FORESCOUT

KNOW YOUR SECURITY RISK

How Secure Is Your Building Automation System (BAS)?

The Forescout Building Automation Risk Report explores the common systems that make organizations vulnerable to cyberattacks and how these systems could be exploited.

By 2026, there will be over

56 million

new BAS devices. [1]

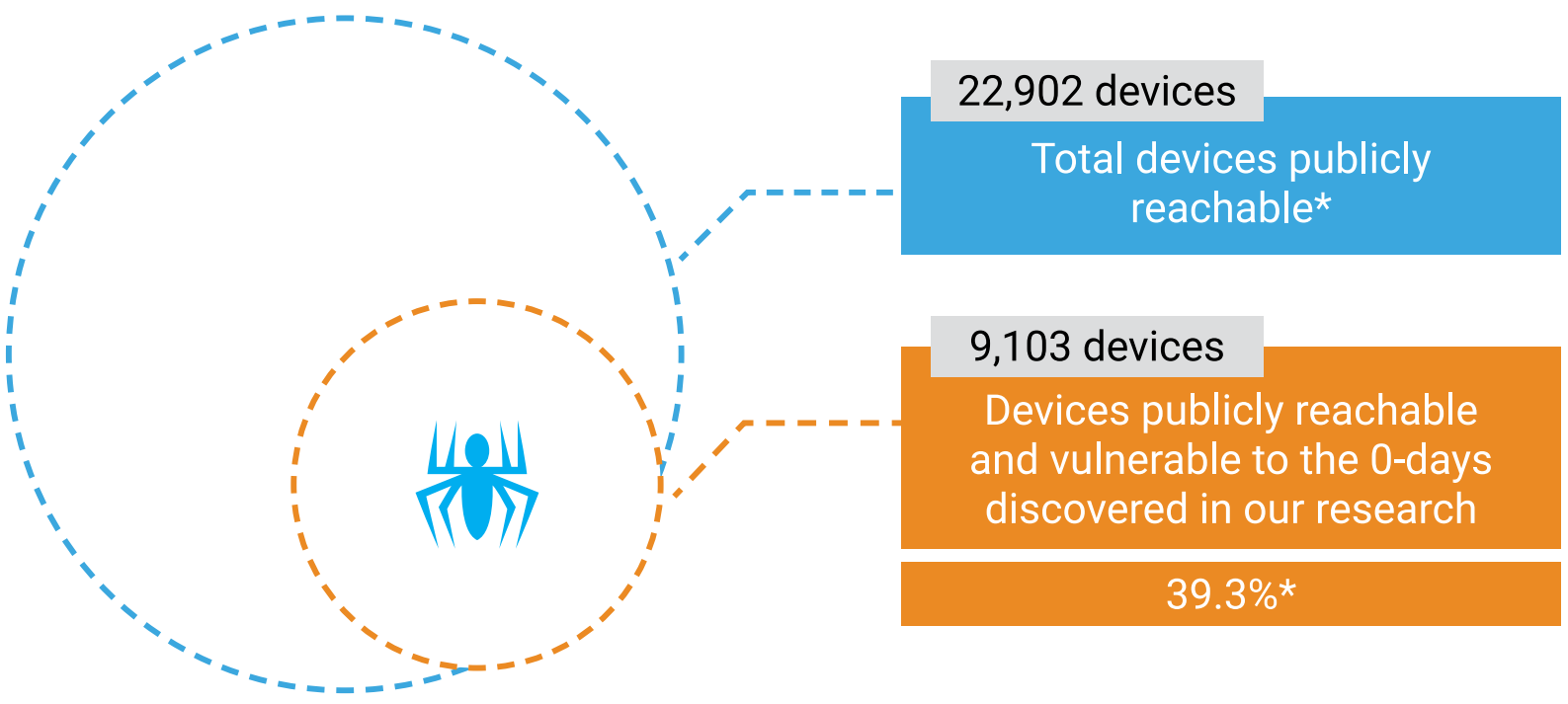
The number of identified vulnerabilities in BAS has increased over

500%

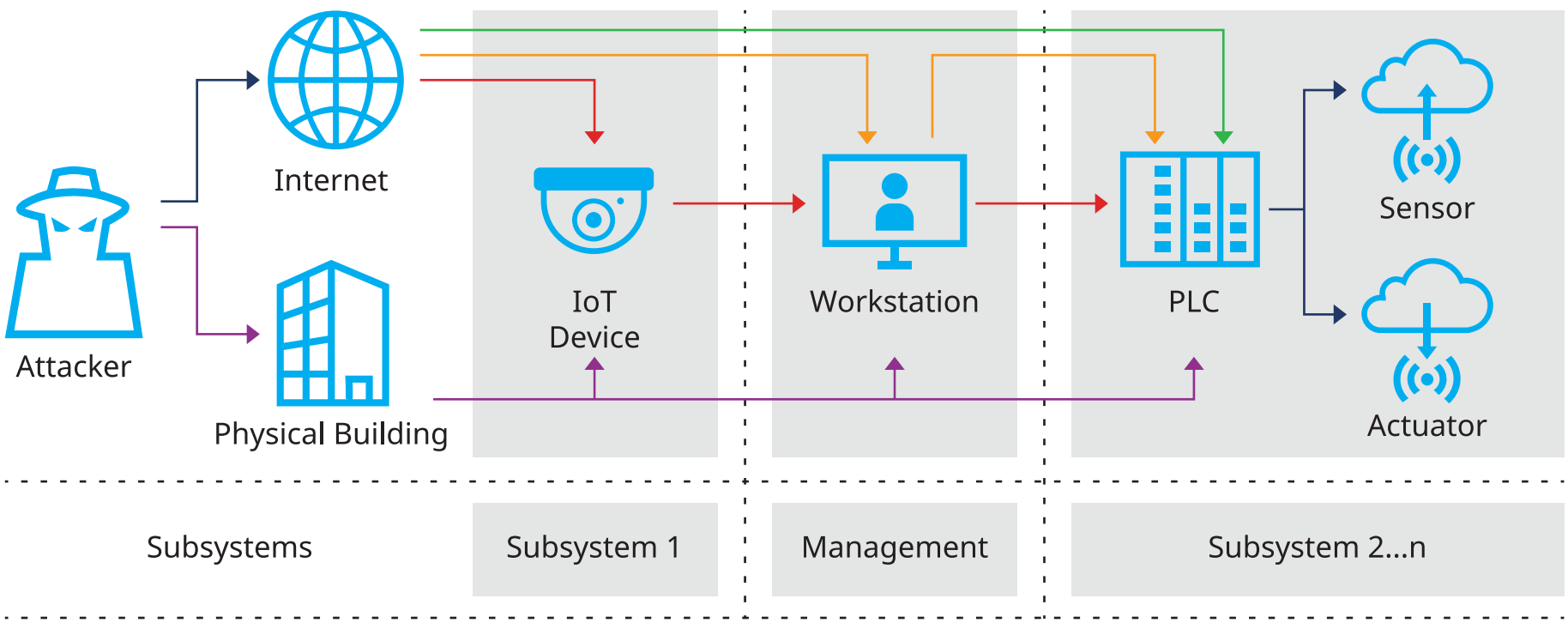
in the past three years. [2]

39.3% of publicly reachable BAS devices are vulnerable [3]

Vulnerable devices include: HVAC PLCs, Access Control PLCs, Protocol Gateways



Potential Attack Paths



1. Publicly reachable PLCs: Using this path, the malware can enter directly from the Internet and exploit the programmable logic controllers (PLCs) controlling the sensors and actuators at the field level, so there is no need to perform any lateral movement from other devices.

2. Publicly reachable workstations: Using this path, the malware can enter a workstation from the Internet at the management level and move laterally to the PLCs.

3. Publicly reachable IoT devices: Using this path, the malware can enter an IoT device, such as an IP camera or a WiFi router, from the Internet and use that entry point to gain access to the internal network, usually moving to the management level first and then to other subsystems.

4. Air gapped network: Using this path, the attacker must have physical access to the building network (which could be accomplished via the HVAC system) and move laterally to reach the PLCs.

Conclusion

Building automation systems (BAS) may be as critical as industrial control systems (ICS) in terms of safety and security, yet receive much less attention from the security community.

Enhancing BAS cybersecurity programs with device visibility and network monitoring can give organizations a thorough understanding of the environment and its connections, making it easier to design effective security architectures, identify attack vectors, and locate blind spots.

Download the full research report to learn more about the current state of smart building cybersecurity

DOWNLOAD

[1] ABI Research, 2019, BAS Wireless Field Equipment Shipments
[2] https://www.cvedetails.com/vulnerability-list.php?vendor_id=109&product_id=&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=1&cvssscoremax=5.99&year=0&month=0&cweid=0&order=1&trc=0&sha=5b596304073bf31b889d18d4577d2d0a4b6f941f
[3] Forescout, The Current State of Smart Building Cybersecurity, 2019: https://www.forescout.com/securing-building-automation-systems-bas/

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com