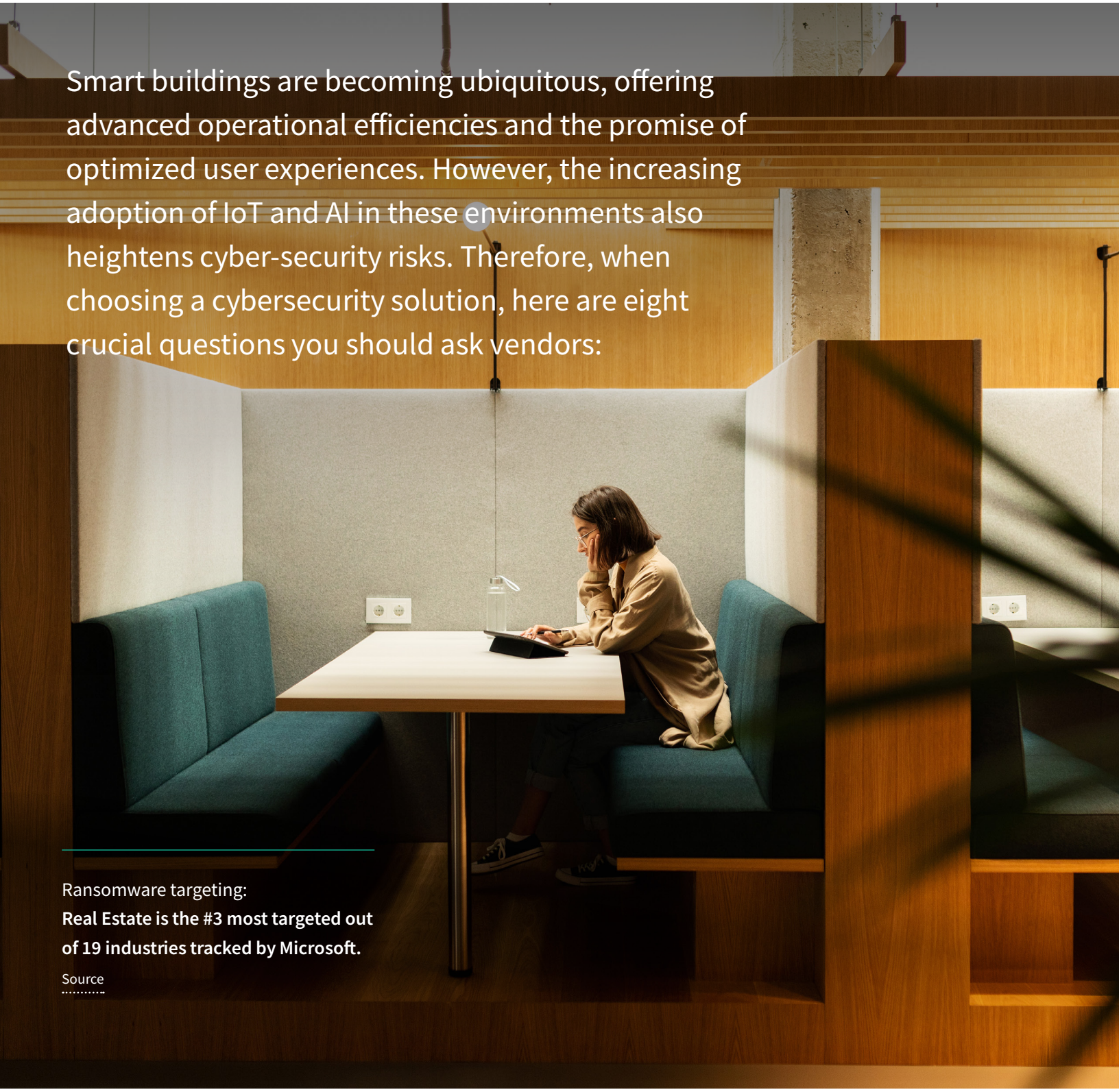
neeve

8 Questions You Should Be Asking Your Cybersecurity Vendors Now



Smart buildings are becoming ubiquitous, offering advanced operational efficiencies and the promise of optimized user experiences. However, the increasing adoption of IoT and AI in these environments also heightens cyber-security risks. Therefore, when choosing a cybersecurity solution, here are eight crucial questions you should ask vendors:

Ransomware targeting:
Real Estate is the #3 most targeted out of 19 industries tracked by Microsoft.

Source

1 Do You Support SASE and Zero-Trust Architecture in OT Environments?

A blended approach that incorporates Secure Access Service Edge (SASE) and Zero-Trust Architecture is no longer optional; it's a necessity.

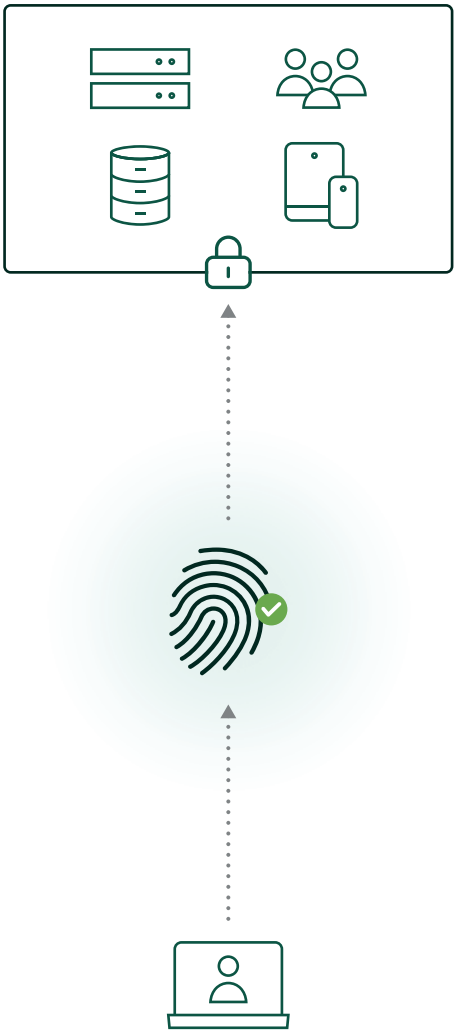
SASE merges network and security services into a single cloud-based offering, providing the scalability and flexibility essential for dynamic OT environments.

Zero-Trust Architecture as part of a SASE implementation adheres to the principle of '**never trust, always verify.**'

It ensures that every request is authenticated with multi-factor authentication, encrypted, and logged, that all access is role-based and granular, that firewalls are default-deny, and more.

All of that is to greatly reduce the attack surface.

You want to ensure your vendors are not merely patching security gaps but rather implementing a comprehensive, integrated, best-practice approach.



In 2022, The ratio of malware explicitly targeting the operational technology (OT) industry has increased by 27.5%. Exploitation of vulnerabilities increased by 55% compared to 2021.

Source

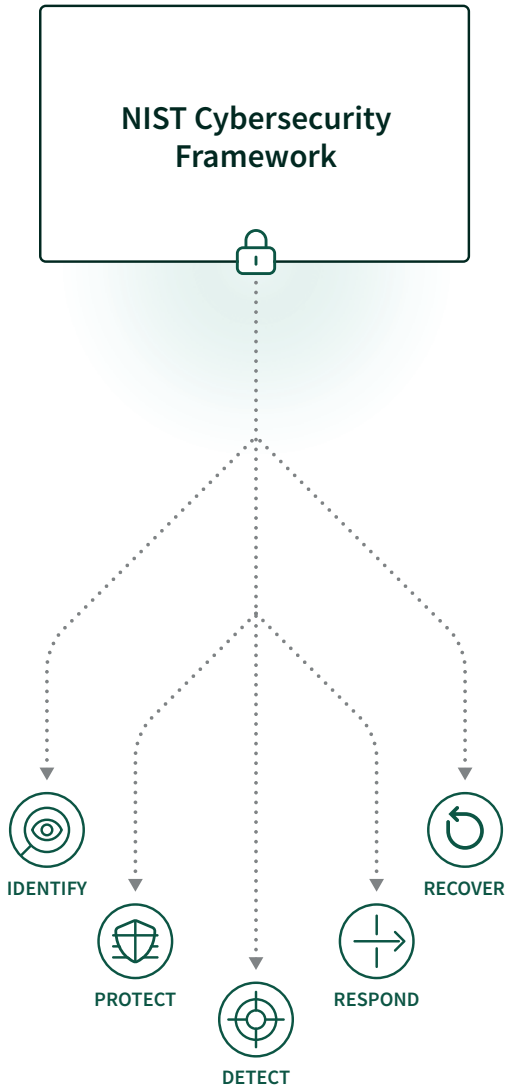
2 How Complete is Your Solution in terms of the NIST Cybersecurity Framework?

While individual cybersecurity solutions may excel in certain areas, the ultimate goal should be to cover every aspect of the NIST Cybersecurity Framework from '**Identify**' to '**Recover.**'

Whether it's asset management, data security, or threat detection, a robust cybersecurity solution should be comprehensive enough to address all dimensions.

This includes redundancy and fail over of critical elements both on prem and in the cloud.

No framework is bullet proof. But, if your vendors don't cover the full spectrum, you may need to cobble together other solutions to plug gaps, creating a complex and possibly weaker security posture.



The average cost of a data breach in 2022 was $4.35m, up 12.7%. And $9.4m in the US.

Source

3

How Does Your Solution Ensure End-to-End Encryption?

Securing communications within OT environments that must always be available and responsive to real-time events often involves unique challenges.

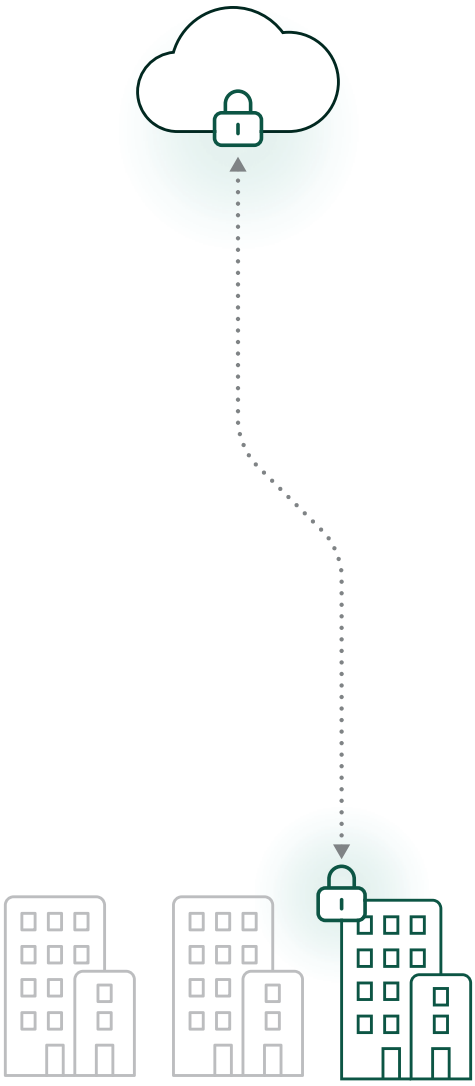
A '**book-ended**' architecture that executes encryption and decryption at the endpoints is one that ensures data **integrity and confidentiality** across the network.

This approach minimizes the risk of Man-in-the-Middle attacks, ensuring that even if data is intercepted, it remains unintelligible.

In the context of a smart building, where numerous sensors and actuators are constantly exchanging data with the cloud, this end-to-end protection is critical.

In addition, platforms should be authenticated with a Trusted Platform Module (TPM).

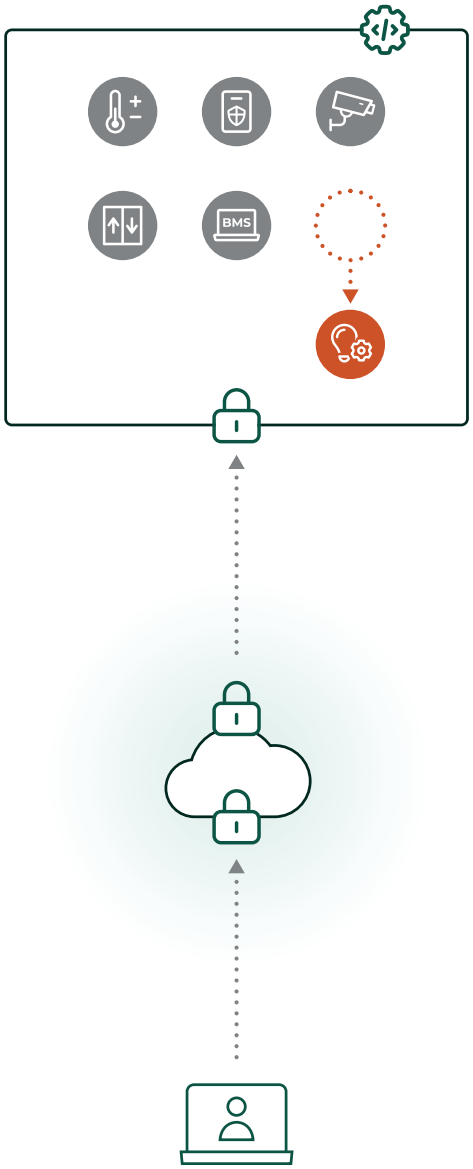
You want to ensure your vendors have architected security to protect every connection and operation.



Basic security hygiene still protects against 99% of attacks. Multi-factor authentication, Zero Trust, Threat Detection, Up-to-Date software, and Data encryption/protection.

Source

4 Can Your System Isolate Operational Subsystems in Software?



Physical isolation of networks in OT environments is an outdated approach that hampers efficiency.

Often it results from uncoordinated system implementations over the years.

Modern cybersecurity solutions should be capable of isolating and micro-segmenting operational subsystems in software, enabling agile policy management and simplified data integration across various systems.

This is more efficient but also reduces the total cost of ownership (TCO) for your cybersecurity infrastructure.

You want to make sure your vendors support a physically converged network with traffic isolation in software that you can verify and manage.

"93% of our ransomware incident response engagements revealed insufficient controls on privilege access and lateral movement."

— Microsoft Customer Security

Source

5

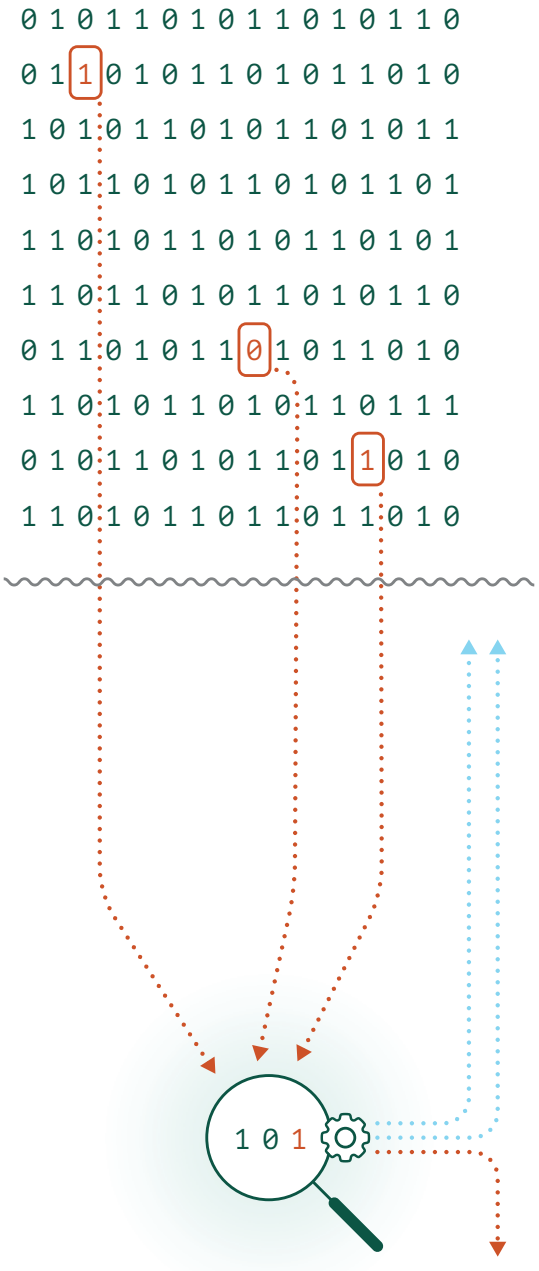
How Does Your Solution Handle Continuous Threat Detection in OT Environments?

OT environments, like smart buildings, are active 24/7, generating a constant stream of real-time data.

A comprehensive cybersecurity solution should include Continuous Threat Detection (CTD) capabilities, continuously analyzing this data for any abnormal behavior or patterns that may signify a security event.

CTD should be able to identify not just known threats but also zero-day vulnerabilities, thereby ensuring a robust and forward-looking security posture.

You want to make sure your vendors offer continuous, real-time monitoring and analytics.



57% of all IoT devices are vulnerable to attacks of medium- or high-severity. 41% of attacks are exploits of IoT device vulnerabilities, with the largest component of this category originating from scans through network-connected devices.

Source

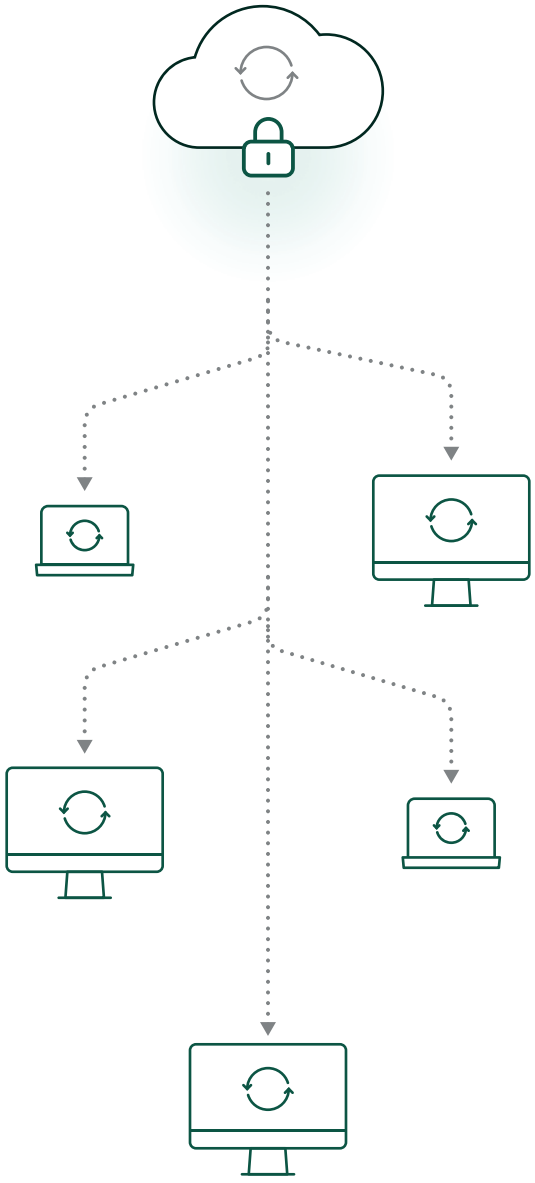
6

What's Your Approach to System Software Updates?

Updates are essential for security. Attackers prey on known vulnerabilities in organizations that do not quickly and consistently update their software with fixes to those problems.

Software releases from organizations that are not thorough and careful about secure software practices can inadvertently introduce new vulnerabilities.

You want vendors with a well-defined strategy for developing, testing, and safely rolling out updates without compromising operational integrity, all while adhering to the OT environment's unique requirements for local processing.

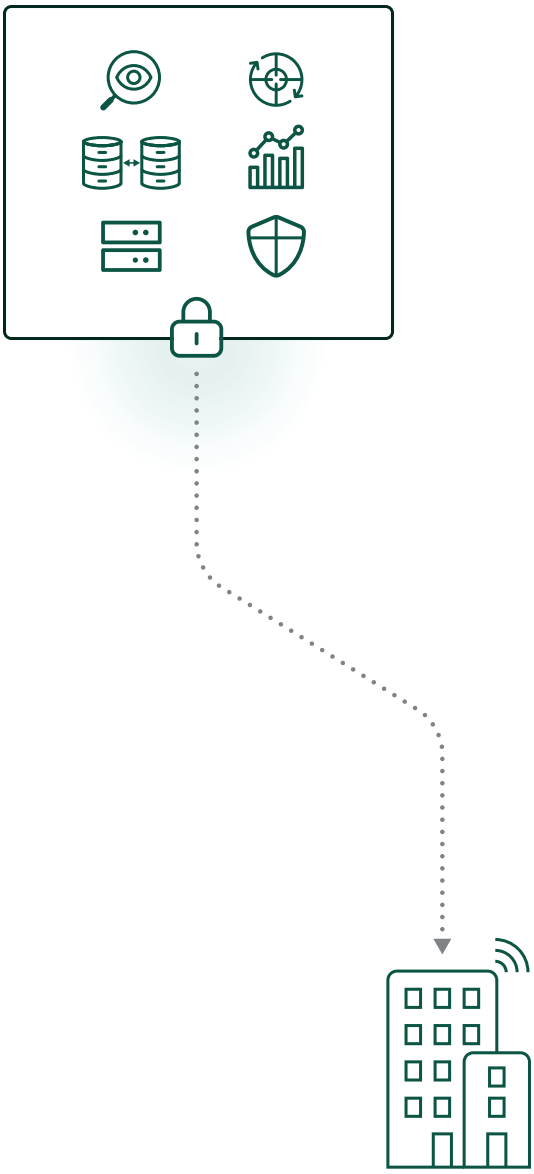


More than 60 percent of OT devices are on firmware versions that expose the devices to eight or more exploitable common vulnerabilities and exposures (CVEs), even when some patches have been available for over five years.

25% of OT devices on customer networks use unsupported operating systems.

Source

7 How Does Your Solution Handle Edge Computing Security?



As smart buildings increasingly rely on edge computing for innovative applications including AI, real-time analytics, and decision-making, the edge application host becomes a new frontier for potential attacks.

You want vendors that incorporate advanced features like local orchestration of edge applications, failover and clustering, and hardened OS, storage, and boot procedures tailored to OT requirements.

80-90% of all Ransomware compromises originate from unmanaged devices. (Author's note: think stand-alone servers and PCs.)

Source

8 What Are Your Compliance Credentials?

OT organizations are typically smaller and rely heavily on vendors compared to IT.

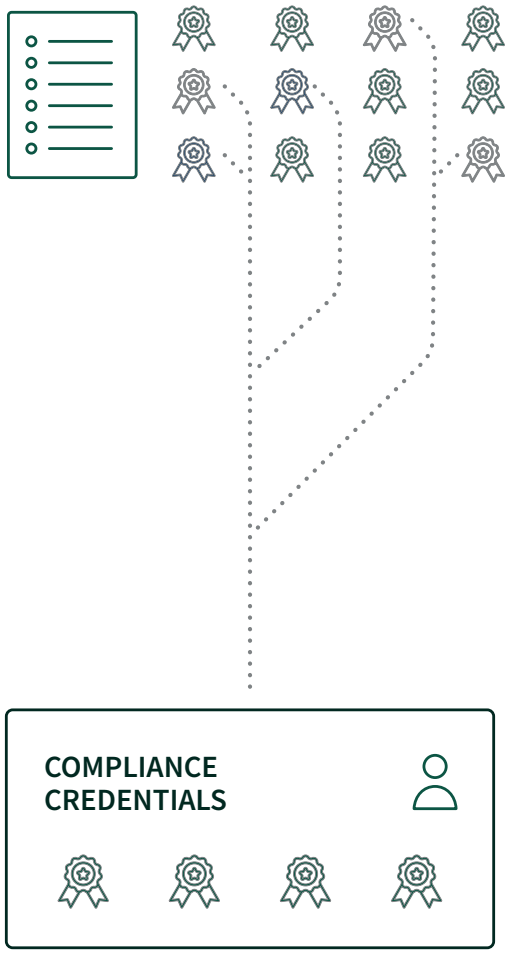
The compliance frameworks for OT have progressed significantly over the last several years and for good reasons.

Compliance ensures that you and your vendors are in fact meeting industry standards and best practices.

For example, many vendors will claim SOC2 compliant infrastructure because they use a compliant cloud provider like AWS.

But better still is if they follow SOC2 practices internally to safeguard access, information, assets, software, and privacy that you rely on.

You want a vendor with a robust set of credentials so that you know they are better equipped to navigate the complex landscape of OT cybersecurity.



Over the last year, 70% of organizations encountering human-operated ransomware had fewer than 500 employees.

Source

neeve

By asking these eight questions, you can assess a vendor's expertise and suitability for safeguarding your smart building's OT environment. Prioritizing these issues will help guide you toward vendors with comprehensive security, aligned with your drive toward efficient, data-driven operations and innovation in your buildings.

To learn more visit us at neeve.ai