Risk assessment processes – security audits and questionnaires, onsite physical assessments, vulnerability testing, penetration testing, and architecture discussions (this should include initial cyber security risk assessments to establish solid cyber security baselines to help use to drive improvement in the cyber security posture).
- Technical solutions to prevent and detect espionage and infiltration techniques
- Locking devices and its firmware during transport, preventing physical hardware attacks and unauthorized modifications

Quantum-Resistant Cryptography

While the development of quantum computing presents key opportunities in critical industries, it also brings considerable risk. Security researchers have discovered that quantum computers could easily break today's most commonly used encryption algorithms. While quantum computers aren't expected to be operational until at least 2030, their impacts are immediate - malicious actors are obtaining sensitive data now with the hope of future access once these computers become available.

Multiple governments are proactively addressing this threat. In August 2024, NIST finalized a principal set of quantum-resistant encryption algorithms developed in concert with industry. A 2025 executive order issued by the Trump administration directed government agencies to identify, inventory, and prioritize agency cryptographic systems for migration to quantum-resistant algorithms. Meanwhile the European Commission developed an April 2024 policy paper detailing an ongoing project to fund research on PQC and outlining a plan to create EU-wide standards for post-quantum cryptographic algorithms and support widescale testing.

Key capabilities to consider:

- Encryption algorithms that have been deprecated by NIST
- Hardware that uses PQC to protect firmware integrity

In the modern cyber threat landscape, it has become critical to be able to define clear security requirements when procuring endpoint devices, software or services, whether to identify a very minimum baseline, or to ensure organizations can benefit from today's available state-of-the-art and be prepared for the threats of tomorrow. HP is committed to working with our customers to provide our expert input and help identify appropriate requirements.

For more information, contact Linda van Renssen or visit https://www.hp.com/us-en/security/endpoint-security-solutions.html