CISO
POINT OF VIEW

The 2026 Infrastructure Security Outlook

Sponsored by core6

Introduction

Infrastructure security is undergoing the most significant transformation in decades. Once viewed as the quiet, foundational layer beneath applications and endpoints, today it has moved to the center of how global enterprises operate, scale, and defend themselves.

This ***CISO Point of View*** Guide brings together insights from leading CISOs to highlight how organizations are redefining infrastructure security — from balancing investments and solving visibility gaps to modernizing operating models, securing storage and backup systems, and preparing for emerging risks like AI-driven attacks and quantum disruption.

Mark Thomson
Deputy Group CISO
Howden

Rick Doten
Former VP Information Security
Centene

Gernette Wright
Former IT Security Officer - Americas
Schneider Electric

Erdal Ozkaya
CISO
Morgan State University

Mats Nygren
Former VP Information Security
U.S. Bank

Girish Kulkarni
CISO
Aurionpro

Matthew Lang
Former CISO
State Employees' Credit Union (SECU)

Bob Turner
Former CISO
Penn State University & University of Wisconsin-Madison

Section 1

Framing the Conversation — The Role of Infrastructure Security

How do you balance investment between traditional security domains (like endpoint or application security) and infrastructure protection?

Mark Thomson
Deputy Group CISO
Howden

Effective security investment begins with a risk-based approach rather than equal distribution across domains.

Conduct thorough risk assessments to identify critical assets and vulnerabilities, ensuring resources are directed where they mitigate the greatest impact. For instance, businesses heavily reliant on cloud services may prioritize infrastructure segmentation and identity controls over endpoint hardening.

Internal strategies and frameworks such as ISO 27001 and PCI-DSS reinforce this alignment by linking controls to business objectives and compliance requirements.

Beyond prioritization, investment needs to be balanced between prevention, detection, and response across endpoint, application, and infrastructure security.

Given the evolving threat landscape, regular reviews and dynamic reallocation are critical to address emerging risks like machine identity sprawl or AI-driven attacks.

A simple yet practical allocation model might dedicate 40% to infrastructure protection, 35% to endpoint and application security, and 25% to detection and response capabilities.

Rick Doten
Former VP Information Security
Centene

To me everything is infrastructure. Applications are their own platforms, creating infrastructure as code, distributed architectures, etc. Endpoints are accessing SaaS tools. Even email security and web gateways are part of the infrastructure.

The only thing I put outside is security operations, which scales based on how much "infrastructure." These need to be monitored, with security events and incidents identified & remediated.

Gernette Wright
Former IT Security Officer - Americas
Schneider Electric

The best way to understand where to focus is through assessments, especially a solid Business Impact Analysis (BIA). That gives you a clear sense of what matters most to the business and where an incident would have the biggest impact and requires an investment in fortification.

At the end of the day, the goal is to align security spending with business objectives, risk tolerance, and compliance needs instead of relying on guesswork.

Erdal Ozkaya
CISO
Morgan State University

There is no perfect balance, just calculated risk. The reality is, my budget isn't infinite. I don't look at it as 'endpoint vs. infrastructure' anymore because the attackers certainly don't.

I look at it like home security. You can put the best locks on the doors (endpoint), but if the walls are made of glass (infrastructure), you're in trouble. My philosophy is pretty simple: follow the data.

I'd rather have decent security everywhere than 'Fort Knox' on the computers and an open door in the cloud. It's about integration – if my firewall talks to my endpoint tool, I get double the value for the same dollar.

Girish Kulkarni
CISO
Aurionpro

Use a risk-based approach: prioritize based on business impact, threat landscape, and shared responsibility. Goal: defense-in-depth.

Mats Nygren
Former VP Information Security
U.S. Bank

In my experience, you cannot balance them with a simple budget split. You need to consider the movement of trust, where there are overlaps and dependencies, inside the enterprise.

To balance investment intelligently, the following should be accounted for:

- **Platform reliability, high availability, and security are now inseparable –** if your infrastructure cannot enforce least privilege, validate service identity, or deploy consistently with guardrails, it doesn't matter how strong your endpoint tooling is. Infrastructure layer security weakness amplifies downstream risk. Investing here becomes a strategic allocation of resources that amplifies their impact on everything above it.

  Automation has created new invisible attack surfaces and threat vectors – AI agents, ephemeral workloads (serverless), pipeline automations, and infrastructure APIs produce risk we don't see until something breaks. These surfaces require investment in things like unified visibility, logging, and continuous monitoring, as well as drift detection and configuration integrity

Infrastructure security is no longer just the foundation beneath the enterprise – it has moved to the center of how we operate, scale, and defend.

Section 1 Summary

Security leaders overwhelmingly agree that modern enterprises can no longer separate endpoint, application, and infrastructure security — the lines have blurred. CISOs emphasize risk-based prioritization, business alignment, and continuous reassessment as the only viable way to balance investments across the security stack.

Infrastructure security has shifted from foundational to central, driven by platform complexity, cloud dependence, machine identities, and automation. Traditional budget splits or legacy models no longer work; instead, organizations must invest where weaknesses create the greatest systemic risk.

Takeaways:

- **Risk-based investment dominates —** business impact, critical assets, and compliance determine priorities, not rigid categories
- **Infrastructure weaknesses amplify all downstream risk;** reliability, identity enforcement, and segmentation must be strong at the core
- **Automation and ephemeral workloads introduce new invisible attack surfaces,** requiring fresh investment in monitoring, drift detection, and configuration integrity
- **Integration > isolation —** security tools must work cohesively (e.g., endpoint + network + identity).
- **Infrastructure is now at the center of trust,** not the perimeter

Section 2

Real-World Priorities & Challenges

As infrastructure becomes increasingly hybrid and distributed, what are the biggest visibility or control challenges you face?

Mark Thomson
Deputy Group CISO
Howden

Adopting hybrid infrastructures spanning on-premises systems, multiple clouds, and edge environments, fragmented visibility becomes a major challenge.

Proprietary monitoring tools across different platforms can create blind spots and inconsistent telemetry, making incident detection, compliance, and resource optimisation difficult.

Common issues include distributed data and applications that obscure dependencies, inconsistent security postures due to varied policies, and complex compliance requirements around data residency and audit trails.

To address these gaps, recommendations may include centralized observability platforms, micro-segmentation to limit lateral movement, and integrated SIEM or SASE architectures for unified monitoring and policy enforcement.

Rick Doten
Former VP Information Security
Centene

It's just scale and surface area. With cloud, it's actually easier because nothing happens without an account, logging, and visibility. It gets more challenging with on-premise because there are isolated segments, separate domains, and things that aren't visible.

Gernette Wright
Former IT Security Officer - Americas
Schneider Electric

Without a doubt, it's about knowing where data is and who can access it. When you combine on-premises systems, multiple clouds, SaaS platforms, and older systems, it becomes hard to keep track.

Access control gets trickier because each platform handles permissions differently. This opens the door for privilege creep. When teams rush or do not follow proper procedures, over-provisioning often results.

AI has made this even more complicated because it creates a lot of data sprawl. Data gets copied, shared, processed, and stored across various tools, teams, and regions.

In a global company, this problem becomes tougher since each country has different rules about data residency and privacy. If we don't clearly understand where data resides, it's easy to fall out of compliance without realizing it.

Gernette Wright
Former IT Security Officer - Americas
Schneider Electric

Another important aspect is knowing where the data came from, how it has changed, who worked with it, and whether the right permissions were in place at each step. Without this traceability, accountability becomes unclear. It also increases security risks because sensitive information can unintentionally end up in systems not meant to store it.

This highlights the need for strong governance and close collaboration with the teams that manage day-to-day data operations. It's an age-old problem that has only become more complicated over time.

Erdal Ozkaya
CISO
Morgan State University

The scariest thing for any CISO isn't the hacker; it's the server someone spun up on a credit card three months ago that nobody knows about. We call it 'Shadow IT,' but really, it's just people trying to move fast.

The challenge is the 'Fog of Cloud.' Assets don't sit in a rack anymore; they exist for five minutes in a container and then vanish. Trying to do asset management today feels like trying to count raindrops in a storm. If I can't see it, I can't patch it, and I definitely can't defend it.

Girish Kulkarni
CISO
Aurionpro

Fragmented visibility across on-prem, cloud, and SaaS.
The solution is to use centralized logging & SIEM, Zero Trust for identity, as well as continuous posture management

Matthew Lang
Former CISO
State Employees' Credit Union (SECU)

Biggest challenges I see currently are insider threats.

Many companies struggle with access controls whether it's from personnel moving from job to job or laziness it's hard to tell, but many companies fail to remove access in a timely manner.

They give access in 72 hours or less but take 6 months to a year to remove access that leads to a lot of risk.

How do you ensure IT teams and security teams stay aligned on priorities and accountability?

Mark Thomson
Deputy Group CISO
Howden

Equally important is ensuring IT and security teams remain aligned on priorities and accountability. Internal initiatives such as IT Security Minimum Standard workshops help establish unified policies and traceability between risks and controls. Alignment strategies include shared KPIs linking uptime and risk reduction, regular joint reviews, and consistent governance frameworks to build trust across the business.

Externally, embedding security into DevOps processes, forming cross functional committees, and leveraging integrated platforms for automation and monitoring are proven approaches to reduce silos and streamline collaboration, ensuring both teams operate collaboratively.

Rick Doten
Former VP Information Security
Centene

Priorities are easy, make sure that which is critical to the business is protected, resilient, and stable. We spend too much time chasing the priorities given by the tools or CVE scores without understanding business context and impact. We have only statically evolved our prioritization based on external facing, or known exploit. But even that might not matter to the business, based on the specific platform.

Gernette Wright
Former IT Security Officer - Americas
Schneider Electric

To me, it starts with shared outcomes and doing what is best for the organization.

When there is a question about what should go first, I go back to the business objectives and the BIA. If a project has a direct revenue impact or carries high risk, it needs to move to the top of the list.

It is also important not to make prioritization decisions in isolation. Working through these decisions with your IT counterpart creates alignment and makes it easier to get buy-in from both teams.

I also set clear timelines for when other projects can begin, and if there is a delay for one reason or another, it is clearly communicated. This cannot be a one-time meeting.

Having this level of consistency and clear ownership drives accountability and keeps everyone moving in the same direction.

Erdal Ozkaya
CISO
Morgan State University

We have to stop being the 'Department of No.' That approach is dead. If I just throw policies over the wall at the Ops team, they'll ignore me and I wouldn't blame them.

I try to embed my security people into the infrastructure teams. We sit in their meetings, use their Jira boards, and speak their language. We frame everything around uptime. I tell them, "I'm not here to annoy you with patches; I'm here to make sure this system doesn't crash on Black Friday because of a DDoS attack." When they see security as a stability tool, the friction disappears.

Girish Kulkarni
CISO
Aurionpro

To ensure these teams stay aligned, its important to have shared KPIs, a RACI matrix, joint risk reviews, and DevSecOps integration.

Section 2 Summary

In hybrid environments, leaders struggle with fragmented visibility, data sprawl, identity complexity, and the accelerating spread of shadow IT. Cloud offers strong telemetry, but legacy on-prem environments remain pockets of blind spots. Insider risks and over-permissioning continue to grow as organizations move faster than governance structures can keep up.

IT/Security alignment depends on shared KPIs, joint risk ownership, and business-driven prioritization, not tool-driven urgency.

Takeaways:

- Visibility gaps are the #1 challenge in hybrid ecosystems — inconsistent logging, siloed platforms, and ephemeral workloads hide risk
- Data governance and access control are increasingly difficult, especially with AI-driven data replication and global residency requirements
- Shadow IT remains a major vulnerability, especially unmanaged cloud resources and short-lived workloads
- Identity lifecycle management is broken — access is granted quickly but rarely removed promptly
- IT + Security alignment requires shared outcomes, not “department of no” dynamics; embedding security into DevOps and infrastructure teams works best

Section 3

Modernization & Transformation

Are traditional infrastructure security models still relevant — or do we need a new operating model for the modern enterprise?

Mark Thomson
Deputy Group CISO
Howden

Traditional perimeter-based security models have been effective in centralized environments with well-defined boundaries. However, today's enterprises operate across hybrid and multi-cloud ecosystems, remote workforces, and distributed applications, making these legacy models inadequate. They fall short in areas such as visibility, dynamic access control, and real-time threat detection.

Modern frameworks like Zero Trust Architecture (ZTA) have become the standard, built on principles of "never trust, always verify," least privilege access, and continuous monitoring. These approaches replace implicit trust with identity-centric security, micro-segmentation, and adaptive policies.

While traditional models still have a role for certain on-premises systems, they must be integrated into a flexible operating model that supports cloud native, API-driven, and automated security practices.

Rick Doten
Former VP Information Security
Centene

Cloud has evolved the model. Many organizations don't have internal infrastructure like was typical before. Servers, email, databases, applications are all SaaS or PaaS, and not in a sever room or data center.

The WAN is more administrative than operational. The fact many users work from home, or some organizations only have offices with Internet connections and laptops highlights how we've changed.

Gernette Wright
Former IT Security Officer - Americas
Schneider Electric

Traditional infrastructure security models still matter, but they are no longer enough on their own. The way we now build our connectivity for our products and core business functions has evolved from just on-prem to a variety of different platforms, including SaaS and IaaS. Therefore, our security models need to evolve to adapt to this new reality.

Modern environments are hybrid, distributed, and constantly changing to suit business needs and customer demands. Data is no longer confined to a traditional perimeter, and mobility and availability are extremely important. The same perspective can be said about OT environments.

What does still work are the fundamentals of security. Knowing what you have to protect and where they are (asset management), understanding who has access to what resource and when (access management), understanding where your data is (data governance), and knowing what traffic is allowed in and out as well as monitoring for malicious activity (network security management).

Gernette Wright
Former IT Security Officer - Americas
Schneider Electric

Our protection scheme has to be able to stretch across our distributed network, on-prem, endpoints, etc. The go-to for most of us is Zero Trust. That means nothing should be implicitly trusted and everything needs to be verified before being authenticated and authorized.

Erdal Ozkaya
CISO
Morgan State University

The old 'Castle and Moat' model? It's gone. It's comfortable to think, 'If I secure the perimeter, the inside is safe,' but it's a lie.

We operate on Zero Trust now, which sounds like a buzzword, but it's actually a mindset shift. It means I treat my internal corporate network with the same suspicion I treat the open internet. It's paranoid, sure, but in this job, paranoia is a virtue. We assume the bad guy is already inside.

Matthew Lang
Former CISO
State Employees' Credit Union (SECU)

Yes traditional security layers are still relevant you have to have a base level of security and then build out based on best bang for the buck.

How do you approach securing "invisible infrastructure" — the underlying systems that run across hybrid cloud, APIs, and automation pipelines?

Mark Thomson
Deputy Group CISO
Howden

Securing invisible infrastructure comprising APIs, automation pipelines, and orchestration layers require embedding security into the design rather than applying bolt on controls (build it in, rather than bolt it on).

Key practices include managing secrets and non-human identities through centralized vaults and automated rotation, enforcing Zero Trust principles for APIs with strong authentication and continuous monitoring, and integrating security controls directly into development and operational pipelines for real-time enforcement.

Observability and automation are also critical, using API gateways, rate limiting, and AI-driven anomaly detection to protect dynamic workloads. Such a proactive approach supports mature security scales with infrastructure complexity, maintains compliance across jurisdictions, and eliminates operational blind spots.

Rick Doten
Former VP Information Security
Centene

I approach securing 'invisible infrastructure' by focusing on the basics: asset management; data protection, identity management, and vulnerability management. Stacked in that order.

Like I mentioned about cloud, nothing happens without being recorded, so make sure you know what could be a risk, and have the right telemetry to monitor it is key.

Gernette Wright
Former IT Security Officer - Americas
Schneider Electric

APIs are fantastic; you can connect almost any application across different types of infrastructure without a lot of pain. But from a security perspective, they can be a nightmare. Without proper safeguards and development practices, data can be pulled and stored in locations they weren't meant to be, exposing sensitive information.

So, before any technology, my first focus is on the fundamentals, and for this area, it's SDL. Developers must understand what they are asking the program to do and what access levels should be in place to secure the data.

The other area is visibility. Like any other asset management process, it starts with ensuring you have the right technology to:

1. Identify where and what cloud processes are in place
2. Identify the APIs and enumerate the various access and configurations

This also ties into your IAM program so permission sprawl, over-permissioning, and unmanaged machine identities or service accounts can be caught and addressed during regularly scheduled review cycles.

Erdal Ozkaya
CISO
Morgan State University

This is the hardest part of the job right now. You can't walk into a data center and point at an API.

We have to shift left. That means we are scanning the code before it ever builds the infrastructure. By the time the server is live, it's too late. I tell my team: "Fix it in the blueprint, not the building." If we can catch a misconfiguration in Terraform or Kubernetes manifests before deploy, we save ourselves a weekend of panic later.

Girish Kulkarni
CISO
Aurionpro

Invisible infrastructure requires security by design:

- API security gateways and runtime protection
- CI/CD pipeline hardening with secrets management
- Infrastructure-as-Code (IaC) scanning before deployment

Matthew Lang
Former CISO
State Employees' Credit Union (SECU)

As far as hidden IT outside the organization, you need extremely good contracts with all 3rd parties – including the right to scan for weaknesses.

Section 3 Summary

Traditional perimeter-based models no longer meet the needs of cloud-native, API-driven, highly distributed enterprises. Zero Trust has emerged as the operating mindset for modern infrastructure, emphasizing continuous verification, least privilege, and identity-centric controls.

"Invisible infrastructure" — APIs, CI/CD pipelines, automations, IaC — requires security built in at design, not bolted on after deployment. Leaders stress shifting left, strengthening secrets management, and improving visibility into machine identities and pipeline behavior.

Takeaways:

- Zero Trust is the new standard, but the fundamentals (asset management, IAM, network controls) still anchor modern security
- Perimeters are obsolete — remote work, SaaS, and distributed apps demand identity- and data-centric controls
- Invisible infrastructure must be secured at the blueprint level: IaC scanning, secrets vaulting, API authentication, pipeline hardening
- Non-human identities represent a growing attack surface, often outnumbering human users by orders of magnitude
- Observability and automation are essential to handle ephemeral workloads and complex API interactions

Section 4

Storage & Backup — The Last Line of Defense

Storage and backup systems are often overlooked but critical in cyber resilience. How do you ensure they're properly secured?

Mark Thomson
Deputy Group CISO
Howden

Securing storage and backup systems is critical to cyber resilience, as they often serve as the last line of defence against ransomware and destructive attacks.

Robust controls include automated and documented backup processes, maintaining isolated or air-gapped copies, and regularly testing restoration procedures to meet recovery objectives.

Advanced measures such as immutable backups, strict segregation of duties, and continuous anomaly monitoring further strengthen protection.

General best practices recommend layered strategies like immutable snapshots, offsite and logically isolated backups, automated recovery orchestration, and AI-driven threat detection integrated into storage platforms.

Hardening backup environments post-deployment through configuration validation and compliance checks is essential, as misconfigured vaults or unpatched systems remain prime targets for attackers.

Rick Doten
Former VP Information Security
Centene

I would say that storage and backup systems are only overlooked in immature organizations, although ransomware has put this to forefront in the last 5-8 years.

Now immutable backups are a must; testing restoration is critical.

Having critical systems on cold or warm sites is not just for large banks anymore. There are plenty of tools and guidance to do this. And cloud has made this easy for many who rely on it.

Gernette Wright
Former IT Security Officer - Americas
Schneider Electric

From my perspective, backup systems are arguably the most critical piece of your BCP and DR strategy. Outside of cost, there are two other critical areas I look for: immutability and speed of restoration.

On the operational side, these backup systems must be tested. I ensure regular restorations are done quarterly and a full restore done annually of a critical system or systems.

Storage security addresses the same fundamentals, encryption, access control, patching, and monitoring. It's important to make sure the storage platform is properly secured through encryption, tight access control, patching, and monitoring, and that sensitive data isn't being copied to

Gernette Wright
Former IT Security Officer - Americas
Schneider Electric

locations that weren't meant to hold it.

For cloud storage specifically, I also look at resiliency, ensuring replicas and redundancy are set up correctly, such as using multiple availability zones in AWS or the equivalent in other platforms. This helps protect against regional outages and ensures that critical data is still accessible even if part of the environment fails.

Bob Turner
Former CISO
Penn State University & University of Wisconsin-Madison

To think about the future, you have to go back to basics: where is your information actually kept?

Your primary data lives in central storage systems that people use to do business. Today, backup systems are also often kept online in some form, which can be risky.

Any primary data source that is critical to the enterprise needs either an offline backup or a very well-isolated backup.

Enterprises that are doing this well aren't usually talking about it publicly, but they're quietly adopting the best security controls the industry can provide. If you're not there yet, that's where you need to be heading.

For me, data is king. On my LinkedIn profile I have a sign that says, "It's all about the data!" and I believe that. You need to understand what your data is, where it lives, where it goes, and how many copies of it exist.

The big questions are: How do you keep relevancy and recency aligned between primary and secondary data? Are all of those locations appropriately secured? And are there conflicts or inconsistencies between them?

At the end of the day, securing storage and backup systems isn't just about hardware and software. It's also about understanding that it's about the data, and designing your architecture, isolation, and backup strategy around that truth.

Erdal Ozkaya
CISO
Morgan State University

Backups used to be the boring part of IT. Now? They are the only thing standing between me and a ransom payment.

I treat my backup console like it holds the nuclear launch codes. It's on a separate network, requires multi-factor authentication, and we use immutable storage. That means once a backup is written, nobody – not even me – can delete it for 30 days. If a hacker gets in and tries to wipe our history, the system just says 'No.' It helps me sleep at night.

Girish Kulkarni
CISO
Aurionpro

To ensure storage and backup systems are properly secured, you need encryption at rest and in transit, strict access controls and MFA, and also regular restore drills to validate integrity and speed of recovery.

Do you see a growing convergence between infrastructure reliability and cybersecurity — especially when it comes to data protection and recovery?

Mark Thomson
Deputy Group CISO
Howden

There is certainly an increasing convergence between infrastructure reliability and cybersecurity, particularly in data protection and recovery.

Traditionally, disaster recovery focused on physical resilience while cybersecurity addressed digital threats, but today these domains intersect as cyberattacks can disrupt critical infrastructure as severely as natural disasters.

Organizations need to embed cybersecurity into resilience frameworks, aligning backup strategies with business continuity plans, and leveraging technologies such as Zero Trust and cyber-resilient storage to ensure operational continuity under attack conditions.

Such a shift reflects a move from siloed strategies to holistic resilience models that unify governance, risk management, and technical controls across physical and digital layers.

Rick Doten
Former VP Information Security
Centene

Again, for mature organizations these have always been aligned. The business knows, either through a BIA, or just basic operations which systems need to be online, reliable, and accurate or the business stops working. It's not just for manufacturing where they know for every 15 minutes their line isn't running; they know how much money they are losing.

This is the same with some critical business applications. This is the A in the CIA triad.

Gernette Wright
Former IT Security Officer - Americas
Schneider Electric

I don't believe the two can be separated. When it comes to data, it needs to be available when it's needed, which means the infrastructure has to be up. If it's up and online, it needs to be protected. If the infrastructure is down, a plan must be in place for fast restoration, whether it's through failover (BCP) or full recovery (DR).

From my perspective, reliability and cybersecurity share the same end goal: keeping the business operating. A hardware failure, cloud outage, misconfiguration, or ransomware event all lead to the same outcome if you're not prepared.

Erdal Ozkaya
CISO
Morgan State University

There's certainly a growing convergence between infrastructure and cybersecurity. In a modern attack, a cyber incident is a disaster scenario.

When ransomware hits, the security team stops the bleeding, but the infrastructure team has to restart the heart. If those two teams haven't practiced together, the business dies on the operating table. We don't just test 'can we restore the data?' – we test 'can we restore it clean, without bringing the virus back?'.

Girish Kulkarni
CISO
Aurionpro

Absolutely. Cybersecurity and reliability are now inseparable. Ransomware has made backup integrity a security priority.

We integrate cyber resilience metrics into business continuity planning.

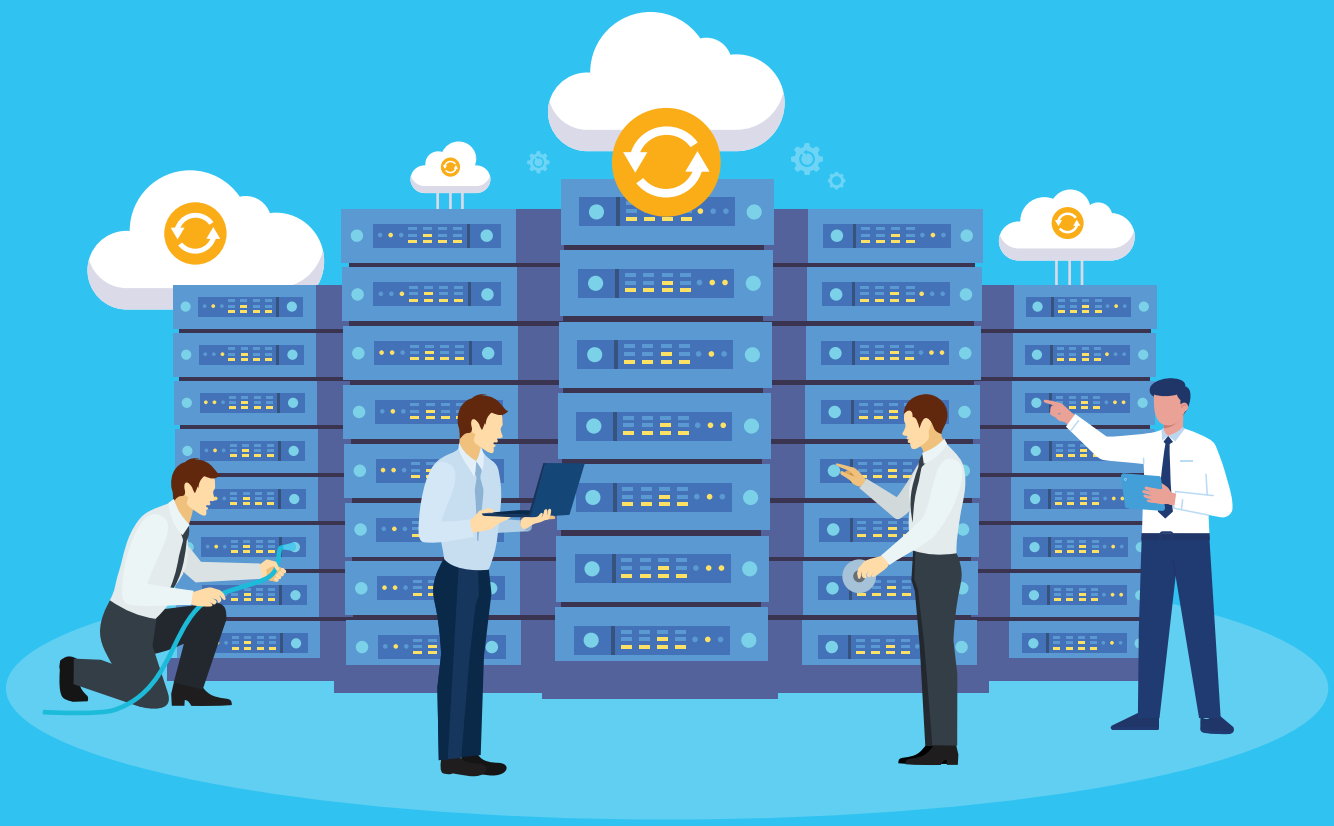
Section 4 Summary

Storage and backup systems have moved from afterthought to critical resilience infrastructure, especially in the age of ransomware. Leaders emphasize immutability, segregation, MFA, air-gapping, and — above all — routine restore testing.

Data governance becomes the organizing principle: if you don't know where data lives or how many copies exist, you can't protect it.

Takeaways:

- Immutable, isolated backups are mandatory, not optional
- Backup restoration testing is the real measure of readiness — quarterly partial tests and annual full restores for critical systems
- Storage platforms must be hardened like any critical system — encryption, access controls, patching, monitoring
- Cloud replicas must be architected for resiliency (multi-region, multi-zone)
- Cybersecurity and infrastructure reliability now converge — cyberattacks are disaster scenarios, and coordinated recovery is essential
- "Data is king" — understanding data lineage, movement, and duplication is central to resilient architecture



Section 5

Looking Ahead — Future of Infrastructure Security

What new trends or technologies do you think will most impact Infrastructure Security in the next 2–3 years?

Mark Thomson
Deputy Group CISO
Howden

Infrastructure security will continue to undergo significant transformation over the coming years, driven by emerging technologies and evolving threat landscapes.

AI-driven automation will play a dual role enhancing predictive threat detection, behavioural analytics, and rapid incident response, while also being exploited by attackers for automated campaigns and deepfake-enabled social engineering.

Zero Trust Architecture will continue to replace traditional perimeter-based models, embedding identity-centric controls and continuous verification across hybrid environments.

Quantum-resilient cryptography is gaining attention as organisations prepare for the disruptive potential of quantum computing, adopting hybrid cryptographic methods to safeguard sensitive systems.

Innovations such as IoT-enabled smart infrastructure, holographic management interfaces, and AI-powered observability platforms promise operational efficiency but introduce new attack surfaces, requiring robust security integration from the outset.

Rick Doten
Former VP Information Security
Centene

Certainly AI (LLMs), and Agentic AI; and tools that leverage these to work as autonomous robots to do work of humans. I talk to lots of cyber startups that are leveraging these for everything from observability, previsioning and de-previsioning of accounts, and vulnerability remediation. We've already been using it for vulnerability identification for years.

Gernette Wright
Former IT Security Officer - Americas
Schneider Electric

Without a doubt, AI will continue to make a tremendous impact on how we operate and do business. We've been talking for years about how AI could rapidly analyze vulnerabilities and generate new attack methods, and we're now seeing the first real examples of that with the recent publications from Anthropic. The attack was stopped, but imagine this running on an untethered system with no guardrails and no monitoring. I believe the next iterations will be even more sophisticated.

Looking ahead, I also believe quantum computing will make an incredible and disruptive impact. If we think back to Y2K, the amount of change required to prevent systems from crashing was a substantial effort.

Gernette Wright
Former IT Security Officer - Americas
Schneider Electric

The shift to post-quantum encryption will be similar, but on a much larger scale. If quantum delivers, and is able to break cryptography keys as theorized, many of the algorithms we rely on today will no longer be considered secure. This means organizations will need to upgrade protocols, rotate keys, replace cryptographic libraries, and redesign parts of their infrastructure to support quantum-safe standards.

Bob Turner
Former CISO
Penn State University & University of Wisconsin-Madison

A major area of both excitement and concern is AI in infrastructure and industrial environments.

Right now, I'm researching AI and how it can support infrastructure security – especially in domains like real estate, smart cities, and industrial operations. There's a huge amount of infrastructure and industrial security activity happening behind the scenes in those environments.

The core questions are: What should we hand over to AI to control? What must remain tightly regulated by humans? And how do we regulate access and "hours of operation" for systems AI is allowed to touch?

Most of the underlying controls already exist today; they've been in industrial environments for decades. The opportunity now is to: understand what those controls can do, use them to save energy and money, and use AI to orchestrate them safely and securely.

As organizations replace older systems, they should be asking: Does this new system have modern controls built in? Does it support strong security features and potentially AI-driven logic? And how secure is the overall design?

I'm not claiming to be a market analyst for every new product out there, but I'm convinced the future lies in trusted infrastructure models – where AI augments human operators, improves visibility and strengthens overall control – without replacing the need for sound governance and security design.

Erdal Ozkaya
CISO
Morgan State University

Non-human identities. We have thousands of employees, but we have millions of bots, scripts, and service accounts talking to each other. They don't sleep, they don't change passwords often enough, and attackers love them. Managing 'machine identity' is going to be the next big battleground.

Also, AI, both as a weapon and a shield. We are drowning in alerts. We need AI to help us filter the noise, so my human analysts don't burn out.

Mats Nygren
Former VP Information Security
U.S. Bank

I see the following developments that will reshape the domain of Infrastructure Security:

AI-driven automation and agentic systems create an entirely new class of infrastructure risks – AI agents will orchestrate workloads, call APIs, provision infrastructure, and chain actions in ways no traditional system ever did. AI will stress every seam in the infrastructure.

Organizations that can't secure these machine-driven workflows will likely face operational and security failures simultaneously.

Security teams will need to govern and continuously monitor agent identity, agent permissions, agent reasoning boundaries and explainability, and agent-to-agent trust.

Resilience will be regulated and require measurability – disclosure requirements and market pressure will make resiliency a board-level expectation.

Recovery time, identity hygiene, and cloud posture drift will become quantitative indicators of infrastructure security maturity.

Infrastructure security will be judged not only on how well it prevents incidents, but how well it recovers from them, in addition to driving value for the business.

What advice would you give to upcoming security leaders about understanding — and championing — infrastructure security?

Mark Thomson
Deputy Group CISO
Howden

For upcoming security leaders, the challenge is to position infrastructure security as a strategic enabler of resilience and business continuity rather than a purely technical function.

This means cultivating a forward-looking mindset anticipating threats like AI-driven attacks and quantum risks and aligning security strategies with organisational objectives.

Embrace Zero Trust and automation, embedding security into every layer of infrastructure from APIs to orchestration pipelines. Beyond technical expertise, develop strong communication and collaboration skills to influence priorities at the executive level and foster cross-functional alignment.

Promote a culture of proactive risk management by using quantitative models to justify investments and integrating cyber resilience into disaster recovery and continuity planning.

Finally, champion secure-by-design practices and continuous learning to stay ahead of regulatory changes and technological shifts. Leaders who combine technical depth with strategic foresight will not only protect infrastructure but also drive trust and innovation across the enterprise.

Rick Doten
Former VP Information Security
Centene

We have more than enough tools to detect problems and vulnerabilities. We now need to focus on how to streamline the fixing, which is largely still a manual process.

The Change management process can be automated and all the things humans do can be managed by AI, leaving humans to make the final judgement for critical actions.

Gernette Wright
Former IT Security Officer - Americas
Schneider Electric

These are the four areas I consider most important:

1. Understand and commit to the fundamentals, and don't overlook the basics. Security doesn't have to be flashy with the latest and greatest. Technologies will change, become more advanced, faster, and more powerful, but the basics will stay the same.

2. Get to know the business leaders and what's important to them, pain points, project horizons, priorities, etc. When I join an organization, I always want to take the sales product training. It's an easy way to learn how the business makes money.

3. Learn how to communicate with the non-technical people in the organization, not just the leaders. A lot of us came up through technical roles, which is great for translating requirements back to the technical teams, but may not be suitable elsewhere.

4. Culture tops my list. Without a good security culture, top-down / bottom-up, your program will struggle, and even if it succeeds, it may just be surface level. Maturing your technology stack to keep pace with the rate of change is a must, but it cannot replace the people in your organization. The end-user community represents the largest attack vector and has an incredibly important role to play.

Bob Turner
Former CISO
Penn State University & University of Wisconsin-Madison

There are some timeless fundamentals you must master: Know your data, know where it lives, know where it's supposed to go, and understand how it's protected along the way. That will never change. What does change is how we do it.

For those growing into infrastructure security leadership today, they're coming in with a much stronger technical baseline than many of us had years ago. Their challenge is to build on that while grasping the next wave of change – especially AI.

If you don't learn how AI works, how to ask the right questions, and how to integrate it responsibly into security programs – they'll fall behind.

They don't necessarily need to be a cryptography PhD, but they should understand the fundamentals of how modern systems secure data, the evolution from mechanical or simple-key-based systems to today's advanced mathematics, and the implications of new security tools and models.

Finally, the most important trait in cybersecurity is curiosity. If they stay curious, keep learning, and never lose sight of the data and its value to the business, you'll be well-positioned to grow into and succeed in an infrastructure security leadership role.

Erdal Ozkaya
CISO
Morgan State University

Don't just be a compliance officer with a fancy title. Get your hands dirty.

Understand how the plumbing works. You don't need to be a coder, but you need to know how a packet moves, how an API call works, and what a cloud architect actually does. If you can't respect the complexity of the infrastructure, you can't secure it, and the engineers won't respect you.

Girish Kulkarni
CISO
Aurionpro

Infrastructure security is evolving fast. Success requires more than technical skills – it demands vision and adaptability.

Think holistically – security goes beyond firewalls. It includes identity, APIs, automation, and resilience.

Embrace continuous learning – cloud and DevOps change the game every year. Stay ahead with cloud-native security, Zero Trust, and emerging tech.

Build relationships – security is a team sport. Collaborate with IT, DevOps, and business leaders for seamless integration.

Focus on resilience – assume breach. Design for rapid recovery and business continuity.

And finally, the future of infrastructure security is proactive, adaptive, and collaborative.

Section 5 Summary

AI — both defensive and offensive — will define the next era of infrastructure security. Leaders foresee rapid changes driven by LLM-enabled attacks, agentic automation, machine identity sprawl, and the disruptive future of quantum computing.

Infrastructure security will increasingly be measured not just by prevention, but by resilience and recovery speed. AI-driven orchestration will touch everything from pipelines to identity governance, forcing security programs to adapt.

Takeaways:

- AI and autonomous agents will reshape attack surfaces, requiring new governance for agent permissions, behavior boundaries, and explainability
- Quantum computing will force a generational shift in cryptography, requiring long-term planning and infrastructure redesign
- Machine identity management becomes a top-tier risk category, surpassing human identity in volume and complexity
- Resilience metrics (RTO, posture drift, identity hygiene) will become board-level indicators
- Trusted infrastructure models will emerge, where AI augments operators but requires strict guardrails
- Next-generation leaders must master fundamentals AND AI, combining technical literacy with strategic foresight

www.CISOpointOfView.com

Sponsored by core6