



Improving cybersecurity practices within utilities

How to close the gap between your OT and IT systems

Gain complete visibility of your network operations and prioritize vulnerability remediation

In this era of volatility and change, of rising prices and global unrest – energy companies must be ready to respond.

Regulatory compliance and risk mitigation are ever more challenging. Attacks on the infrastructure we depend on for energy, water, and food are on the rise. Equally concerning, cybercrime is proving to be increasingly costly. At the time of writing, the cost of a data breach averaged USD 4.35 million in 2022, 2.6% increase from previous year.¹

As every security professional will acknowledge, you cannot protect what you cannot see. And you cannot prioritize without complete visibility.

Broadly, the utilities industry must protect its critical infrastructure and its supply chains. It must secure sensor data, notably the Internet of Things (IoT). It must ensure that the information it collects and processes remains protected with the highest observed privacy standards.

All this is happening as organizations seek to bring analog and digital systems together for the first time. Closing

the air gap between operational technology (OT) and information technology (IT) maximizes resource utilization and expands access to actionable insights, increasing the threat vector.

The utilities sector faces five era-defining trends: volatility, decarbonization, decentralization and convergence, digitalization and regulatory complexity. In this paper, we explore all five trends and examine the compliance and risk implications. With this insight, organizations can improve security visibility, collaboration, and defense strategies.

Today's business leaders need to see around corners to get ahead of their threats. At Skybox, we don't just serve up data and information; we provide the intelligence that allows you to make informed decisions. Nowhere is that more important than in the volatile world of energy.

All this is happening as organizations seek to bring analog and digital systems together for the first time.

Risk factors facing utilities

- + Specialized devices with long lifespans
- + Previously air-gapped systems now connected and accessible
- + Software obsolescence and difficulty in patching devices
- + Fragmented visibility of IT and OT assets and vulnerabilities
- + Overarching Health, Safety, & Environment (HSE) concerns
- + Compliance with increasingly stringent regulatory standards
- + Cybersecurity talent gap

¹ Cost of a Data Breach Report 2022, IBM Security, July 2022



Five trends shaping cybersecurity practices in utilities

1. Volatility

We live in uncertain times. Rising prices, aging fleets, geopolitical forces, forced consolidation of energy suppliers, changing consumer behaviors, sharp fluctuations in supply and demand (exacerbated by the pandemic), supply chain fragility, and the ongoing threat of cyber-attacks on critical national infrastructure all contribute to a sense of unpredictability.

The final cause of volatility is most closely aligned to the security and technology leader's day job: the increased risk of cyber-attacks on critical infrastructure. These are not theoretical threats. The most notable ransomware attack of recent times led to the closure of the Colonial Pipeline in the United States. To understand the impact of that April 2021 attack, consider that the pipeline usually supplies 45% of the East Coast's fuel. This includes gasoline, diesel, home heating oil, jet fuel, and military supplies.² In Europe, meanwhile, one utility operator faced an €11 million ransomware demand after falling victim to the Ragnar Locker ransomware attack in 2020.³

At the same time, OT assets are increasingly connected to networks, exposing critical infrastructure and other vital systems to potentially devastating breaches. New vulnerabilities in operational technology (OT) rose by 88% from 2020 to 2021.⁴

87%

of utilities organizations suffered operational technology (OT) breaches in prior 36 months⁵

² Colonial Pipeline attack: Everything you need to know, ZDnet, May 2021

³ EDP faces \$11m ransomware demand after 'potentially catastrophic cyberattack', Recharge, April 2020

⁴ Vulnerability and threat trends report 2022, Skybox Security, April 2022

⁵ Cybersecurity risk significantly underestimated by operational technology organizations, Skybox Security, November 2021

2. Decarbonization

If the world reaches net-zero carbon emissions by mid-century, no industry sector will play a more significant role than energy. Although travel direction is clear, decarbonization requires a careful balance between clean technologies and ongoing affordability. It also requires high levels of threat alert.

Unfortunately, cybercriminals have a track record of targeting all four stages of the electricity value chain as the design of legacy infrastructure was not built with security in mind.

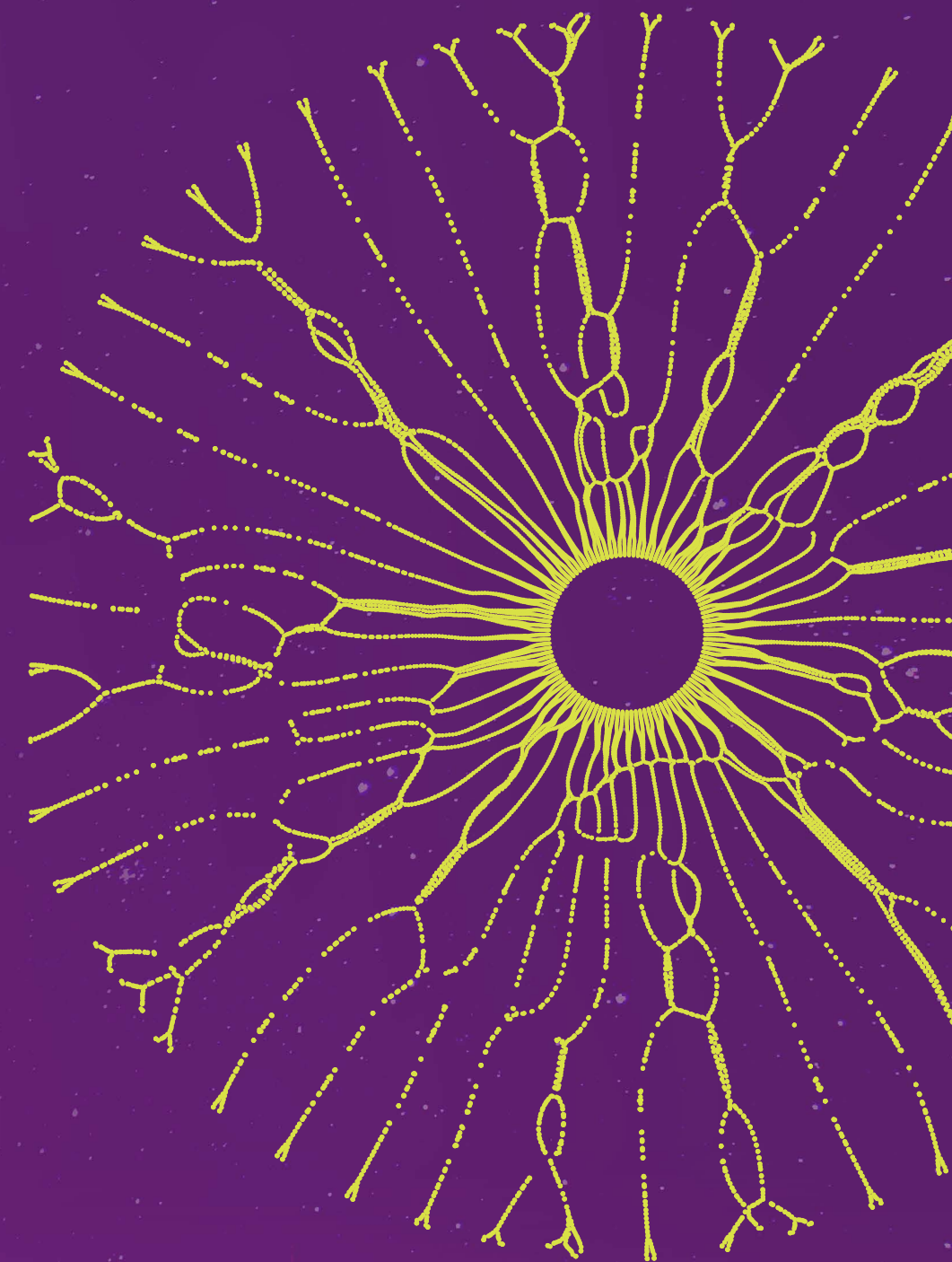
Diverse network of electricity generation will also expand utility companies' exposure to cyber-attacks. Securely managing the changes in their business shape will require an understanding of their attack surface and visibility into interconnected mesh of systems.

3. Decentralization and convergence

Energy production is becoming more dispersed when companies from across the power sector and beyond congregate around common provisions and services. As a result, there is more significant competition for incumbent players and the emergence of novel business models, many services based.

As consumers become energy producers, and as solar, wind, and tidal become mainstays of the grid, distribution will dramatically change. In this scenario, the decentralization of electricity generation will likely become the chief role of energy companies in the coming decades. Distributed energy resource (DER) will become an arena where energy utilities may choose to play, providing the aggregation platforms that make sense of devolved production. However, it will require digital understanding and greater awareness of security threats.

Distributed assets offer optimal access points for targeted attacks and the reconnaissance of wider infrastructure. At the same time, operators lack the visibility to effectively identify harmful changes at an early stage. This is especially true for remotely controlled assets such as substations, switchgear, renewable energy plants, and affiliated municipal utilities.



4. Digitalization

The move to digitalization is motivated by the ability to accelerate the other imperatives, notably decarbonization and decentralization. Digital technology empowers energy users to be more flexible – and sustainable – in their energy use. In addition, it empowers energy providers to balance supply and demand while opening up new market opportunities, especially on the service side.

Today's organizations are connecting things that were never connected before. Operational technology (OT) and information technology (IT) sat in entirely different parts of the organization. As a result, today's attack surface is far larger and the risk greater because two different architectures are brought together without the necessary oversight. As a result, there is a high likelihood of misconfiguration.

5. Regulatory complexity

One constant is the need to comply with industry-specific and economy-wide regulations. As operators of essential services overseeing critical national infrastructure, many energy firms need to demonstrate a good overview of governance, risk management, asset management, and management of third-party and supply relationships.

Across the world, additional regulatory pressure is being applied to those who manage critical infrastructure. In Europe, this is a mandate by the EU's Network and Information Systems (NIS) Directive. In the United States, meanwhile, critical infrastructure protection is enshrined in NERC CIP – the North American Electric Reliability Corporation Critical Infrastructure Protection Plan – and outlined in the Biden administration's Industrial Control Systems Security Initiative. Elsewhere, organizations deal with ISA/IEC 62443 and the Australian Critical Infrastructure Bill of 2021. While compliance is critical, it does not guarantee organizational security.



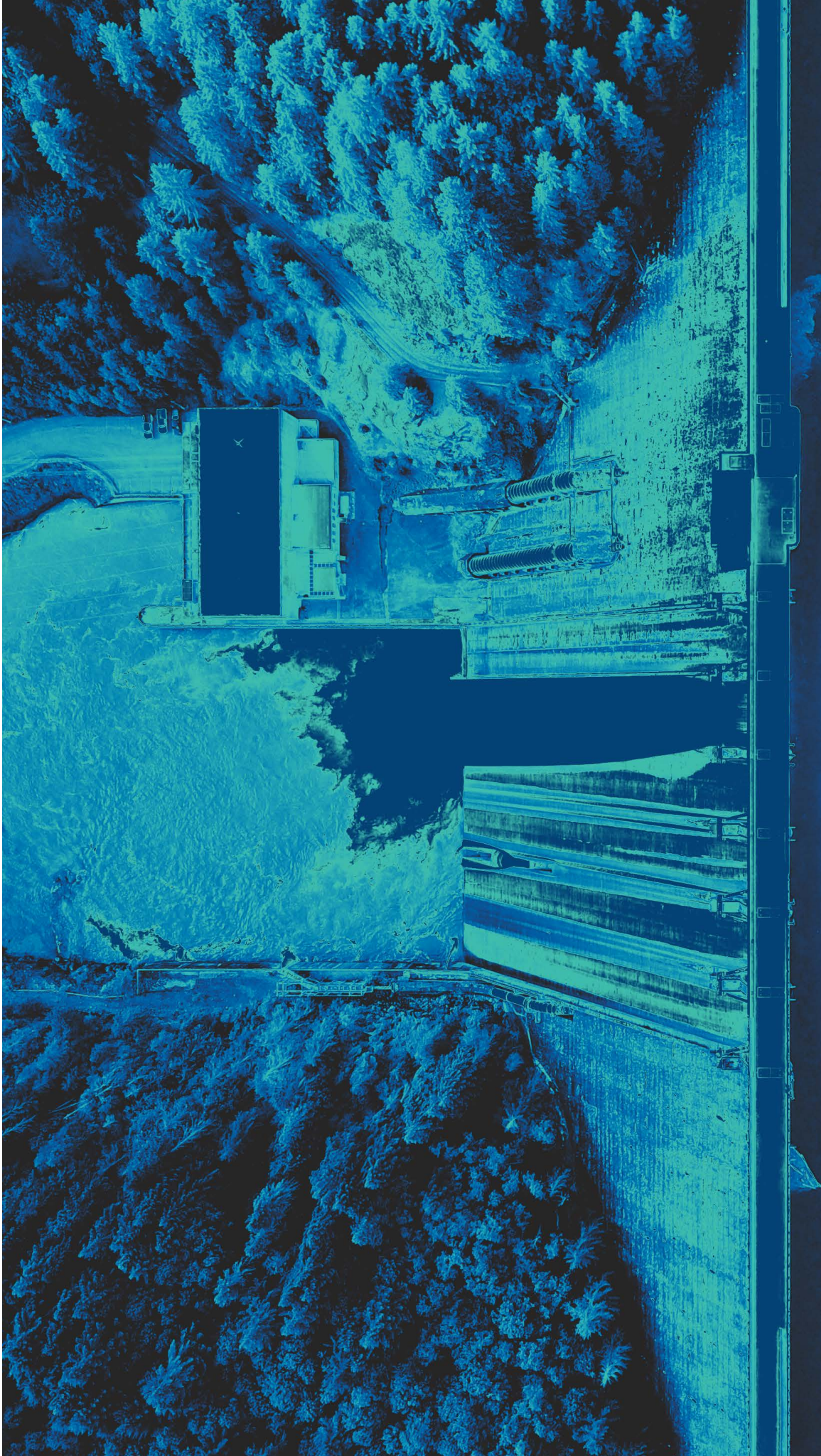
The way forward: utilities de-risking IT/OT convergence

No company is safe from cyberattacks, but those with OT environments are particularly vulnerable. The desire to close the gap between OT and IT is understandable. The tangible benefits are centralizing and unifying remote management while extracting data analytics that proves as useful in the boardroom as they do on the production floor. However, they come with risks if not managed properly. And there is plenty of evidence that organizations are more confident than they should be when managing that risk.

For example, as Skybox's research indicates, organizations with OT environments tend to underestimate the risk of a cyberattack. According to our survey, 71% of utility respondents are highly confident that their organization will not experience an OT breach in the coming year. However, 87% acknowledged that they had experienced at least one breach in the previous 36 months.⁶

The longevity of OT systems – and their deployment in remote locations – creates three potential problems. First, it increases the likelihood of software obsolescence. Second, it is likely to lead, in turn, to unpatched vulnerabilities – simple patching procedures may require complex change management processes due to the risk of equipment downtime or unforeseen hazards. Finally, it creates a cybersecurity talent gap where specialized IT/OT architecture expertise is lacking.

⁶ Cybersecurity risk significantly underestimated by operational technology organizations, Skybox Security, November 2021

An aerial photograph of a large concrete dam spanning a river, surrounded by dense green forest. The image is used as a background for the right side of the slide.

“Just as evil thrives on apathy, ransomware attacks will continue to exploit OT vulnerabilities as long as inaction persists.”

**Gidi Cohen, CEO, and Founder,
Skybox Security**

88%

**Increase in OT
vulnerabilities
between 2020
and 2021⁷**

OT systems were never meant to be networked

Mechanical rather than digital, these systems are repaired when they go wrong. If it's working, it doesn't tend to get touched. Unlike IT systems, there isn't a culture of introducing regular patches. OT systems need to be running 24/7 – patching is anathema to that goal. And unlike an IT lifecycle of 3-5 years, OT systems can last for several decades, often outlasting the vendors who would otherwise be able to support them.

A further complication comes from a typically hands-off approach to third-party vendors. When they carry out maintenance and tests, they often freely plug a laptop into internal networks without oversight. As a result, utilities firms open themselves up to infection and exploitation. Our research shows that 78% of respondents acknowledge that multivendor complexity presents a unique challenge.

The result? A 'candy shell' network – hard firewalls on the outside but gooey on the inside, internal networks left open to reduce friction but, inevitably, leaving an organization exposed. For evidence of how open internal networks can provide the opportunity for malicious actors, look no further than the WannaCry ransomware attacks of 2017.

More needs to be done. More means greater visibility. Misconfigurations will go undetected without complete network visibility of the IT/OT attack surface.

Similarly, identifying vulnerability exposure and access policy violations will become increasingly difficult, if not impossible.

In addition to poorly-configured IT networks and unpatched OT systems, there's another common threat to security. Namely the fact that many organizations outsource OT management to third parties. When external contractors manage operational work, enterprise-wide visibility suffers.

Therefore, full visibility and end-to-end teamwork are the holy grail of secure network management and the only way to overcome remediation complexity. IT and OT teams need solutions that advance a collaborative approach to prioritize critical vulnerabilities, bolster security resilience, and limit downtime—knowing which network configurations and security controls exist, including IPS, endpoint security, and router ACLs. No organization can rely on patching.

Organizations need to think beyond compliance, too. While plan documentation or a checkmark provides a valuable baseline – concentrating minds and alerting organizations to potential control gaps – it won't on its own protect an organization from security breaches. Just because you are compliant doesn't mean you are secure.

It is time to stop looking in the rear-view mirror when it comes to security.

Five steps to de-risk IT/OT convergence in the utility sector



1. Create mature, consistent, and enterprise-wide security posture management.

Unfortunately, too many organizations find themselves playing security catch up. Teams invest increasing amounts on point solutions in the hope of finding an answer to yesterday's exploitation. It's a reactive approach and creates a vicious cycle in the hope of keeping pace with the rapidly evolving threat landscape. Instead, organizations should focus on deploying an enterprise-wide security posture management program that is both mature and consistent. With visibility and context across both IT and OT environments, utility leaders can reduce exposure to risk by optimizing security planning, deployment, and remediation processes.



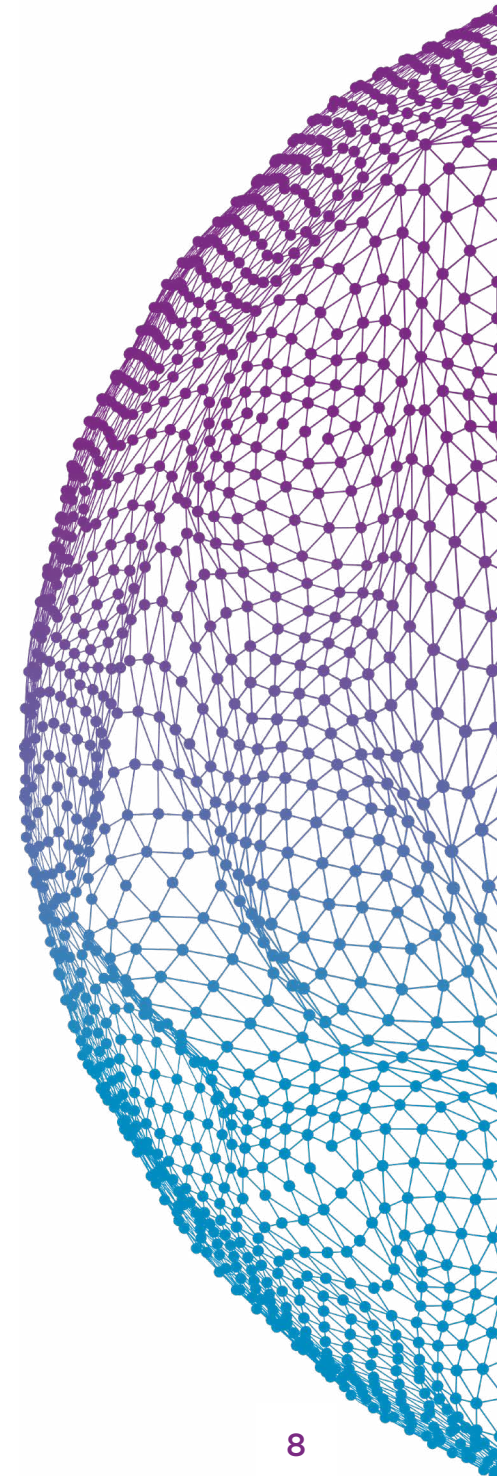
2. Apply automation to reduce risk of misconfiguration and ensure continuous compliance.

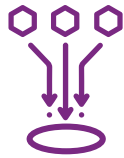
The volume and variation of security controls, rules, and policies needed across a multivendor environment make oversight and change management increasingly complex. Without proper updates and configurations, compliance remains a challenge. Automating workflows, including change processes and validation, eliminates human errors and streamlines operations, reducing the risk of misconfigurations. It also allows teams to set globally applied standards and ensure future compliance. For larger organizations, the ability to assign multiple compliance requirements on a single unified platform is an essential step in understanding network risks.



3. Create a common view across security, IT, and OT.

Utilities must be able to see their entire attack surface. Our approach is to apply a network model. This provides visualization of all environments, both in their enterprise-wide context and with specific rules and configurations in mind. The network model allows an organization to run assessments and simulations against all devices, vulnerabilities, and configurations. This means organizations can leverage their network model to assess the effectiveness of security controls. Critically, an organization can also gauge access compliance with network segmentation requirements, validate configurations and changes, and identify and precisely measure their exposure.





4. Eliminate silos and remove security blind spots.

Aggregating and normalizing data across devices enables teams to work together to identify and prioritize critical vulnerabilities. If the IT team knows all paths and firewalls, it can patch precisely and on the fly without bringing production to a halt. With Skybox Vulnerability Control, organizations can aggregate a wide range of data from scanners, security, network infrastructure, configuration databases, non-scannable assets, etc. Then, using passive assessment technology that detects vulnerabilities in off-limits network zones and devices, teams can fill in what would otherwise be blind spots. For OT risk teams, access to both forms of vulnerability-identifying technology – active and passive – is essential to gain timely insights, deploying scanless detection where necessary.



5. Reduce downtime by optimizing remediation options beyond patching.

Our approach means organizations can identify the most dangerously-exposed vulnerabilities and choose the best option to remediate these risks -the ability to choose matters, especially in OT environments with stricter policies. Teams need a solution that calculates risk scores for assets by factoring together four critical variables: the asset's measured Common Vulnerability Scoring System (CVSS) severity; asset exploitability; asset importance; and asset exposure based on the security controls and configurations in place across the network. We provide critically-important exposure analysis – often, a company's smaller assets are the most vulnerable and have an outsized financial impact on their business. For example, when one client detected tens of thousands of vulnerabilities in just one environment, we used exposure analysis to determine that vulnerabilities on only 4-6 assets had the potential to cost them many millions of dollars if compromised.

Case study 1: Gaining visibility of an entire OT/IT estate – from a single management console

Skybox Security partnered with an organization that controls the regulated activities of Italy's natural gas sector, managing the transport, storage, and regasification of natural gas.

The organization operates in a highly regulated environment. It must be able to demonstrate its compliance with health, safety, and environmental legislation, ensure uptime and be ever vigilant in the fight against cyberattacks.

The organization needed to monitor and protect its Supervisory Control and Data Acquisition (SCADA) assets from attack. These assets underpin a downstream network and storage infrastructure that spans Europe across over 40,000 km of pipeline and storage.

A key requirement was that the solution would complement their existing investments and enable them to see their consolidated security posture across both IT and OT networks.

The Skybox Security Posture Management platform comprises Firewall Assurance, Network Assurance, Change Manager, and Vulnerability Control modules. By integrating OT security scanning data from Nozomi Networks into the platform, the organization has gained visibility of the entire OT/IT estate from a single management console.

The benefits of proactive security posture management

- **Materially drive down risk.** Ensure that critical infrastructure is not externally accessible, shield the most sensitive parts of the network, and validate existing segmentation.
- **Demonstrate the value of the security program.** By illustrating risk reduction by, for example, showing a causal link between a drop in outages and a reduction in vulnerabilities, a CISO can demonstrate to leadership the value of the work done by the security team.
- **Remediate faster.** Organizations no longer have to wait for the next maintenance window to reduce risk. With complete visibility, action – even addressing Zero-Day attacks – can be taken in short order.

Case study 2: Monitoring and maintaining network access and separation across OT networks

This UK-based multinational electricity and gas infrastructure provider, controls the national transmission and distribution of electricity and gas, serving the needs of over 50 million people and more than 5 million businesses.

As a cornerstone of the UK's critical national infrastructure, the organization operates with a mandate to deliver energy to the point of need safely, reliably, and efficiently. Turning this into reality means managing a vast array of overhead lines, pylons, underground cables, pipes, and transmission substations.

The organization uses a dedicated Operational Technology (OT) network to manage these electricity assets. They needed a solution to help them manage access to this network and ensure compliance with best practices for network segregation.

A key requirement was that the solution should work with the organization's installed base of Industrial Control System (ICS) firewalls and switches.

The Skybox Security Posture Management platform solved these challenges through a combination of firewall and network assurance. The platform creates a network model that emulates the actual OT network of the organization. It is a dynamic, visual representation of the network generated by aggregating and centralizing data from the ICS firewalls and network assets.

The model eliminates any potential for blind spots in the network and ensures complete visibility for the team. Marking the network model in terms of access zones makes it possible to analyze network access compliance.

“Using the Skybox platform we can test, demonstrate and ultimately ensure we comply with the regulations governing network separation.”

How Skybox Security can help

The trends explored throughout this paper paints a picture of an industry sector undergoing tremendous change. It is an exciting time to be in the utilities sector – not least to lead the broader economy through the energy transition – but organizations must protect themselves, their customers, and wider society from increasing cyber threats.

The cornerstone of an effective cyber security strategy is a comprehensive inventory of assets and vulnerabilities spanning IT and OT estates. Today, the volume of vulnerabilities defined as ‘critical’ or ‘high severity’ according to the Common Vulnerability Scoring System (CVSS) scores only increases alert fatigue. The likely result: breaches from missed alerts. Instead, vulnerability management analysts seek intelligence based on asset importance, vulnerability exploitability, and asset exposure.

At Skybox Security, we provide a unified view of assets, controls, configurations, and vulnerabilities across your IT and OT environments. With our platform’s robust exposure analysis and threat intelligence, we help you eliminate security blind spots, reduce risk, and drive compliance with regulatory frameworks.

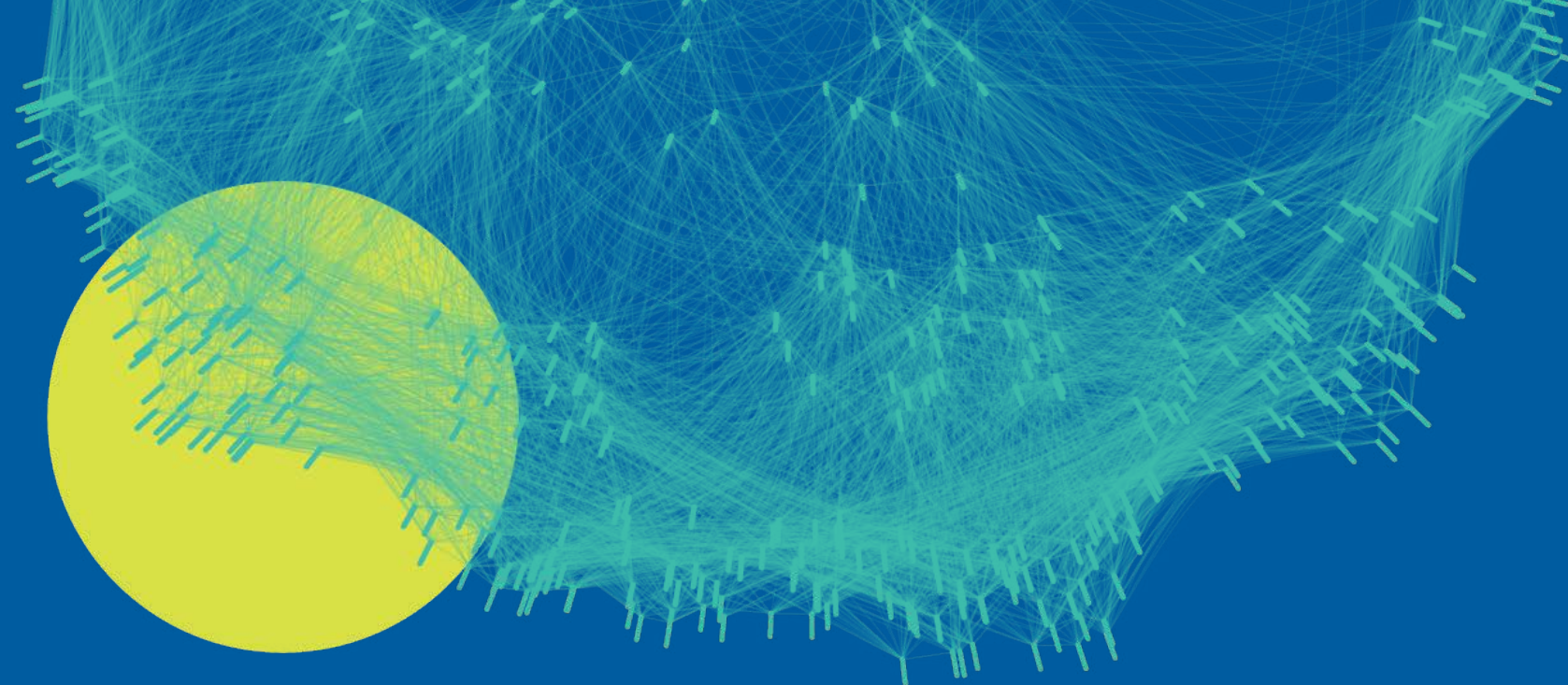
Through comprehensive modeling and analytics and vulnerability detection that’s both passive and active, Skybox can provide complete visibility across

the entire attack surface, including third-party networks. As a result, you can properly understand and proactively respond to security risks – and better protect your critical assets against vulnerabilities.

With Skybox by your side, we can help you:

- 1. Discover** what is on your network. You can’t defend what you can’t see.
- 2. Validate** controls. Work with network teams to identify how systems connect and use Skybox to validate your understanding of segmentation, ascertaining which areas should and should not talk to each other.
- 3. Prioritize** vulnerabilities and work out a plan of action. Decide which vulnerabilities can be addressed now and which should be scheduled for the next maintenance window.

To find out how we can help meet your challenges, please visit skyboxsecurity.com.



Complete visibility

At Skybox, we understand the transformative challenges the utilities industry faces.
And we're experts when it comes to security visibility, analytics, and automation.
To find out how we can help meet your challenges, let's connect.

skyboxsecurity.com/contact-sales/