Keep the Operation Running

OT Patch Management Playbook:

Defend Without Disruption

Introduction

Operational Technology (OT) environments are the backbone of critical infrastructure, encompassing industries such as manufacturing, utilities, energy, as well as food and beverage. OT encompasses hardware and software designed to monitor and control physical equipment, processes, and events within organizations. These systems are typically built for longevity, often operating for over a decade.

However, these environments face a significant challenge: patch management. Unlike traditional IT systems, OT systems prioritize continuous operations, making the application of security patches a complex and often delayed process that leaves organizations vulnerable to cyber threats. And that's if a patch is even available, given OT's reliance on legacy devices and unsupported operating systems for which patches are no longer made.

With data from TXOne Networks' 2024 Annual OT/ICS Cybersecurity Report, which surveyed 150 C-level OT cybersecurity decision-makers across the globe, this eBook serves as a guide to navigating the complexities of OT patch management and achieving a resilient cybersecurity framework. Inside, you'll find practical guidance on:

- **Implementing phased and tested patch deployments to avoid business disruption**
- **Leveraging dedicated testing environments to reduce risk before changes go live**
- **Applying compensating controls, such as micro-segmentation and real-time monitoring, to defend systems during patch delays**
- **Utilizing virtual patching and dynamic prioritization models to address critical vulnerabilities when patching isn't immediately possible.**
- **Working with OT-specific solutions designed with expert knowledge of that environment**

Whatever challenges stand in the way, effective OT security is more doable than you think. By adopting a proactive and adaptive patch management strategy, organizations can effectively safeguard their OT environments against evolving cyber threats while ensuring business continuity.

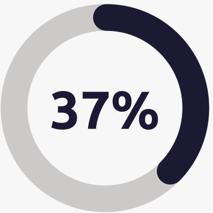
Challenges to Patching OT Environments

OT systems are typically built for durability, often operating for over a decade. Many OT assets still rely on outdated platforms, such as Windows XP, released more than 20 years ago — and the risk of patch incompatibility discourages organizations from implementing updates. As a result, infrequent patching leaves systems exposed to known vulnerabilities for extended periods.

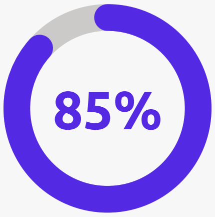
A staggering 85% of organizations do not conduct regular patching in their OT environments due to downtime concerns, which leaves them more exposed to known vulnerabilities.

This neglect places critical infrastructure at significant risk, as attackers could exploit unpatched vulnerabilities to disrupt operations essential to daily life. It also highlights the need for critical defense during patch delays and a dynamic patch prioritization model to optimize the use of limited resources and time.

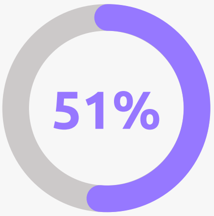
Patching Challenges and Interim Defenses



of organizations have experienced OT cyber incidents related to software vulnerability exploitation.



of organizations in OT environments do not patch frequently due to concerns about downtime.

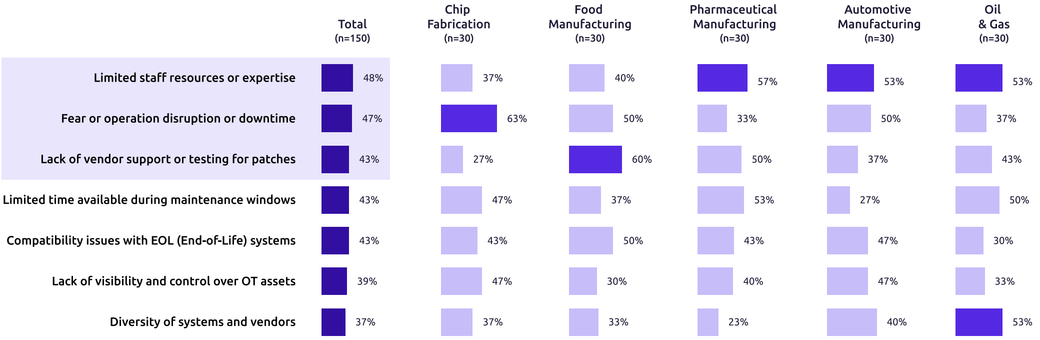


of organizations opt for increased monitoring when patches are unavailable, but this is not an adequate solution.

In a survey of 150 C-suite executives, several critical challenges to patching in OT environments were identified, with the top three being:

- **Limited personnel or expertise (48%)**
- **Concerns about operational disruptions or downtime (47%)**
- **Lack of vendor support or patch testing (43%)**

To overcome these obstacles, organizations must adopt more flexible and collaborative patch management strategies as well as leverage automation tools and innovative technologies to balance cybersecurity with operational efficiency. Addressing compatibility issues in End-of-Life (EOL) systems and the constraints of maintenance windows require long-term optimization planning.



QC3: What are the main challenges your organization faces when applying patches to OT environments? (Rank Top 3)

Approaches to Secure OT Patch Management

Why are factory managers hesitant to modernize these assets? It's not due to ignorance of cybersecurity risks — in fact, managers are acutely aware of them. Instead, the challenge lies in balancing cybersecurity with other factors, such as continuous operations. Cost is another issue, from the price of the software upgrade itself to the cost of replacing deprecated assets that should really be retired.

Patch management strategies in OT environments must be tailored to industry-specific needs. The importance of these strategies is underscored by the 2024 incident involving SaaS-based cybersecurity company CrowdStrike. The incident was not even an attack — CrowdStrike simply released a faulty update — yet it still affected nearly eight million Windows devices globally and disrupted multiple industries.

This highlights the importance of rigorous testing to identify potential issues, phased deployment to minimize impact, and rollback mechanisms to quickly restore systems. Integrating dynamic tools and virtualization can materially improve security and operational continuity.

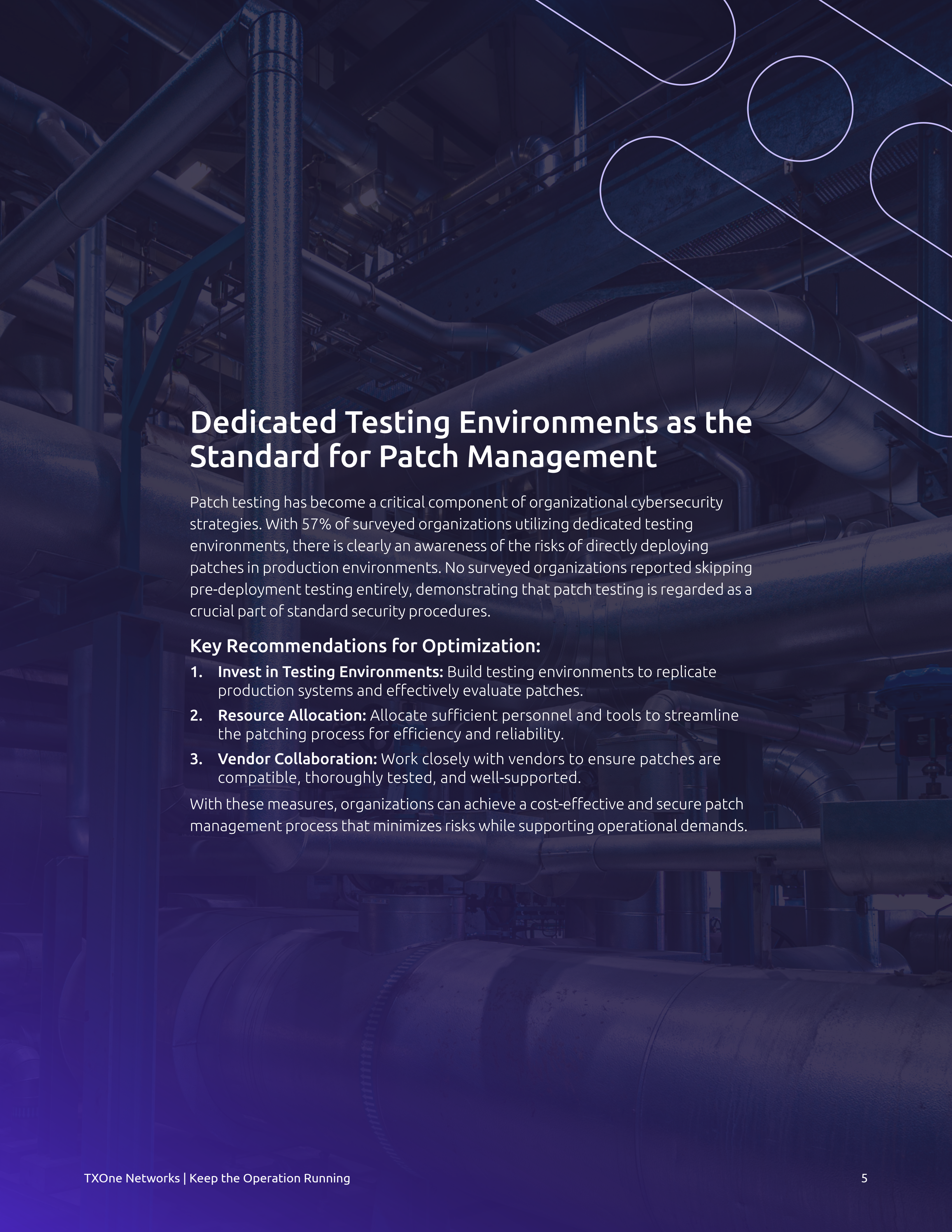
Flexible patch management strategies equip organizations with the adaptability necessary to address diverse challenges while maintaining robust OT cybersecurity.

Key approaches include:

Scheduled Downtime and Maintenance Windows: Applying patches during planned downtime or maintenance windows. While effective in avoiding operational disruptions, this approach requires meticulous planning and can be challenging for industries with high-efficiency demands.

Controlled Environment Testing: Pre-deployment patch testing in controlled environments minimizes risks. This step is crucial, as unvalidated changes by third parties to internal endpoints can introduce vulnerabilities or cause disruptions.

Phased Rollout Deployment: Rolling out patches incrementally reduces the impact on the entire system. This strategy combines dynamic technologies with virtualized testing environments, enhancing both efficiency and security in patch deployment.



Dedicated Testing Environments as the Standard for Patch Management

Patch testing has become a critical component of organizational cybersecurity strategies. With 57% of surveyed organizations utilizing dedicated testing environments, there is clearly an awareness of the risks of directly deploying patches in production environments. No surveyed organizations reported skipping pre-deployment testing entirely, demonstrating that patch testing is regarded as a crucial part of standard security procedures.

Key Recommendations for Optimization:

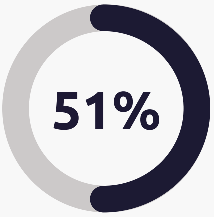
1. **Invest in Testing Environments:** Build testing environments to replicate production systems and effectively evaluate patches.
2. **Resource Allocation:** Allocate sufficient personnel and tools to streamline the patching process for efficiency and reliability.
3. **Vendor Collaboration:** Work closely with vendors to ensure patches are compatible, thoroughly tested, and well-supported.

With these measures, organizations can achieve a cost-effective and secure patch management process that minimizes risks while supporting operational demands.

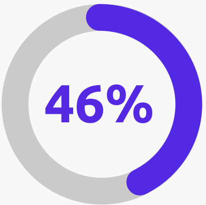
Critical Defense Strategies During Patch Delays

Strategies like relying solely on monitoring and compensating controls prolong exposure to vulnerabilities, increasing organizational risk. Delaying patches is particularly dangerous, as attackers often exploit vulnerabilities before updates are released.

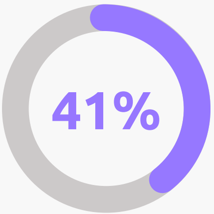
To address these challenges, organizations should adopt multi-layered, industry-specific measures, including compensating controls, virtual patching, and external expert support, to effectively manage security risks during patch delays.



of organizations use compensating controls (e.g, network segmentation, system hardening) to mitigate the impact of vulnerabilities.



of organizations rely on enhanced monitoring and intrusion detection when patches are unavailable, a temporary solution that fails to resolve the underlying vulnerability.



of organizations delay patch updates until vendor support is available, which increases the window of vulnerability to potential attacks.

Integrate Monitoring with Compensating Controls

Monitoring alone is insufficient; its value is maximized when combined with compensating controls. One effective starting point is network segmentation, adopted by 46% of respondents, to isolate high-risk devices from critical infrastructure and reduce the attack surface.

Real-Time Monitoring: Helps security teams quickly identify threats through alerts for suspicious behavior.

Micro-Segmentation: Takes traditional network segmentation further by implementing fine-grained control, limiting attackers' lateral movement within systems.

Human Error Mitigation: Even with advanced technologies, human negligence remains a common entry point for attackers, emphasizing the need for comprehensive training.

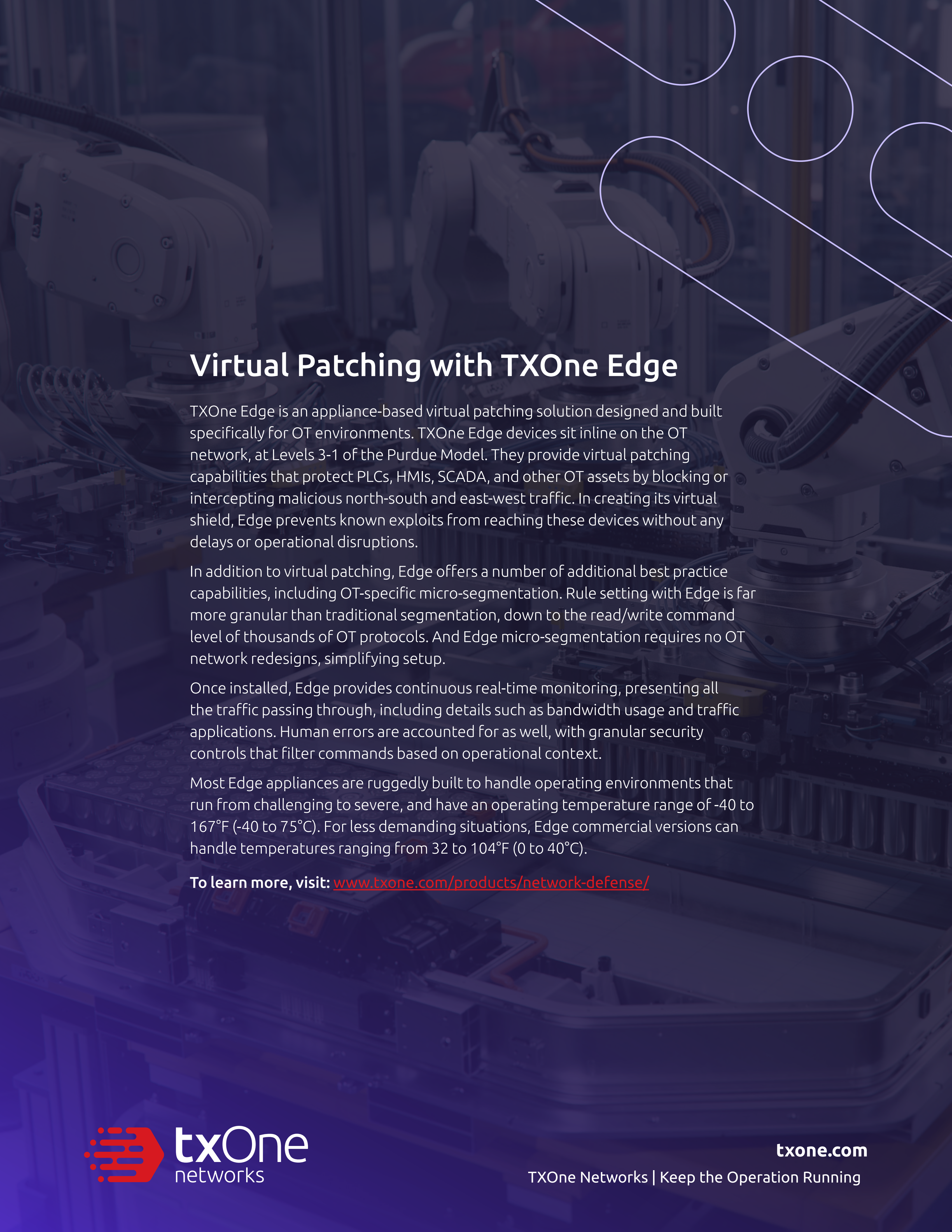
Virtual Patching

When immediate patching is not feasible, virtual patching provides an essential stop-gap defense. This technique establishes a temporary security barrier for vulnerable applications and devices without altering system code, preventing attackers from exploiting known vulnerabilities. Virtual patching ensures that organizations maintain a defense layer while working to resolve underlying vulnerabilities, minimizing risks associated with unpatched systems.

Dynamic Patch Prioritization Model

A dynamic, industry-specific prioritization model enables organizations to optimize their patch management strategies by effectively allocating resources, collaborating with vendors, and applying risk-driven methodologies.

By taking a multi-factor approach to patch prioritization, organizations can balance factors such as system criticality to operations, patch availability, and risk exposure.



Virtual Patching with TXOne Edge

TXOne Edge is an appliance-based virtual patching solution designed and built specifically for OT environments. TXOne Edge devices sit inline on the OT network, at Levels 3-1 of the Purdue Model. They provide virtual patching capabilities that protect PLCs, HMIs, SCADA, and other OT assets by blocking or intercepting malicious north-south and east-west traffic. In creating its virtual shield, Edge prevents known exploits from reaching these devices without any delays or operational disruptions.

In addition to virtual patching, Edge offers a number of additional best practice capabilities, including OT-specific micro-segmentation. Rule setting with Edge is far more granular than traditional segmentation, down to the read/write command level of thousands of OT protocols. And Edge micro-segmentation requires no OT network redesigns, simplifying setup.

Once installed, Edge provides continuous real-time monitoring, presenting all the traffic passing through, including details such as bandwidth usage and traffic applications. Human errors are accounted for as well, with granular security controls that filter commands based on operational context.

Most Edge appliances are ruggedly built to handle operating environments that run from challenging to severe, and have an operating temperature range of -40 to 167°F (-40 to 75°C). For less demanding situations, Edge commercial versions can handle temperatures ranging from 32 to 104°F (0 to 40°C).

To learn more, visit: www.txone.com/products/network-defense/

txOne networks

txone.com

TXOne Networks | Keep the Operation Running