Discovery Report

March 2023

The State of Edge Security Report

Commissioned by

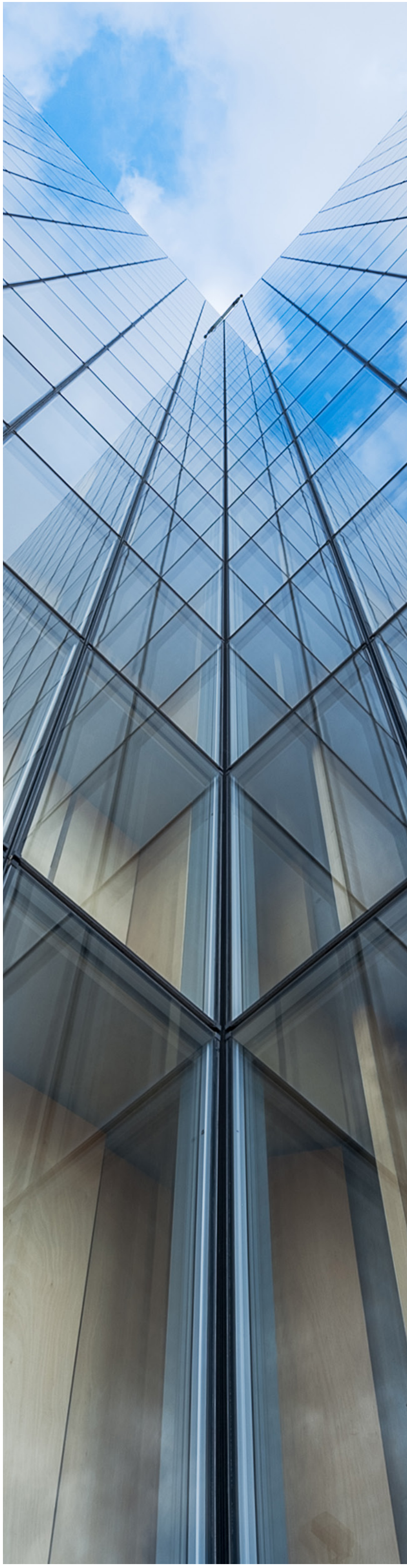
Red Hat

S&P Global
Market Intelligence

Introduction

Edge computing is evolving from limited use in a few industries to the next generation of decentralized infrastructure supporting digital transformation and latency-sensitive workloads that require powerful and localized computation. Despite its critical nature, maintaining a cohesive strategy and resilient security posture can be a challenge for large enterprises expanding their infrastructure footprint beyond the secure environment of a datacenter.

The State of Edge Security Report provides a benchmark for current edge deployments in terms of the scale of projects, investments, use cases and endpoints, as well as possible efficiencies from scaling edge initiatives effectively and security challenges from this immense and expanding attack surface area. The report addresses the top security threats facing the edge with comprehensive insights into the edge security stack required to support edge projects and the need to develop an edge ecosystem.



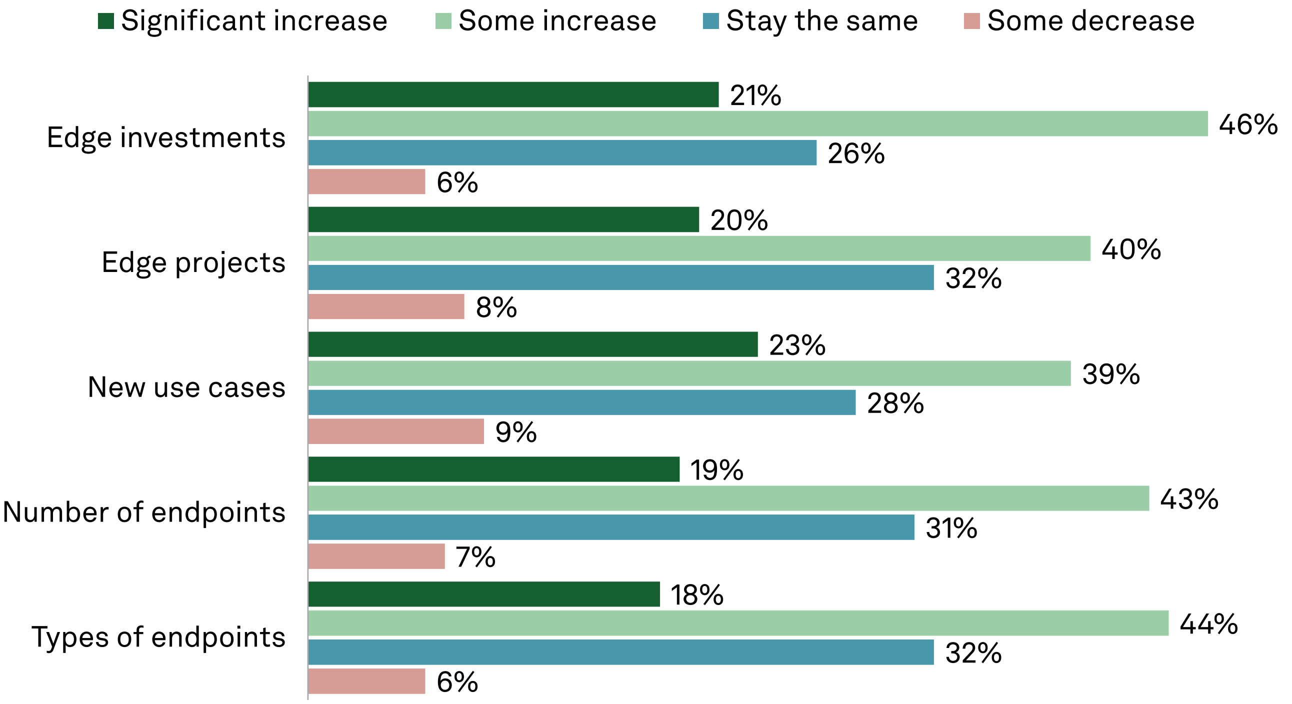
Key findings

- Edge deployments are increasing in scale across investments, projects, use cases, endpoints and types of endpoints.
- Security is the top challenge cited by enterprises with edge deployments.
- Risks to edge systems such as cyberattacks and from edge systems due to vulnerabilities and misconfigurations are on the rise.
- Enterprises effectively scaling edge deployments can attain efficiencies and massive cost savings as rollouts span hundreds of edge servers and thousands of IoT devices. However, scaling also expands the attack surface for cyber criminals.
- Enterprises value a comprehensive stack of edge security capabilities across supply chain, network, data, physical device and endpoints.
- Forming an edge ecosystem of trusted partners and software vendors is necessary for ensuring operational resiliency and long-term project success.

Edge deployments are expanding and maturing quickly

The edge is a strategic growth pillar for enterprises to generate new revenue and reduce costs. More than two-thirds (68%) of companies surveyed plan to increase their edge investments by "some" or "significant" amounts in the next two years. These investment dollars are funding growth for existing and new edge projects, use cases and endpoints.

Figure 1: Steady growth across the edge



Q. How will your edge deployments develop over the next two years?
Base: All respondents (n=302).
Source: S&P Global Market Intelligence and Red Hat edge security report.

Edge projects enable innovative use cases and diverse endpoints that use this increasingly decentralized infrastructure. These use cases range from externally facing applications that could generate revenue to internally focused cost-saving ones. For example, customer experience optimization and supply chain management/logistics are top-three externally facing edge computing use cases, according to 46% and 35% of survey respondents, respectively. Top internally facing use cases include private wireless 4G/5G network software enablement (cited by 20% of respondents) and industrial process management/automation (20%).

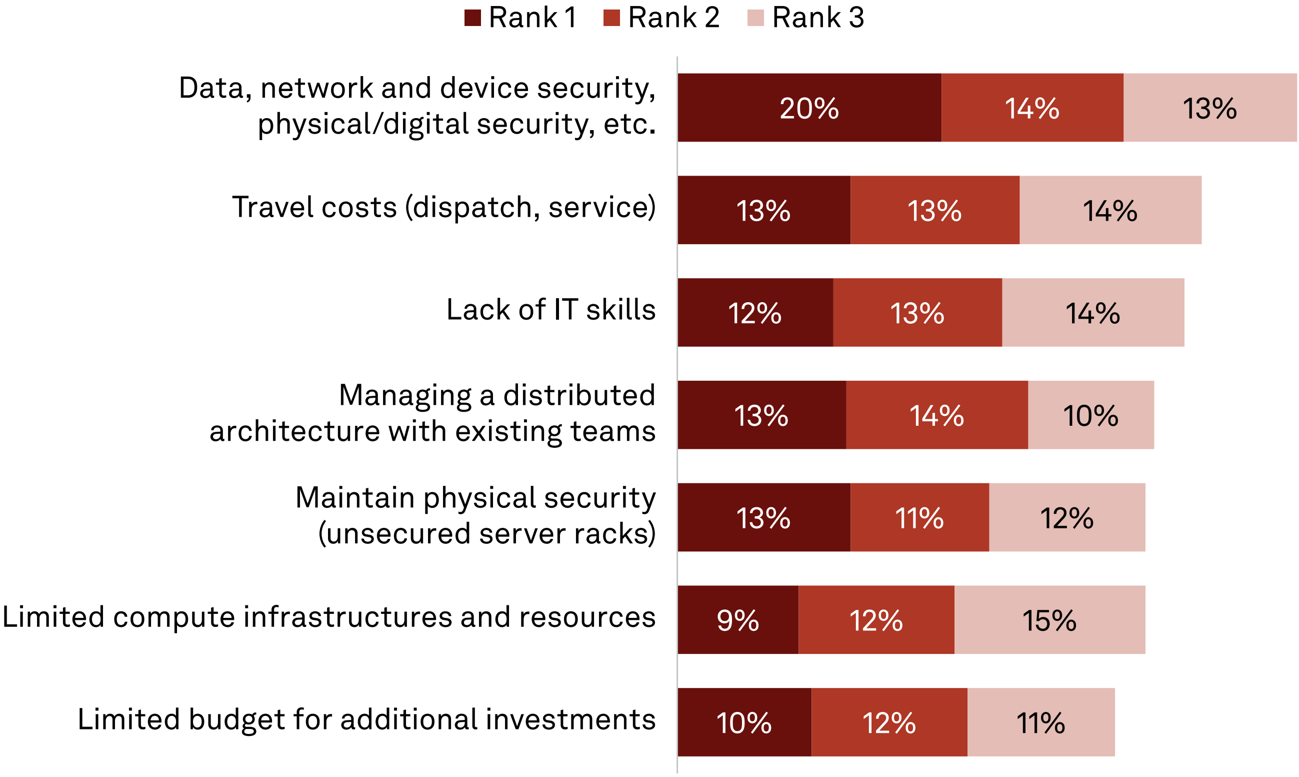
Observations

Funding this growth requires senior leadership buy-in to generate the necessary financial backing, alignment across stakeholders and strategy behind edge-enabled digital transformation strategies. While there may be friction from competing priorities, enterprises shouldn't limit coordination and participation to a few specific roles because the edge can benefit a variety of personas. Survey respondents cite a broad swath of the C-suite as the key stakeholders of their edge computing strategy, including chief digital transformation officer (14%), chief information officer (14%), CEO (13%), chief procurement officer (13%), chief digital officer (12%), chief information security officer (12%), COO (11%) and chief technology officer (11%).

Security is the top edge deployment challenge

Our research further supports the notion that there is a paradox in edge security; it is deemed a massive technical challenge and threat for enterprises but also an opportunity. The attack surface area is unquestionably expanding; according to 451 Research's Voice of the Enterprise: Edge Infrastructure & Services, Use Cases 2022, within two years, nearly a quarter of organizations will have more than 100 sites with dedicated edge infrastructure. Maintaining a resilient cybersecurity posture with this edge infrastructure buildout creates challenges across both physical and digital systems.

Figure 2: Edge deployment challenges



Q. Across your edge computing deployments, what would you consider are your biggest challenges?
Base: All respondents (n=302).
Source: S&P Global Market Intelligence and Red Hat edge security report.

Nearly half of decision-makers (47%) say that data, network and device physical and digital security is among their biggest challenges in edge deployments. As with broader IT, cybersecurity has become the top enterprise challenge in edge deployments as digitalization continues to open the attack surface. Enterprises are wrestling with a need to expand their infrastructure footprint and effectively secure not only the infrastructure itself, but also the larger number of IoT endpoints that are connected to it. This is an area where many believe the adoption of new operational patterns, such as cloud native and DevOps, can improve their security posture alongside their operational efficiency.

Observations

While the edge can present innovative use cases driving long-term growth, underinvestment in security can quickly undermine the benefits of any edge initiative. Those who view the edge as an opportunity to update and upgrade their cybersecurity systems will lessen the growing risks this expanding infrastructure creates.

Risks both to and from edge systems are on the rise

Cyberattacks from both inside and outside the organization pose the greatest risk of security incidents with edge systems. Whether for personal, financial or geopolitical reasons, malicious insiders stealing sensitive data and intellectual property is a growing threat. However, nearly a quarter of organizations keep their edge computing equipment in an unsecured IT rack/enclosure, according to 451 Research's Voice of the Enterprise: Edge Infrastructure & Services, Use Cases 2022.

Criminal organizations and attackers funded by nation-states see the industrial base, critical infrastructure and companies of all forms as highly valuable targets. Being composed of hundreds of remote servers and thousands of IoT devices, the edge presents an attractive target for cybercriminals to expand their armies of bots for activities such as denial-of-service attacks and crypto mining. The data itself is a valuable target, as is the ability to hold an operational control environment for ransom, potentially costing millions for recovery and impact on operational downtime.

Figure 3: Edge system security incident risks

Greatest risk of security incident with/from edge systems

(Respondents who cited critical/high edge security risk)

1. Cyberattacks (malicious insiders) (70%)
2. Cyberattacks (outside attackers) (69%)
3. Vulnerabilities (68%)
4. Misconfigurations (62%)
5. Delays in patching/updating (56%)
6. End of life/unsupported hardware (52%)
7. Supply chain/third-party security (46%)
8. Nation-state actors (45%)

Feedback from edge practitioners

Cyberattacks (attackers): "Cyberattacks by outsiders and insiders are very difficult to predict and deal with... For the outside hackers, all we can do is hope they don't get smarter than any available technology. Actually, the "best" hackers are ahead of the existing techniques of securing systems."

CIO, energy/oil and gas, 1-5,000 employees

Vulnerabilities: "Known/unknown vulnerabilities represent a critical risk due to our current inability to quickly mitigate exploitation."

Global head of cloud infrastructure,
pharma/biotech, 50-100,000 employees

Delays in patching/updating: "Delays in patching can make systems susceptible to a variety of compromises from ransomware to viruses, and even instability/incompatibility with certain applications."

Infrastructure services manager,
manufacturing, 1-5,000 employees

Q. How would you rate the following items that increase your risk of a security incident with/from your edge systems? (critical/high edge security risk).
Q. What are your greatest edge threats?
Base: All respondents (n=302).
Source: S&P Global Market Intelligence and Red Hat edge security report.

Many legacy edge systems are approaching their end of life and/or may not have the compute resources or cost efficiencies to support frequent software updates and patches. These older edge systems with outdated operating systems or vulnerable applications are a possible attack path for cybercriminals. Even short gaps in updates can expose vulnerabilities and misconfigurations because edge systems often have minimal access to central IT governance and policies.

Incorporating security earlier into the application development pipeline, or “shifting security left,” is a possible solution but also brings challenges. These include a lack of security gates at the development stage, meaning that security issues aren’t caught until an application is close to deployment, when it’s too late or too costly to fix (cited by 63% of respondents as a top-three challenge). Respondents are also concerned that developers are not equipped with security tools, and traditional tooling fails to protect cloud-native apps at the edge (61%).

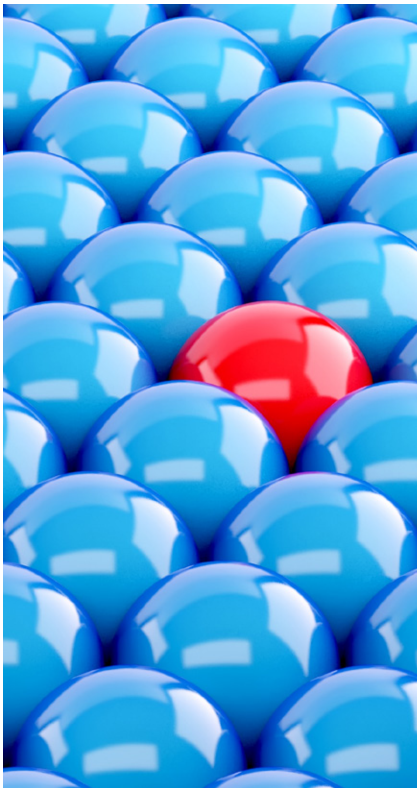
Finally, cybercriminals are increasingly looking at weak links in both the digital and physical supply chains. The software supply chain is coming under increasing pressure as attackers shift their focus to indirect pathways into targets’ operations. A compromised software supplier or software library is much more difficult for a target company to detect. Hardware supply chains are also coming under attack, although doing so is more complicated to achieve. In edge computing, where software and hardware are more tightly coupled than in other areas of computing, attacks are more complex, and protections must be much more robust to effectively counter them.

Imprudent trade-offs, in which organizations have mistakenly prioritized connectivity, digital experiences or ease of use over security, have led to well-publicized incidents. Cybercriminals have compromised poorly secured devices and their supporting environments to wreak havoc, resulting in lawsuits, fines and regulatory action.

Observations

Cyberattacks present a growing risk to enterprises, and the expansion of edge infrastructure presents a greater attack surface. Enterprises need to assess their current cybersecurity posture for risks from vulnerabilities and misconfigurations; safeguard edge systems from being compromised by a range of internal and external threat actors; and invest in tools and technologies to maintain and enforce centralized governance and policies.

Scaled out edge infrastructure brings larger security concerns



Edge infrastructure is becoming an area of substantial investment and is starting to rival spending in other infrastructure venues, such as public cloud. A major driver of this edge infrastructure is the growth of IoT devices and the need to manage the significant data volumes they generate and critical applications they enable. There are some notable floors and ceilings that enterprises should prepare for as they provision edge servers to support the scaling of IoT device counts. While scale is important, rapid expansion brings significant security concerns. The greater number of devices, supporting edge servers and their interconnections presents a larger attack surface for attackers. Securing them effectively not only becomes a more critical concern, but also a complex problem. The ability to build on common platforms with consistent security characteristics and capabilities can help organizations manage security at scale by reducing operational complexity. Having a common foundation gives device and server teams a shared set of capabilities without having to translate security policies and controls across these two domains.

Figure 4: Expanding edge infrastructure increases attack surface

	IoT devices deployed							
Edge servers deployed	1-99	100-249	250-499	500-999	1,000-4,999	5,000-9,999	10,000-25,000	25,000+
500+	0%	0%	0%	0%	11%	40%	100%	100%
100-499	0%	0%	0%	0%	50%	60%	0%	0%
51-100	0%	0%	28%	37%	39%	0%	0%	0%
26-50	0%	23%	34%	32%	0%	0%	0%	0%
11-25	2%	40%	38%	32%	0%	0%	0%	0%
6-10	55%	17%	0%	0%	0%	0%	0%	0%
1-5	43%	20%	0%	0%	0%	0%	0%	0%

Q. How many remote or edge servers would you estimate your organization has deployed today?
Q. How many IoT devices would you estimate your organization has deployed today?
Base: All respondents (n=302).
Source: S&P Global Market Intelligence and Red Hat edge security report.

Our analysis above shows how expansive these edge deployments are becoming; however, enterprises are still at varying points of maturity. We've found that the vast majority of deployments with fewer than 100 IoT devices have fewer than 10 edge servers, whereas deployments with more than 10,000 IoT devices have at least 500 edge servers.

There are potentially millions of dollars in IT capital expenditures that are exposed to cyber risks, depending on where the organization lies on this spectrum. These are risks that can widen and create costly operational security gaps as organizations scale. For example, the difference between managing 250 IoT devices with 50 edge servers (deployment A) versus five edge servers (deployment B) would create IoT-device-to-edge-server ratio of 5:1 (A) versus 50:1 (B). If the company were to add another 1,000 devices and maintain the ratio, deployment A would have to add 200 edge servers, whereas deployment B would only have to add 20 to support this scaling.

Security management practices that could support a small number of servers and devices with configuration, vulnerability and patch management on an individual basis will be quickly overwhelmed at larger scale. To operate at scale, security teams require operating environments that deliver a common set of security characteristics across devices and servers that give them the ability to build common security policies and practices. It simplifies the automation of security operations, as well as reduces the chance for errors caused by misconfiguration.

The variations in the device-to-server ratio highlight the potential for additional challenges: Enterprises that over-provision edge servers may be missing opportunities to achieve efficiencies that larger scale could provide and find themselves contracting deployments over the long term to contain management costs. Under-provisioning edge server resources could create bottlenecks in IoT device control capacity and data throughput at these sites, potentially creating security vulnerabilities if patching operations cannot be completed in a timely fashion.

Observations

The ratio of edge servers to IoT devices isn't an exact science because not every edge use case will be IoT-centric, but there are very few in which IoT won't play an increasingly prominent role. Enterprises need to invest in strategic planning and establish operational and technological best practices to operate efficiently, effectively and securely at scale. Understanding the impacts of physical (i.e., IT truck rolls) and digital (remote service) operational challenges reinforces the importance of leveraging technologies from a trusted edge technology ecosystem, which can alleviate scaling costs, drive edge efficiencies and enforce operational resiliency.

Enterprises value a comprehensive set of edge security capabilities

The emerging edge security stack boasts both new and existing security technologies purpose-built for this decentralized infrastructure. Six pivotal edge security areas for IT teams to consider are supply chain, data, network, threat detection, endpoint and device. When our survey asked for respondents' priorities, there was minimal statistical significance across these six categories. This supports the notion that decision-makers believe they all play a critical role and are required to secure a complex and growing edge infrastructure.

Figure 5: The edge security stack

Internet edge

Supply chain

- Governance and access control
- Attestation
- Vulnerability management
- Integrated development environment
- Software bill of materials
- Configuration management

Enterprise and network edge

Data

- Data loss prevention
- In-transit encryption
- Access control
- Sovereignty/locality
- In-use encryption
- At-rest encryption

Network

- Network validation
- Network access control
- Network segmentation/isolation
- Network security observability

Threat detection

- Intrusion detection
- Onboarding to management platform

Device edge

Physical device

- Identity
- Remote deployment/replacement
- Trust/authentication
- Physical access

Endpoint

- Access control
- Encryption

Source: S&P Global Market Intelligence and Red Hat edge security report.

To reiterate, the ever-growing and increasingly connected digital and physical supply chain presents a sizable risk to edge sites, such as those in close proximity to suppliers upstream or to customers downstream. Systems that maintain governance and access control are key to ensuring the integrity of digital and physical touchpoints across edge systems. The ability to provide device and data attestation across the supply chain can reduce the risk of tampering and mitigate configuration errors. Tools are emerging that better identify and manage vulnerabilities across networks and assets, which increasingly include parts from external software suppliers and open-source projects. The software bill of materials (SBOM) is an emerging concept being driven by federal mandates for companies to start understanding the linkage of vendor components that make up software they use and the associated risks from using it. SBOMs can help enterprises comprehend the full set of software components that are used in their environments and prioritize remediation when new vulnerabilities are identified.

Data is a key asset that the edge unlocks, but it is also a lucrative target for cybercriminals and malicious insiders. Protecting data's integrity from the source through the network as it hits multiple venues for computation is paramount, but it is also a challenge because data is constantly in motion to and from IoT devices and other edge systems. Encryption is the top technique for ensuring the data is protected from interception or alteration by malicious actors when it is at rest, in use and in transit between its creation at the edge and its use and storage. Data-loss-prevention tools provide another layer to mitigate risks to this sensitive data at the edge from unauthorized or accidental disclosures. This is a critical issue in compliance-sensitive industries (e.g., healthcare) where safeguarding data is strictly enforced by regulatory bodies, and in these instances, it is a common requirement that data stay at the edge or locally to comply with data sovereignty mandates.

Networks are increasingly complex and diverse, blending older and newer architectures (e.g., SD-WAN) to transmit data to and from resource-constrained edge devices. Network validation ensures edge devices are compliant with the network's standards and can help IT identify problematic devices or suspicious activities. Network access control can provide a necessary layer to limit external and internal access to other services via the network. Network segmentation isolates networks within a cluster environment to keep attacks from spreading laterally and compromising adjacent systems. The more quickly and accurately IT can detect network threats, the better equipped the team will be to mitigate any associated risks and prevent new ones.

Setting up physical edge devices and servers in geographically dispersed areas requires a security-first mindset. Onboarding devices securely can be a challenge, but the FIDO Alliance Device Onboard specifications can expedite and ease the setup process. Managing and authenticating the identification of edge devices and servers is also critical to ensure only authorized systems are granted access to the network. Remote management of edge servers and IoT devices is key to lowering operational costs to service these systems in the field, as well as ensure they are updated with the latest firmware, security credentials and other policies from IT. With the expansive and global mix of edge deployments, IT should operate under the mindset that these physical systems are at risk of being compromised and take stringent measures such as “always on” encryption and encrypting data in memory and in storage.

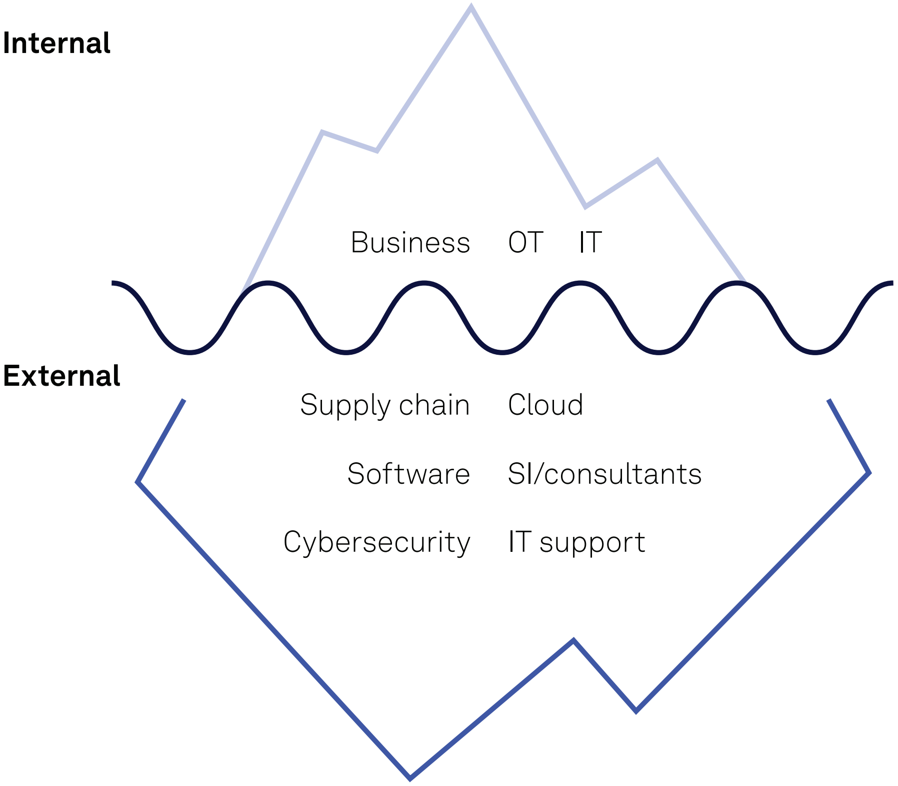
Observations

There isn’t a silver-bullet technology for edge security from a single vendor that can cover this expanding and complex stack. Enterprises that are leveraging existing edge infrastructure or opting for a refresh will need to intensively evaluate vendors in each of these categories and prioritize those with demonstrated success, innovative features, proper certifications, partnership ecosystems, and training and support programs. The edge requires a multi-layered and comprehensive edge security architecture. Forward-thinking enterprises can leverage it as an opportunity to update and upgrade systems and improve operational resiliency.

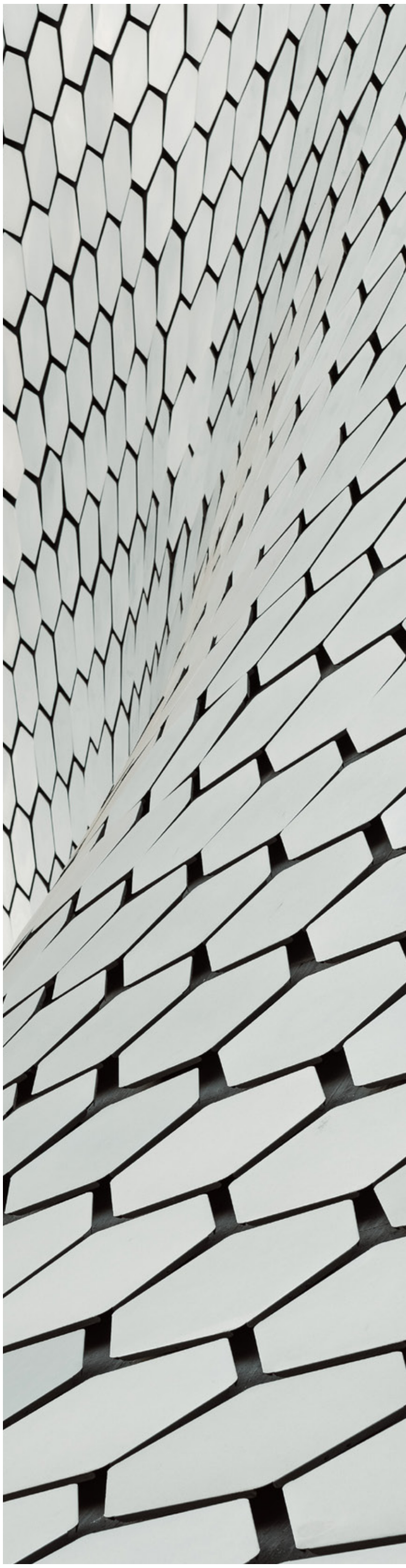
Conclusion

Edge capabilities are being put into real-world use by organizations on a massive scale, presenting an opportunity that they can't ignore. But this impetus comes with challenges, particularly in security, and that's an area where organizations see the ability to use new, more efficient technologies, such as cloud native, to gain a competitive advantage. Partnering with leading providers to help manage this rapidly expanding and critical edge environment is paramount to maintaining security across it.

Figure 6: Edge ecosystem



Source: S&P Global Market Intelligence and Red Hat edge security report.



Simply put, it takes an edge ecosystem to scale edge deployments and ensure a resilient security posture that can support it. As with an iceberg, enterprises can see what’s “above the water line” in terms of orchestrating internal stakeholders and necessary investments in their edge strategies. However, many overlook what’s “below the water line”: initial and ongoing investments in external partners and technologies that support scaling. Aligning with sound edge security principles, embedding repeatable processes and investing in best-in-class security capabilities from cutting-edge and trusted providers are necessary initial investments that will drive even greater long-term impact when at scale.

Methodology

The findings presented in this report draw on a US survey fielded in Q4 2022. The survey targeted 302 edge decision-makers/influencers in companies with more than 1,000 employees and greater than $500 million in annual revenue. The study prioritized the following industries: automotive, communications, energy/oil and gas, finance, government, healthcare, insurance, IT and services, manufacturing/industrial products, retail, telecommunications, transportation/logistics and utilities. This report also draws on contextual knowledge of additional research conducted by S&P Global Market Intelligence.

About the authors

Eric Hanselman

Principal Research Analyst

Eric Hanselman is the Principal Research Analyst at S&P Global Market Intelligence. He has an extensive, hands-on understanding of a broad range of IT subject areas, having direct experience in the areas of security, networks, application and infrastructure transformation and semiconductors. He coordinates industry analysis across the broad portfolio of 451 Research disciplines, contributes to the Information Security and Cloud Native Channels, and is a member of the Center of Excellence for Quantum Technologies.

David Immerman

Consulting Analyst

David Immerman is a Consulting Analyst for S&P Global Market Intelligence's TMT Consulting team based in Boston. Prior to S&P Market Intelligence, David ran competitive intelligence for a supply chain risk management software startup. He spent nearly four years at an industrial software vendor providing thought leadership and market research on technologies and trends in manufacturing. Previously, David was an industry analyst in 451 Research's Internet of Things channel for three years, primarily covering the smart transportation and automotive technology markets. He holds a bachelor's degree in Business Administration from Marist College.

Jay Lyman

Senior Research Analyst, Cloud Native and DevOps

Jay Lyman is a Senior Research Analyst with the Cloud Native and Applied Infrastructure & DevOps Channels at S&P Global Market Intelligence. He covers infrastructure software, primarily private cloud platforms, cloud management and enterprise use cases that center on orchestration, the confluence of software development and IT operations known as DevOps, Docker and containers. Jay's analysis encompasses evolving IT operations and software release models, as well as the technology used to create, deploy and support infrastructure and applications in today's enterprise and service-provider markets. Key areas of research also include OpenStack, PaaS and enterprise end users.

About this report

A Discovery report is a study based on primary research survey data that assesses the market dynamics of a key enterprise technology segment through the lens of the "on the ground" experience and opinions of real practitioners — what they are doing, and why they are doing it.

About S&P Global Market Intelligence

S&P Global Market Intelligence's Technology, Media and Telecommunications (TMT) Research provides essential insight into the pace and extent of digital transformation across the global TMT landscape. Through the 451 Research and Kagan products, TMT Research offers differentiated insight and data on adoption, innovation and disruption across the telecom, media and technology markets, backed by a global team of industry experts, and delivered via a range of syndicated research, consulting and go-to-market services, and live events.

CONTACTS

Americas: +1 800 447 2273
Japan: +81 3 6262 1887
Asia Pacific: +60 4 291 3600
Europe, Middle East, Africa: +44 (0) 134 432 8300

www.spglobal.com/marketintelligence

www.spglobal.com/en/enterprise/about/contact-us.html

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global keeps certain activities of its divisions separate from each other to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain nonpublic information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its websites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.