Living on the Edge: Building and Maintaining Security at the Network Edge

Edge computing is still new enough that security teams have to figure out for themselves how to secure it. Best practices haven't been written yet.

INSIDE:

Brought to you by informa tech

Next

FEATURE

Living on the Edge: Building and Maintaining Security at the Network Edge

Edge computing is still new enough that security teams have to figure out for themselves how to secure it. Best practices haven't been written yet.

By George V. Hulme, Contributing Writer, Dark Reading

There has always been a push and pull relationship between centralized computing and distributed computing, from the age of mainframes to distributed computing ushered in by PCs, to the rise (and recentralization of data and applications) of the cloud. Today, with the growing popularity of edge computing architectures, compute power and data are fragmenting again. In the months and years ahead, more security teams will have to understand the security implications of edge computing or their organizations will likely pay a high price.

Edge computing — which is simply compute power, applications, and storage shifted closer to the sources of data — is an architecture undergoing radical growth thanks to increased bandwidth speeds and availability, the increased power of Internet of Things (IoT) devices and sensors, and the vastly improved methods for managing massive amounts of telemetry and data. Edge computing promises to speed on-site decision-making and better enable digital transformation efforts. It also dramatically increases the enterprise attack surface.

"Edge computing use cases apply to every industry," says Kieran Norton, infrastructure security leader at consultancy Deloitte & Touche LLP. "These technologies enable things to happen that were not really viable in the past."

Get Security Right This Time

According to market research firm Grand View Research, the edge computing market is expected to reach $61 billion by 2028 and grow annually by just over 38%. During this period, the demand for edge servers will make it the fastest-growing server segment. These edge systems will help satisfy the demand for increased edge intelligence for most verticals, from manufacturing and healthcare to retail and supply chain management to smart-building and smart-city management.

While edge computing will help drive innovations, it will also increase the enterprise attack surface and bring more ways for attackers to infiltrate enterprise systems through operating systems, applications, network layer attacks, and data exfiltration. "I think it's also important for CISOs to envision the enablement capabilities of the edge and see the opportunity and not just the threat," says Norton. "They have to see and address the threats, but historically, there has been lots of resistance to change, such as with the cloud and the iPhone — and a lot of those scared teams are now playing catch-up. Let's not play catch-up this time."

The challenge of securing edge computing will be high, as there are few general edge computing enterprise best practices established, let alone security best practices. "Everything is its own unique beast for every company, and that's where many challenges come from. Teams are not going to be pulling solutions off the shelf. They're not going to get a total package product with cybersecurity built-in. They're going to have to engineer that in themselves," Norton says.

In many ways, edge computing resembles how cloud computing looked about a decade ago. There were many capabilities and new tools that enterprise teams didn't yet understand how to use. Today with the edge, as with cloud computing back then, success will require a lot of deep security talent to learn how to best secure these systems. "It will be years before enough patterns emerge so that, no matter what vertical, packaged solutions and best practices emerge to tackle the edge security challenge directly," Norton says.

> **"Historically, there has been lots of resistance to change, such as with the cloud and the iPhone — and a lot of those scared teams are now playing catch-up. Let's not play catch-up this time."** —Kieran Norton, Deloitte & Touche

The first decision most enterprises will have to make, which will substantially affect security strategy, is whether a system belongs at the edge or within a cloud.

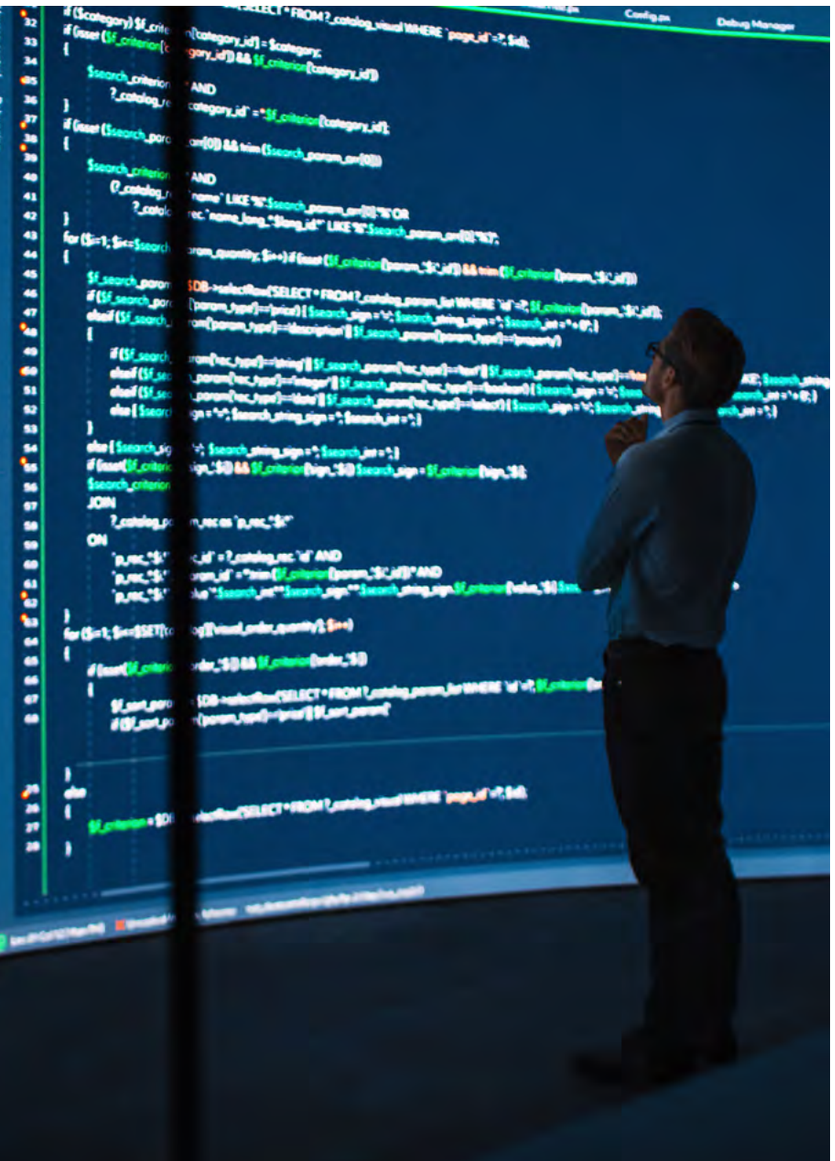
A Question of Architecture: Edge vs. Cloud

When looking at any use case, one of the first architectural decisions is whether heavy computational lifting computing will occur within an edge or a cloud. "I think the answer here is optimized based on the use case," says Michele Pelino, an analyst at Forrester. "What is the enterprise trying to achieve with a particular use case or scenario? That decides what needs to happen at the edge or what needs to happen within the cloud. And it will help determine the applications necessary, and what kinds of functionality need to happen regarding data analysis."

"This decision always comes down to how much data are you moving, and where," says Andy Ellis, operating Partner of YL Ventures and advisory CISO at Orca Security. "When it's too expensive to move data, it will be a cloud system. If timing is that essential, it leans toward the edge," he says.

"Such immediacy also defines what types of capabilities and functionality are needed to happen. These are the starting points," says Pelino. "Other use cases could be focused on augmented virtual reality or connecting drones or robotics within critical environments. Or differ-

Previous Next



ent types of use cases that help to personalize retail customer experiences. The personalization at the edge will differentiate that experience for that individual. All of that will happen at the edge."

Assessing the Attack Surface

When it comes to securing these devices, systems, and data, the challenges will require nearly every aspect of a security program to both be extended to the edge and to scale considerably: identity and access, application security, data security and privacy, threat detection, vulnerability management, patching, configuration management, business continuity, and disaster recovery. "Generally, enterprises are going to have a much more broad and complex attack surface," Pelino predicts.

Where should CISOs start their efforts to secure the edge? Typically, the experts we interviewed suggest that the first step is to threat model the use case for the edge computing and the technical architecture. "Each of these layered, fragmented edge environments become their own starting point for a security assessment," Pelino says.

To successfully secure these environments, each layer must be evaluated for risk: networks, devices, applications, data, and business use case. Those interviewed agree that the task won't be easy. Jason Hicks, field CISO at security consultancy Coalfire, says a significant challenge for CISOs will be inventorying the sheer proliferation of edge computing devices and locations — each with potentially sensitive data or applications running that are mission-critical to the business. "There will also be challenges with getting your security tooling and processes to quickly scale and will require some refinement," Hicks says.

Echoing the lessons learned from secure software development, security teams must be brought in early in the planning and edge computing architecture discussions. "These types of [security] conversations have to happen early and with business use cases in mind. When discussing these use cases, the requirements come from other organizational stakeholders who want to deploy connected experiences in remote environments. You need to make sure that the team is thinking about security from the very beginning," Pelino says.

This risk is organizations will repeat the same mistakes they made with the rise of distributed computing, Web-based e-commerce, and cloud computing.

Focus on Data, Devices, Applications, and Networks

The security difficulties surrounding user access, networks, IoT devices, services, and data are well known. The same types of incidents that plague on-premises and cloud systems, such as credential-based attacks, ransomware, and other malware, will also affect edge environments. As will data exfiltration, destruction, and manipulation, as well as

denial-of-service attacks and other disruptions that target edge systems.

It's essential that CISOs and organizational business teams focus on each layer.

Mind the Data

One of the first objectives is to protect the data collected and analyzed at the edge, as well as the data that is transmitted back to the cloud or data center.

In addition to ensuring data collected and generated at the edge doesn't get exfiltrated, it's also essential to think about the integrity of the data and any privacy concerns and regulatory mandates within the local (to the edge) geography. "The first question around edge data is data providence," says YL's Ellis. "How do you know that the data that you processed actually came from where you thought it did? And when you summarize and send that data back to the core, how do you know that data actually is what you think it is?" There are many reasons criminals, hacktivists, nation-states, and others may want to tamper with an organization's data, ranging from the sheer adventure to possibly destroying telemetry to affect production efforts.

The other aspect of data security at the edge is jurisdictional and regulatory. "How do you make sure that you're following the rules of all the locations? Imagine your edge is hospitals. The hospitals in Europe have to follow different rules than the hospitals in the US when it comes to moving data around. What are the standards of anonymization that need to be done for the data? What level of privacy will make your customers happy?" Ellis asks.

"How do you know that the data that you processed actually came from where you thought it did? And when you summarize and send that data back to the core, how do you know that data actually is what you think it is?"
—Andy Ellis, YL Ventures and Orca Security

Norton explains that edge computing security isn't just about risks. It can also be an opportunity to reduce the risk to data. "A security advantage of edge, if you're processing data that matters and then you're disposing of it immediately, is that it actually provides an opportunity to minimize your attack surface," Deloitte's Norton explains. "On the flip side, if you're not doing disposing of the data immediately, and you're storing massive amounts of it, then you are creating substantial risk for yourself."

Ritesh Mukherjee, senior vice president and general manager at Inseego, advises enterprises to make their edge computing data security efforts consistent across the organization. "As the number of locations increases with the edge, the complexity, scale, and points of entry increase. Automated and consistent security controls and policies for data at rest and in motion at all locations are the biggest challenge. A single misconfigured device, an imposter device hiding among many legitimate devices, or lower-cost devices not meeting the standard can be an entry point for a hacker," Mukherjee says.

Mind the Devices and Applications

The same challenges with identity management, asset management, and vulnerability and configuration management certainly extend to the edge. And when it comes to edge server management, the rules for defending cloud and traditional services apply, as do the rules for securing IoT devices. Security teams should continually evaluate edge IoT sensors for how well they are designed when it comes to their native security and the ability to securely manage those devices over time, such as with access controls and software and firmware updates.

"Identity and access management becomes a huge challenge at the edge, and you are going to have to extend these programs to the edge," says Norton.

Ellis agrees: "You absolutely have to consider what your

PKI [system] looks like. How will you perform certificate rotation on these machines? Each machine must have a unique identity; how do they update themselves and tell you their new identity? How do you deal with disconnected devices and trust? What if a machine is offline for three months right before its certificate expires? How does it tell you it has a new certificate when it's time? How does it tell you if it doesn't have a good certificate?"

Keeping up with edge devices and servers is going to require continuous scanning of existing systems and devices, as well as looking for new assets that pop onto the network. "For each edge environment, all of that maintenance must be done," Forrester's Pelino says. "That means maintaining proper configurations and getting devices and applications their needed maintenance and security updates."

"These devices pose a big challenge in certain use cases, such as medical and manufacturing. You can't just set everything to update at noon on Fridays because these are often mission-critical applications," Ellis says. "You have to design and perform controlled updates, such as updating a small percentage of systems at a certain time or whatever works for a particular use case."

The security experts we interviewed agreed that edge devices need tight controls, such as creating allow-lists for specific applications and user access. "You never want to trust these devices for command and control of your network, which will limit the ability for malware to cause damage," Norton says.

Mind the Network

As with data, application, and device security, all of the challenges associated with network security will also be found at the edge. This means data in transit, whenever possible, should be transported encrypted. And while 5G has many security risks, it also has built-in security capabilities, such as mutual authentication, no assumption of trust with networked products and processes, and mandating network traffic encryption. Still, as with any new technology, new risks do emerge.

One such risk was recently demonstrated at the RSA Conference 2022 when researchers from Deloitte & Touche disclosed a potential attack vector on 5G networks that target a core aspect of 5G network design: network slices. During their demonstration, the researchers revealed that a network slice could be exploited by attacking open ports and vulnerable protocols or using metadata to identify all of the networked services. From there, the researchers showed through device emulation that attackers could leap from that initially compromised network slice to another. These attacks are akin to a hypervisor escape in virtualized environments or a container escape in clouds. This shows attacks on the infrastructure while nontrivial are also possible.

Edge Computing Availability and Resilience

Finally, other aspects of a security program will also have to be extended to the edge, such as backup and recovery, availability, and incident response. "You must layer on technical resilience to your edge architecture," Norton says. "The way we think of that is designing systems for five-9s capability because things like destructive malware can cause a denial of service attack and can propagate through backup systems. That's what they do," he says.

You must also plan for business continuity and availability, adds YL's Ellis. "The rule is: Systems always fail. Does that mean you run duplicate systems everywhere? Your CFO is probably not going to be happy. Is there a way to have some systems on standby in case of a failure? That's an option, and all of these things will have to be thought through," he says.

Edge devices need tight controls, such as creating allow-lists for specific applications and user access.

Coalfire's Hicks adds the concerns surrounding incident response and to think especially carefully about the incident response needs for the areas of the edge infrastructure, not under the direct control of the organization. "You will have to understand the incident response processes and options available to you from each cloud provider," Hicks says. "This will also likely require some training for your incident response team, although this transformation is already underway at most organizations due to cloud adoption."

Additionally, the expansion of networks, devices, data, and applications to the network edge is going to strain the already over-strained demand for cybersecurity skill sets even more, says Diana Kelley, the CTO and co-founder of cybersecurity advisory SecurityCurve. Not only for the increased security pressures on enterprise security teams but also for edge servers, services, and device designs.

"As the technologies change and shift quickly, we'll need deep experts in those areas to design and implement the solutions," Kelley says "But, if everybody who's building a new solution or adopting a solution could at least have a security mindset and think about building privacy and security by design, we can get a lot better. But we need the experts to actually do it, and we need everybody, every company that's building one of these solutions, to at least prioritize and think about security early in design.

"Otherwise, we're just going to end up where we always do in security, which is bolting security on after the fact after something terrible has happened. Let's build it in this time, especially now, as the impact of many of these new technologies on humanity is much greater. We've seen little bits of [what's to come], with events such as the Colonial Pipeline attack and people not being able to gas up their cars on the Eastern seaboard, but we haven't learned all of our lessons yet."

Forrester's Pelino agrees. "I think that the idea is to think strategically about the use cases: We need to have security as part of all of these conversations up front, because we start connecting these environments, delivering on these edge experiences, security has to be an integral part of the whole. We're going to have more and more of these edge experiences, not fewer," she says. And that will take everyone from the builders to the implementors to get security right.

About the Author: ***For more than 20 years George V. Hulme has written about business, technology, and cybersecurity topics. He currently focuses on cybersecurity and digital innovation. Previously he was senior editor at InformationWeek magazine, and has freelanced for many trade and general interest publications.***

An Emerging Threat: Attacking 5G Via Network Slices

A successful attack against 5G networks could disrupt critical infrastructure, manipulate sensor data, or even cause physical harm to humans.

By Tara Seals, Managing Editor, News, Dark Reading

While 5G security is not new as a topic of conversation, emerging attack vectors continue to come to the fore. Deloitte & Touche researchers have uncovered a potential avenue of attack targeting network slices, a fundamental part of 5G's architecture.

The stakes are high: Not just a faster 4G, next-generation 5G networks are expected to serve as the communications infrastructure for an array of mission-critical environments, such as public safety, military services, critical infrastructure, and the Industrial Internet of Things (IIoT). They also play a role in supporting latency-sensitive future applications like automated cars and telesurgery. A cyberattack on that infrastructure could have significant implications for public health and national security, and impact a range of commercial services for individual enterprises.

At the heart of any 5G network is a flexible, IP-based core network that allows resources and attributes to be assembled into individual "slices" — each of these network slices is tailored to fulfill the requirements requested by a particular application. For instance, a network slice supporting an IIoT network of sensors in a smart-factory installation might offer extremely low latency, long device battery life, and constricted bandwidth speed. An adjacent slice could enable automated vehicles, with extremely high bandwidth and near-zero latency. And so on.

Thus, one 5G network supports multiple adjacent network slices, all of which make use of a common physical infrastructure (i.e., the radio access network, or RAN). Deloitte collaborated on a 5G research project with Virginia Tech to explore whether it was possible to exploit 5G by compromising one slice, then escaping it to compromise a second. The answer to that turned out to be yes.

"Throughout our journey with Virginia Tech, our objective was uncovering how to make sure that appropriate security is in place whenever a 5G network is put in for any type of industry or any customer," Shehadi Dayekh, specialist leader at Deloitte, tells Dark Reading. "We saw network slicing as a core area of interest for our research, and we set about discovering avenues of compromise."

Achieving Lateral Movement Via Network Slicing

Abdul Rahman, associate vice president at Deloitte, notes that attacking one slice in order to get to a second could be seen as a form of container escape in a cloud environment — in which an attacker moves from one container to another, moving laterally through a cloud infrastructure to compromise different customers and services.

"When we look at the end-to-end picture of a 5G network, there's the 5G core, and then the 5G RAN, then there are the end devices and the users after the end devices," he says. "The core has really evolved to a point where a lot of the services are essentially in containers, and they've been virtualized. So there may then be a similar [attack-and-escape] process where we're able to influence or affect a device on network slice two from a device or a compromise within network slice one."

The research uncovered that an initial compromise of the first network slice can be achieved by exploiting open ports and vulnerable protocols, he explains. Another path to compromise would involve obtaining the metadata necessary to enumerate all of the services on the network, in order to identify a service or a set of services that may have a vulnerability, such as a buffer overflow that would allow code execution.

Then, to achieve "slice-escape," "there are capabilities in the wireless space to emulate tons of devices that can join networks and start causing some stress on the core network," Dayekh says. "It's possible to bring in some scanning capabilities to start exploiting vulnerabilities across slices."

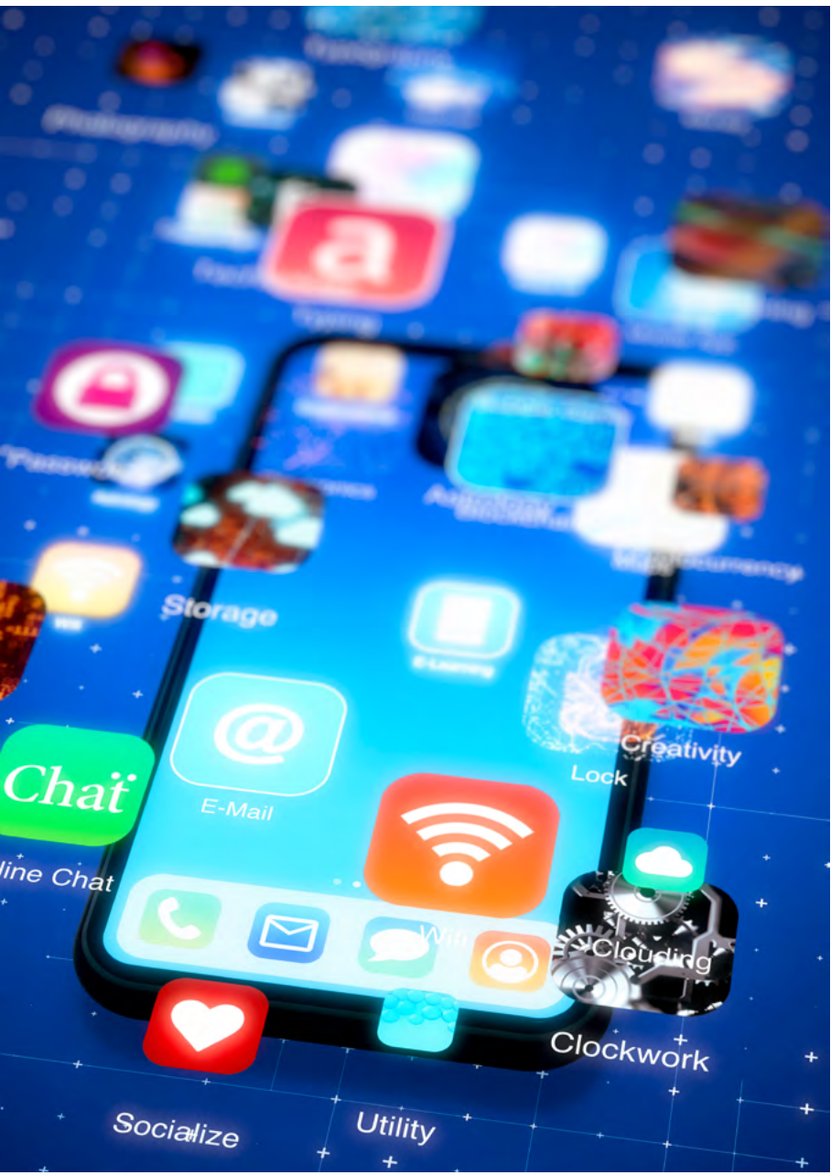
A successful attack would have a number of layers and steps, and would be nontrivial, Deloitte found — but it can be done.

From a real-world feasibility perspective, "it's really dependent on how much money is spent," Dayekh says, adding that cyberattackers would likely make an ROI calculation when weighing whether an attack is worth the time and expense.

"It's about how serious [and hardened] the network is, if it's a mission-critical network, and how serious the target application is," he explains. "Is it an application for, say, shelf replenishment or cashierless checkout, or is it a military or government application?"

If the attacker is a well-funded advanced persistent threat (APT) interested in mounting destructive attacks

Previous Next



on, say, an automated pipeline, the approach would be more convoluted and resource-intensive, Rahman adds.

"This sets the stage for a bad actor that utilizes advanced recon and surveillance-detection techniques, to minimize on the blue side being seen," he says. "You utilize observation to determine avenues of approach and key terrain, while ensuring concealment. If we're going to recon a network, we want to do it from a place where we can scan the network and obfuscate our reconnaissance traffic amongst all the other traffic that's there. And they're going to build this network topology, aka an attack graph, with nodes that have metadata associated with enumerative services around what we would like to attack."

Real-World Risk

When it comes to potential outcomes of a successful attack, Rahman and Dayekh use the example of a campaign against an industrial sensor network for a smart-factory application.

"Ultimately, we can deploy malware that can actually impact the data that's gathered from those sensors, whether it's temperature, barometric pressure, its line of sight, computer vision, whatever that may be," Rahman notes. "Or it may be able to occlude the image or maybe only send back a portion of the results by manipulating what the sensor has the ability to see. That could potentially cause false readings, false positives, and the impact is huge for manufacturing, for energy, for transportation — any of those areas that depend on sensors to give them near-real-time outputs for things like health and status."

The Internet of Medical Things (IoMT) is another area of concern, due to the ability to directly impact patients using remote health services such as kidney dialysis or liver monitoring, or those who have a pacemaker.

There's also another form of attacks that involve deploying malware on vulnerable IoT devices, then using them to jam or flood the air interfaces or take up shared computational resources at the edge. That can lead to denial of service across slices since they all share the same RAN and edge computing infrastructure, Deloitte found.

Defending Against 5G Network-Slicing Attacks

When it comes to defending against attacks involving network slicing, there are at least three broad layers of cybersecurity to deploy, the researchers note:

- Convert threat intelligence, which consists of indicators of compromise (IOCs), into rules.
- Use artificial intelligence and machine learning to detect anomalous behaviors.
- Implement platforms that contain standard detection mechanisms, filtering, the ability to create automation, integration with SOAR, and alerting.

It's important, as ever, to ensure defense in depth. "The rules have a shelf life," Rahman explains. "You can't totally depend on rules because they get aged off because people create malware variants. You can't totally depend on what an AI tells you about probability of malicious activity. And you can't really believe in the platform because there may be gaps."

Much of the defense work also has to do with gaining a view into the infrastructure that doesn't overwhelm defenders with information.

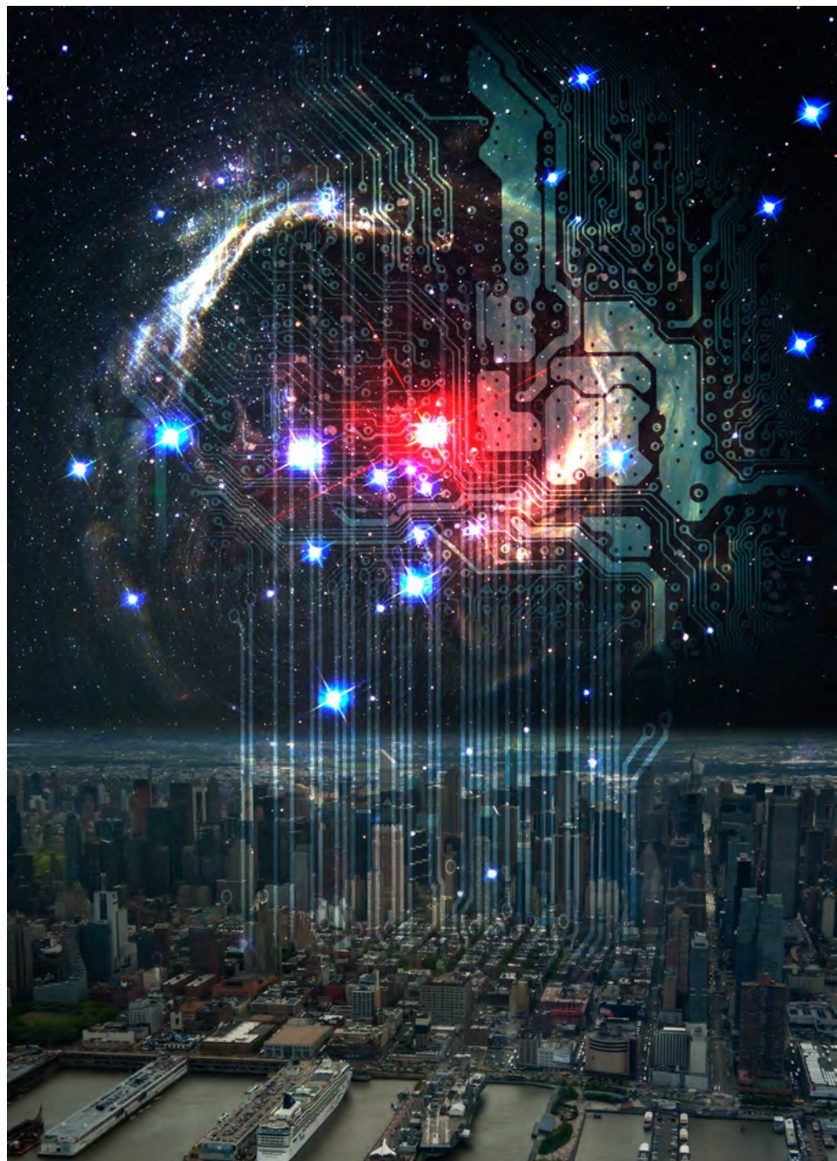
"The key is visibility," Dayekh says, "because when we look at 5G, there's massive connectivity: A lot of IoT, sensors, and devices, and you also have containerized deployments and cloud infrastructure that scales up and down and gets deployed in multiple zones and multiple hybrid clouds, and some clients have more than one vendor for their cloud. It's easier when we don't have a lot of slices or we don't have a lot of device IDs or SIM cards or wireless connections. But there are potentially millions of devices that you may have to look at and correlate data for."

There's also ongoing management to consider, since the 5G standard is updated every six months with new features.

As a result, most operators are still scratching the surface on the amount of work they have to put into shoring up security for 5G networks, the researchers say, noting that the workforce shortage is also affecting this segment. And that means that automation will be required to handle tasks that need to be done in a repeatable manner.

"Automation from a source perspective can go out to these devices and reconfigure them on the fly," Rahman says. "But the question is, is do you want to do that in production? Or do you want to test that first? Typically, we are risk averse, so we test when we do change requests, and then we vote on it. And then we deploy those changes in production, and that takes a certain amount of time. But those processes can be automated with DevSecOps pipelines. Solving this will take some out-of-the-box thinking."

About the Author: *Tara Seals has 20+ years of experience as a journalist, analyst, and editor in the cybersecurity, communications, and technology space. Prior to Dark Reading, Tara was editor-in-chief at Threatpost, and before that, the North American news lead for Infosecurity Magazine. She also spent 13 years working for Informa (formerly Virgo Publishing), as executive editor and editor-in-chief at publications focused on both the service provider and the enterprise arenas.*



7 Cross-Industry Technology Trends That Will Disrupt the World

Recent McKinsey analysis examines which technologies will have the most momentum in the next 10 years. These are the trends security teams need to know to protect their organizations effectively.

By Fahmida Y. Rashid, Managing Editor, Features, Dark Reading

Imagine a scenario where retailers combine sensors, computer vision, artificial intelligence, augmented reality, and immersive and spatial computing to deliver immersive user experiences. Or imagine automakers using sensors to capture vehicle signals, monitor the condition of each system in the car, and notify the owner to schedule repairs before a breakdown occurs.

These scenarios are already possible. Technological innovation is happening at an unprecedented pace, and there are seven cross-industry trends that, individually and in combination, will have a seismic impact across industry sectors, according to research from McKinsey & Co.

These trends, below, have the potential to reshape current business models, enable new applications and services, and redefine how work is done. Security leaders will need to understand their impact to ensure the proper safeguards and protections are in place while unlocking their potential applications and benefits.

1. Next-Level Process Automation

Around half of all existing work activities could be automated by 2025, McKinsey says. Next-level process automation and virtualization includes industrial IoT (IIoT),

collaborative robots, and robotic process automation (RPA). Process virtualization includes advanced simulations using digital twins and 3D/4D printing to change how products are developed. More than 50 billion devices will be connected to the IIoT by 2025, and 70% of manufacturers will be regularly using digital twins by 2022, McKinsey predicts.

2. Future of Connectivity

Faster connectivity — made possible by 5G networks and the booming IoT market — will enable faster connectivity across longer distances. New services will include remote patient monitoring; new business models, such as new ways of energy delivery; and next-generation customer experiences, such as virtual reality. By 2030, McKinsey predicts either high-band or low- to mid-band 5G is expected to reach up to 80% of the global population, McKinsey predicts.

Security leaders are already dealing with the challenges of protecting IoT, and the expected uptake in adoption will complicate things even further. Data protection will continue to be a significant security concern.

3. Distributed Infrastructure

Cloud and edge computing adoption will continue to grow. By 2022, 70% of companies will be using hybrid-cloud and multicloud platforms as part of a distributed IT infrastructure, McKinsey says. By 2025, more than 75% of enterprise-generated data will be processed by edge or cloud computing. Software sourced by companies from cloud-service platforms, open repositories, and software-as-a-service providers will rise from 23% today to nearly 50% in 2025, McKinsey predicts.

"Wide availability of IT infrastructure and services through cloud computing will vaporize on-premise IT infrastructure and commoditize IT setup and maintenance," McKinsey says. Companies could reduce complexity, save costs, and strengthen their cybersecurity defenses.

4. Next-Generation Computing

Next-generation computing is perhaps the most far-reaching trend, as it includes quantum computing and "neuromorphic" computing, which involves the development of application-specific integrated circuits. McKinsey predicts the value of potential of quantum-computing use cases at full scale by 2035 will be greater than $1 trillion.

Keep in mind that quantum computing will likely break the majority of modern cryptographic security algorithms. This will have a significant impact on how organizations protect information. Organizations must safeguard trade secrets and other data during the shift from current to quantum cryptography, McKinsey says.

5. Applied AI

AI is still in its early stages, and companies continue to look for ways to leverage it properly. “While any company can get good value from AI if it’s applied effectively and in a repeatable way, less than one-quarter of respondents report significant bottom-line impact,” McKinsey says.

As AI matures and continues to scale, it will enable new applications by processing data to uncover detailed customer insights and automate repetitive tasks, such as filing and document preparation. It is also expected to support specialized services, such as allowing engineers to perform repairs remotely. AI can play a role in security defenses by training machines to recognize patterns and then respond to the detected pattern accordingly.

6. Future of Programming

McKinsey predicts “Software 2.0,” where neural networks and machine learning will be used to write code and create new software. There could be as much as a 30 times reduction in the time required for software development and analytics, McKinsey estimates.

Software 2.0 will help develop and apply complicated AI models, but it will also improve current software development by standardizing and automating mundane programming tasks. By providing a more iterative and intuitive way to customize existing code, it could potentially eliminate some common programming errors.

7. Trust Architecture

The last trend — trust architecture, such as the zero-trust security model — “describes a set of technologies and approaches designed for a world of increasing cyberattacks,” McKinsey says. “The trust architecture provide structures for verifying the trustworthiness of devices as data flows across networks, APIs, and applications.”

As companies use zero-trust security measures to reduce the threat of data breaches, their cyber-risk will decrease. While zero trust may lower the operating and capital expenditures associated with cybersecurity in some cases, other areas will see cybersecurity spending increase dramatically.

Impacts Will Vary

These technology trends will affect all sectors, but the amount of disruption and technological impact will vary by industry, McKinsey notes. For example, while the shift to new trust architectures will be felt across all sectors, McKinsey’s analysis suggest pharmaceuticals, healthcare, information technology, and telecommunications will experience the most disruption. In comparison, changes in trust architecture will have a limited impact in automotive and chemical industry sectors. Applied AI and next-level process automation, meantime, will have the most widespread impact, affecting multiple industries.

McKinsey examined a range of factors — such as patent filings, publications, news mentions, online search trends, private-investment amount, and the number of companies making investments — to identify technology trends that matter the most to top executives and their organizations. They may not all necessarily represent the coolest or most bleeding-edge technologies, but they are still attracting significant venture capital and are expected to have the biggest impact on the organization.

About the Author: *Fahmida Y. Rashid is an analyst who has covered networking and security for a number of publications, including PCMag, eWEEK, and CRN. She has written about security, core Internet infrastructure, networking security software, hardware, cloud services, and open source.*

Introducing 'Secure Access Service Edge'

The industry buzzword is largely a repackaging exercise that bundles a collection of capabilities together and offers them as a cloud-delivered service.

By Rik Turner, Principal Analyst, Infrastructure Solutions, Omdia

SASE, a recent acronym invading the marketing materials of cybersecurity vendors, stands for secure access service edge. The term, coined by Gartner, refers to a technology trend in support of cloud-based applications and remote working, in which networking and security functionality converge in a single offering.

Omdia has its reservations about SASE as a product category, but we recognize that numerous vendors have adopted this parlance to describe all or part of their network security offerings.

The idea of SASE is attractive: that a single vendor, operating from the cloud, can offer an enterprise all its requirements for branch and remote employee networking, plus all the functionality to deliver that connectivity securely. On the networking side, this mainly covers functionality delivered by most software-defined wide area networking (SD-WAN) platforms, including:

- Dynamic WAN link management
- Multipath application steering and failover
- Quality of service
- Network-layer visibility and path monitoring

Meanwhile, in terms of security, a range of capabilities should be present, namely:

- Application-aware firewall (NGFW-like functionality)
- Secure Web gateway (Web traffic proxying)
- Cloud access security broker (CASB, delivering policy-based SaaS access management)
- Access control (VPN or zero-trust access)

An argument can be made for other subgroups here, such as data loss prevention (DLP), which many CASBs now include as a matter of course, as well as capabilities such as mobile device management (MDM) and decryption and inspection of encrypted traffic.

As such, it becomes clear that SASE is essentially a repackaging exercise, bundling a collection of capabilities together and offering them as a cloud-delivered service, almost certainly as a shopping list from which the customer can pick and mix individual features. While delivering traditionally on-premises-based networking and security capabilities from the cloud is significant, mode of delivery alone does not make SASE a new class of technology. As such, the term is reminiscent of UTM (unified threat management), an early 2000s-era term for multifunction security appliances sold for small businesses and branch offices. While SASE may serve to encapsulate an idea, it is an exercise in marketing rather than an advance in technology.

Reactions Vary From Enthusiasm to Skepticism

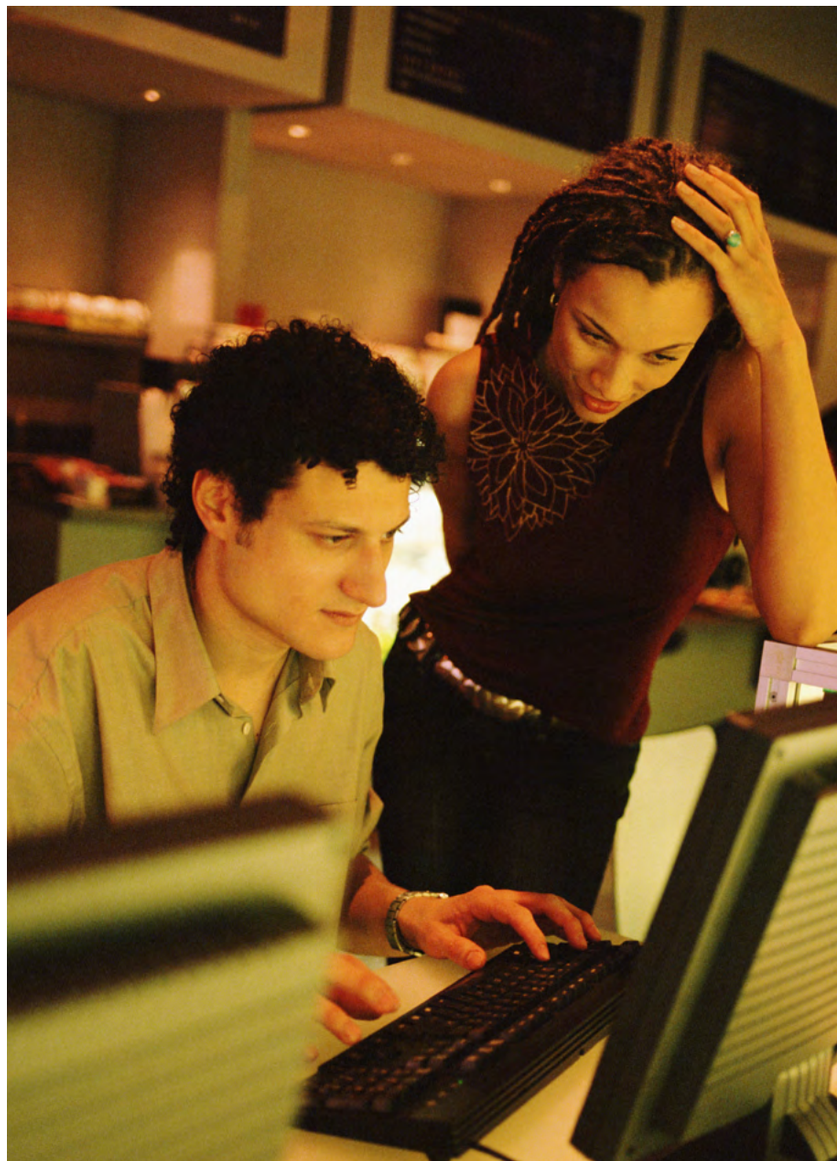
SASE is largely about mode of delivery and product marketing, which explains why it is so easy for different types of vendors to adopt SASE and apply it to their offerings. Omdia identifies at least three groups of vendors that have applied the SASE marketing concept to position their product offerings:

Type 1. There are the top-tier cybersecurity, networking, and data center specialists, such as Palo Alto Networks, Akamai, VMware, and Zscaler, that have latched onto SASE as a "market" into which they can sell a subset of their overall portfolios. Several SD-WAN vendors are also in this group.

Type 2. Those CASB vendors that were not acquired during the great landgrab in that space (Netskope, Bitglass, and CipherCloud) have generally embraced the term, albeit with differing degrees of enthusiasm.

Type 3. Then there is a group of vendors that had been struggling to find an appropriate acronym for what they do. They can complement, or obviate the need for, an SD-WAN: OPAQ, NetFoundry, and Cato Networks are in this category. SASE provides a convenient peg on which to hang their respective hats.

For all this enthusiasm, however, SASE is not without its critics. Omdia's Clifford Grossner has described it as "simply edge computing, connectivity, and security with



Previous Next

integrated management," and questioned whether enterprises would want to buy all this from a single supplier, since it means placing a sizable bet on just one technology provider.

There are those who have criticized the absence of analytics or machine learning for purposes of automating functionality from the basic set of capabilities. And while some in the vendor community have hailed SASE as "the future of SD-WAN," others point to the evolution of SD-branch as the more likely route.

SASE Should Eventually Cede to Multimodal Solutions

Perhaps the most helpful benefit SASE provides the marketplace is an easy-to-understand shorthand to describe a cloud-delivered solution set combining integrated networking and security functions. What was recently a somewhat obscure, hard-to-define concept for individual vendors to articulate suddenly becomes much faster to convey and easier to understand, particularly for those learning about the associated solution sets for the first time. This alone will unquestionably help facilitate adoption of SASE-aligned product offerings.

Despite the many benefits of cloud-delivered IT, SASE is merely the latest waypoint of an ongoing journey that will see continued evolution in the way cybersecurity technology is delivered. The rise of microservices-based and serverless architectures will again require security to be delivered through alternative means, likely as componentized functions within modular application architectures. The ongoing proliferation of Internet of Things (IoT) devices, most notably on the network edge, will drive growing need for IoT security functionality, delivered from the network edge in order to reduce IoT application latency and ensure bandwidth efficiency. Undoubtedly, other technologies that Omdia expects will become prominent in the coming decade — such as 5G, autonomous systems, and quantum computing — will further disrupt and change the way in which cybersecurity solutions are delivered.

Multimodal Requirements

Ultimately, Omdia sees most cybersecurity technology segments evolving toward a multimodal delivery paradigm. As digital transformation takes hold, enterprises will come to demand fluidity in how their cybersecurity technology is delivered, based on evolving business needs (a new branch office opens; another company becomes a subsidiary; a division is spun off and requires access to some applications during the transition; even perhaps a new strain of virus forces an entire business unit to work from home indefinitely…).

An increasing pace of change within enterprise IT means today's need for cloud-delivered security may fluidly evolve into tomorrow's need for security delivered on the edge or as componentized functions, and just as quickly revert back again. Enterprises can expect multimodal offerings that can be dynamically provided in a variety of delivery modes, with pricing and licensing to accommodate change on demand.

About the Author: *Rik Turner is a principal analyst in Omdia's IT security and technology team, specializing in cybersecurity technology trends, IT security, compliance, and call recording. He provides analysis and insight on market evolution and helps end users determine what type of technology and which vendor they should be pursuing.*

Previous Next

INFOBLOX PERSPECTIVES

Streamlining Operations at the Edge

How to quickly deploy, manage, and secure your expanding edge at scale

By Roderick Dixon, Senior Product Marketing Manager, Infoblox

The world as we know it has changed dramatically in the last few years, including our desired work styles, locations, and overall business expectations. Whether we are executives, rank-and-file employees, customers, or suppliers, we now demand greater access, faster response times, and more reliable connections to applications and services — anytime and from anywhere. As organizations strive to keep pace with demands, competitive pressures, and rapid growth, business networks are transforming at the edge where the number of sites and the devices within them are increasing exponentially.

Expectations, Challenges & Technologies

These macro-level trends and expectations are driving organizations to rethink their processes, deployment models, and underlying networks to ensure their service level and quality objectives are met. However, allocated IT staff and budgets remain flat, so viable solutions must be cost-effective, easy to deploy, and optimized to improve access, performance, and security across expanding environments.

There is a noticeable shift from traditional data centers to the network edge, or simply, "the edge." Despite the benefits of this shift, ensuring optimal user experiences at the edge brings its own deployment, management, and security challenges. Fortunately, advances in technologies have emerged to address these issues, namely cloud and edge computing.

What are these advances, and how can they help you build, maintain, and even scale your management infrastructure to meet the needs of the expanding edge? We're glad you asked!

First, here are a couple of quick definitions. Cloud computing is the on-demand delivery of shared applications and services (e.g., compute and storage) distributed across multiple locations. Cloud computing has many benefits, but two of the more common are eliminating the overhead of managing on-premises

resources and the "pay-as-you-go" subscription-based pricing model, allowing a shift from CapEx to OpEx for significant cost reductions.

Similarly, edge computing is a distributed networking approach that brings computing, storage, and related services closer to where the activities are performed (e.g., self-driving cars). This concept and changes to the underlying infrastructure improve response times and minimize network overhead. Cloud and edge computing are two of the more common technologies behind most digital transformation initiatives and are also at the core of the innovative Infoblox networking and security solutions.

Managing & Securing at Scale

Infoblox, a provider of DNS, DHCP, and IP address management (DDI) technologies, offers a cloud-managed solution for these critical network services. BloxOne DDI utilizes cloud-based technology to centralize the visibility, automation, and control of DDI for distributed environments of any size.

Mobile, IoT, and cloud solutions are sensitive to latency and depend heavily on reliable DDI infrastructures. This dependency is significant for devices and users at the network edge. BloxOne DDI leverages the flexibility of centrally managed on-premises hosts to provide a single interface for visibility, automation, and control across multiple sites, locations, and services. BloxOne DDI also redirects network traffic to the closest SaaS entry point for improved application performance and ensures local survivability of all sites and locations at the edge in the event of lost connections to primary networks. All resulting in a more accessible and resilient network for applications and users, regardless of location.

Security is also a significant concern in every organization and network, as attacks increase in frequency, complexity, and impact. BloxOne Threat Defense is a SaaS solution that delivers next-level threat intelligence, optimized to protect devices everywhere on the network, regardless of location, including roaming and distributed sites for users at the edge.

BloxOne Threat Defense also leverages cloud-native technology and core network services to detect and block data exfiltration and malware attacks. Threat Defense also utilizes content categorization and policy enforcement to restrict user access and activity. It also reduces threat investigation time and effort through automated lookups across dozens of trusted data sources. Combining to deliver immediate improvement to the security of organizations of any size.

Bringing It All Together

Infoblox BloxOne DDI and BloxOne Threat Defense leverage an extensible cloud-native platform that utilizes a microservices and container-based architecture to simplify deployments, streamline operations, and minimize the overall total cost of ownership.

A complete set of APIs is also provided for secure, programmatic access to supported features throughout the solution set. Infoblox networking and security solutions have what you need to quickly deploy, manage, and secure your expanding edge at scale, regardless of size or complexity.

About Infoblox: *Infoblox delivers modern, cloud-first networking and security experiences that are simple, automated, scalable, and reliable. The company is the market leader with over 12,000 customers worldwide, including over 70% of the Fortune 500. The company's portfolio of SaaS, data center, and hybrid offerings for DHCP, DNS, IPAM, and security solutions enable organizations to leverage the advantages of on-premises and cloud-first architectures. The combination of NIOS, BloxOne DDI, BloxOne Threat Defense, and threat intelligence services provides a robust foundation for connecting and securing the modern enterprise. Visit* www.infoblox.com *to learn more.*

Previous