Protect and empower your business with Alcatel-Lucent Enterprise

Tackling the growing complexity of cyber threats and evolving regulatory requirements

Brochure

Alcatel·Lucent
Enterprise

Introduction

As organizations navigate major shifts in their businesses, security is one key area being upended. The rise of AI technologies has disrupted traditional security models, forcing a rethink of longstanding practices.

In response, our team of cybersecurity experts in network, communications and cloud solutions has joined forces to share key insights into the new risks enterprises face and how to add vital layers of protection to stay ahead.

The changing landscape of cybersecurity

The cybersecurity environment is defined by rapid technology evolution, more sophisticated threats and shifting regulations. Industry experts highlight three major trends now shaping enterprise cybersecurity:

1. The dual-edged role of artificial intelligence
2. The continuing rise of ransomware and supply chain attacks
3. The necessity for robust identity management within zero trust architectures

The dual-edged role of AI in cybersecurity

AI as a weapon for attackers

The malicious use of artificial intelligence has emerged as one of the most significant threats to enterprise security. Cybercriminals leverage AI to automate reconnaissance, craft hyper-personalized phishing campaigns and develop adaptive malware capable of evading traditional detection systems.

AI-powered tools analyze publicly available data to profile targets, generate convincing deepfake audio and video and exploit vulnerabilities with surgical precision. A notable example includes AI-generated phishing emails that mimic legitimate communication styles, increasing success rates by 40% compared to traditional methods. These attacks are further amplified by the commoditization of AI tools, which lowers the barrier to entry for less-skilled attackers.

Deepfake technology represents a particularly insidious application of AI, enabling threat actors to impersonate executives or trusted colleagues in real-time video calls to authorize fraudulent transactions or disclose sensitive information. In one documented case, a deepfake video of a CFO instructing a wire transfer resulted in a $25 million loss for a multinational corporation. Such incidents underscore the need for advanced authentication protocols and employee training to recognize synthetic media.

AI as a defense mechanism

Paradoxically, AI also serves as the backbone of modern cybersecurity defenses. Machine learning algorithms analyze vast datasets to detect anomalies, predict attack vectors and automate incident response. For example, AI-enhanced security systems can identify zero-day vulnerabilities by recognizing subtle behavioral patterns in network traffic, reducing mean detection times from weeks to hours. Gartner says organizations investing in AI-driven threat intelligence platforms experience 30 percent fewer successful breaches compared to those relying on legacy systems[1]. AI-driven systems are especially effective in identifying insider threats by monitoring user behavior and flagging unusual access patterns, which is increasingly critical in today's remote and hybrid work environments.

Regulatory and ethical challenges

The dual-use nature of AI has prompted stringent regulatory responses. The EU AI Act, enacted in February 2025, prohibits high-risk AI applications in areas like biometric surveillance and mandates transparency in algorithmic decision-making. Enterprises must now conduct third-party audits of AI systems, document data provenance and ensure ethical usage — a complex undertaking given the opacity of many machine learning models. Organizations are establishing cross-functional AI ethics committees to navigate this landscape and partnering with regulators to shape future frameworks.

1. https://www.gartner.com/en/newsroom/press-releases/2025-03-03-gartneridentifiesthe-top-cybersecurity-trends-for-2025

Escalation of ransomware and supply chain attacks

Targeting critical suppliers

Ransomware attacks have evolved from opportunistic campaigns to strategic operations targeting critical suppliers and service providers. The 2024 attacks on CDK Global and Change Healthcare demonstrated how compromising a single vendor can paralyze entire industries, costing billions in operational disruptions and recovery efforts. Today, attackers increasingly focus on software-as-a-service (SaaS) providers and cloud infrastructure firms, exploiting their centralized role in enterprise ecosystems. For example, a ransomware attack on a major cloud storage provider could lock thousands of businesses out of their data simultaneously, magnifying extortion leverage.

The proliferation of interconnected systems and insufficient supply chain risk management facilitates these attacks. Many enterprises lack visibility into their vendors' security postures, leaving them vulnerable to cascading failures. Gartner reports that 60 percent of organizations will face a significant supply chain breach by 2026, driven by third-party vulnerabilities in DevOps pipelines and IoT device fleets[1].

Ransomware-as-a-service (RaaS) ecosystems

The rise of ransomware-as-a-service platforms has democratized access to advanced attack tools, enabling even low-skilled criminals to launch sophisticated campaigns. RaaS operators provide customizable malware, payment portals and negotiation support in exchange for a share of ransoms — typically 20 to 30 percent. This model has led to a 150 percent increase in ransomware incidents since 2023, with average ransom demands exceeding $5 million per incident.

Modern ransomware employs AI-driven obfuscation techniques such as polymorphic code and time-delayed encryption to evade detection. Attackers also exfiltrate data before deploying encryption, threatening to leak sensitive information unless paid — a tactic known as double extortion. Enterprises are countering these threats with air-gapped backups, decentralized storage solutions and blockchain-based integrity verification systems.

Organizations will need secure technology across the board to prevent, contain and limit the impact of ransomware and supply chain attacks.

1. https://www.gartner.com/en/newsroom/press-releases/2025-03-03-gartneridentifiesthe-top-cybersecurity-trends-for-2025
2. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Identity management and the zero trust imperative

The machine identity crisis

As enterprises adopt generative AI, IoT and cloud-native architectures, machine identities — credentials for devices, APIs and automated workloads — have surpassed human identities in volume and risk. In 2025, Gartner identified unmanaged machine identities as a top attack vector, with compromised API keys and service accounts enabling 45 percent of cloud breaches[1]. To address this, companies are increasingly deploying certificate management tools that automate more frequent credential rotation, strengthening their least privilege policies to detect abnormal machine behavior in real time.

Zero trust architectures in practice

Zero trust frameworks, which assume no human or machine entity is inherently trustworthy, have shifted from aspirational goals to operational necessities. Implementation focuses on continuous authentication, micro-segmentation and encrypted communications. For instance, a zero trust network might require biometric verification for sensitive data access, isolate development environments from production systems and encrypt all east-west traffic within data centers.

The U.S. National Institute of Standards and Technology (NIST) reported in an evaluation of effectiveness that organizations adopting zero trust architecture [2] reduce breach impacts by 70 percent on average. Success hinges on integrating zero trust principles with existing infrastructure, a challenge for enterprises with legacy systems. Hybrid approaches are gaining traction, such as software-defined perimeters for on premises assets and cloud-native zero trust solutions.

Human factors and insider threats

According to the World Economic Forum, 95 percent of cybersecurity incidents occur due to human error. Phishing attacks leveraging AI-generated content bypass email filters 30 percent more effectively than traditional methods, while employees inadvertently exposing credentials in collaborative tools account for 25 percent of breaches. Insider threats are exacerbated by manual network access configuration errors and remote work, where personal devices and unsecured networks create entry points for attackers.

It has become essential to help users better protect themselves while easing the burden of increasingly restrictive security policies. For network and application administrators, automation of operations and active assistance through AI must provide the tools needed to protect against the consequences of potential misconfigurations.

The ALE approach for securing communications and network products

The Alcatel-Lucent Enterprise approach to security is to ensure that digital interactions are effective and compliant with industry-standard regulations. Digital technology is widespread, with the growing adoption of AI and IoT devices collecting data to support real-time alerts and future planning. Securing and strengthening the networks and communications that power today's business is vital to avoid service disruptions. ALE solutions for business communications and network infrastructure implement cybersecurity end-to-end because it's the only way to ensure security is applied comprehensively. This approach to cybersecurity helps enterprises and public institutions:

- Prevent cyberattacks by implementing cybersecurity in every aspect of product design to reduce the attack surface
- Protect against cyberattacks by implementing the latest security standards and best practices in all solution components to increase resistance
- React to cyberattacks by enabling swift and appropriate actions to limit impact and improve resilience, should an attack occur

As a manufacturer of hardware and software-based products, ALE's cybersecurity approach focuses on the areas described below to target potential vulnerabilities in the cyber threat landscape.

1. Secure by design

Historically, most solution designs were driven by the need for new features, and security was an essential, but secondary, consideration. With the changing landscape, traditional design priorities have reversed. Cybersecurity requirements must now drive solution designs. Hardware and software solutions that are secure by design take security into account during every step of product definition, development and delivery. All hardware and operating systems are hardened, denial of service (DoS) protection is built in, and solutions implement the best cybersecurity practices that are most important for the industry.

2. Zero trust network access security

Security strategies that provide trust based on a user's location inside the corporate firewall, the credentials they enter or the application or device they use are no longer adequate, even when multiple security mechanisms are combined. Today, no user, device or application should have implicit trust. The zero trust network access (ZTNA) security model helps organizations effectively counter ever-evolving threats. ZTNA does not trust any user, device or application, regardless of location. ALE enforces ZTNA by enabling role-based policy enforcement, location-aware access control (built-in Unified Policy Authentication Manager-UPAM) and dynamic segmentation across users, devices and applications (by default with Shortest Path Bridging-SPB, User Network Profiles-UNP) — whether managed or unmanaged.

3. Macro- and micro-segmentation

Macro- and micro-segmentation enable a granular and highly controlled approach to cybersecurity for all users, devices and applications that access the network. Macro-segmentation segregates users, devices and applications according to their functional domain so they cannot communicate with the elements in other macro-segments. For example, the unified communications and collaboration applications in one macro-segment cannot communicate with security technologies, such as CCTV cameras and door-lock systems, in a second macro-segment or the sensors and controls for lighting, heating and air conditioning in a third macro-segment.

Micro-segmentation defines how users, devices and applications within a macro-segment can interact with each other and is typically governed by specific security policies. For example, a surveillance camera should not be allowed to interface with a door lock, even though they are in the same security-related macro-segment.

4. End-to-end encryption

Employees, customers, partners and suppliers can be anywhere in modern organizations. And the solutions they use to communicate and collaborate may be installed in the building they work from, on the other side of the city or in a data center on the other side of the world. In every case, people must be able to securely and confidentially exchange information using voice, video and text. To ensure only conversation participants can access the information being exchanged, every conversation must be fully encrypted from origin to destination. That means each hardware and software element involved in end-to-end communications must have encryption mechanisms approved by security agencies built natively into them.

5. Security and privacy certifications and compliance with regulations

A few years ago, the most stringent security certifications and accreditations were only required for security products like firewalls or industries like defense. Today, security-specific standards must be applied to all technology products across all sectors. Verifying that recognized certifications and accreditations back up cybersecurity claims is critical.

Here are a few examples of compliance to look for:

- Global security and privacy standards, such as ISO 27001
- Industry-specific security and privacy standards, such as the Health Insurance Portability and Accountability Act (HIPAA) in the USA and Hébergeurs de Données de Santé (HDS) for health data hosting in France
- Regional security and privacy regulations, such as the General Data Protection Regulation (GDPR) and the NIS 2 Directive in the European Union

6. Continuous, specialized security testing

Like security standards, specialized security testing processes once reserved for security products are now mandatory in unified communications and collaboration solutions. Penetration tests are a prime example. These tests simulate cyberattacks to reveal security vulnerabilities so they can be proactively addressed before issues arise. To stay ahead of cyberthreats in an ever-evolving landscape, penetration tests driven solely by cybersecurity requirements must be performed continuously. Technology providers dedicated to helping their customers maintain maximum cybersecurity must provide the resources, tools and expertise needed to perform continuous penetration testing.

7. Data sovereignty

Data sovereignty has become a significant concern for most enterprises that must protect their intellectual property, preserve customers' trust and ensure a competitive advantage. With the adoption of new technologies such as the cloud and, more recently, AI, the openness of organizations' communications systems to the outside world has never been more important, and the security of network access is just as critical. Some companies will opt for a public cloud solution that meets their needs while limiting the internal attack surface of their information system. Others will opt for a more traditional approach, with unified communications applications hosted on their private network, either on-site or in a dedicated private cloud. Whatever the customer's choice, ALE can provide its products and services in all deployment contexts to ensure sovereignty over critical data.

8. Intelligent operations and security automation

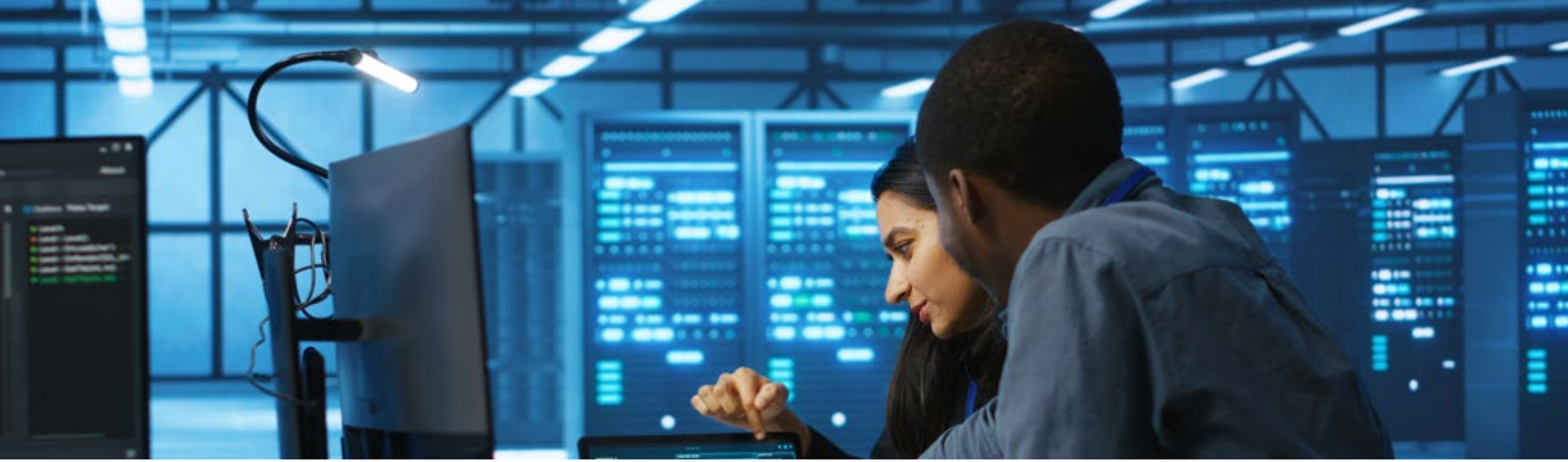
ALE's OmniVista suite and Network Advisor introduce advanced operational security through real-time monitoring, configuration audits and threat response automation. With embedded AIOps, network anomalies are detected proactively and guided remediations are provided, often requiring a single click to resolve QoE or compliance issues. This reduces human error, accelerates incident response and ensures policy compliance across complex environments.

9. Secure anywhere connectivity

ALE supports secure SD-WAN for distributed enterprises and remote work, combining network visibility, security and performance optimization, aligning with modern work-from-anywhere models. With MACsec encryption, data integrity and confidentiality are preserved across multisite WAN environments.

10. Trusted software supply chain

ALE applies rigorous measures to secure its software supply chain, including signed firmware images, secure boot processes, hardened operating systems and independent source code validation. These practices limit exposure to software-based threats and ensure trusted deployment environments.



Why ALE is your trusted supplier to secure your network infrastructure and business communications platform

While many technology providers emphasize cybersecurity, not all have the comprehensive expertise to implement end-to-end security. Alcatel-Lucent Enterprise goes above and beyond other providers to implement all required best practices for end-to-end cybersecurity.

We are committed to:

- Follow National Institute of Science and Technology (NIST) best practices and recommendations when performing risk assessments on new features and when implementing cybersecurity features, such as native encryption, in our products
- Apply ISO 27001 standards to all our solutions
- Support ZTNA, granular network segmentation and concrete security policies to reduce the risk of unauthorized activities
- Execute highly specialized, security-specific tests — such as penetration tests — on all our products
- Ensure our products achieve key industry certifications, such as HDS, HIPAA, the Family Educational Rights and Privacy Act (FERPA) and FIPS 140-2 for government and defense
- Take regional certifications into account for our products, such as CSPN by ANSSI in France, ENS in Spain, C5 in Germany and ANATEL in Brazil
- Comply with regional security and privacy regulations, such as GDPR, CRA and NIS 2 Directive in the European Union

As recognized cybersecurity experts, we contribute to European Union proposals for cybersecurity directives. We also leverage our expertise to help our customers choose and implement with the lowest TCO (30-50% off) the right mix of secure network and communications solutions for their needs and train their employees in cybersecurity best practices. Our comprehensive approach to Zero-Trust architecture enables our customers to demonstrate to their insurers that they are taking a proactive approach and generally benefit from a discount up to 20-30% on their cybersecurity insurance.

Conclusion

The cybersecurity trends of 2026 demand a paradigm shift in enterprise strategy. Organizations must reconcile the dual role of AI as both threat and defender, invest in resilient supply chains to withstand ransomware onslaughts and rearchitect identity management systems for a zero trust world. Regulatory compliance, ethical AI usage and cross-industry collaboration will be pivotal in mitigating risks. As attack surfaces expand with edge computing and IoT adoption, enterprises that prioritize adaptive defenses, employee education and proactive threat hunting will be best positioned to thrive in this volatile landscape.

The way forward requires technological innovation and the support and expertise of a trusted builder like ALE.

Learn more

To learn more, please visit ALE Security Solutions. If you would like to speak to one of our security experts, please contact us.

Alcatel·Lucent Enterprise