UNLOCK DATA-CENTRIC SECURITY

Focusing on the data is key to tomorrow's security

special report

An SC Media publication

Sponsored by

virtru

Companies seek to protect their data rather than networks

Today's 'perimeter' might well be off your corporate network. Locking down the data, not the infrastructure, is the key to reducing data loss, especially when third parties are involved. Esther Shein explains.

One can think of perimeter security like an octopus' tentacles — it reaches far beyond the borders of the corporate network. Those tentacles can embed themselves in your partners' networks, in the cloud, on kiosks and mobile devices that are outside of your physical control. In short, they can move into a myriad of locations beyond the typical purview of an administrator. Applying perimeter defenses and assuming you are safe is a recipe for disaster.

For the chief information security officer, perimeter security requires a balance of strategic security measures and accepting a degree of risk to ensure the business stays competitive and to encourage innovation.

The traditional network perimeter was the physical safe harbor CISOs relied on. It included techniques and tools such as next-generation firewalls, intrusion prevention systems and data loss prevention to ensure the validity of incoming and outgoing traffic, notes Mario Procopio, founder of Pro CISO, a cybersecurity advisory services organization based in Amsterdam.

"This paradigm has been slowly losing its effectiveness in the past decade, evolving into a patchwork of compromises to facilitate migration to the cloud on one hand, and on the other hand" providing capabilities for remote work, Procopio says.

"What we used to view as a perimeter no longer exists," agrees Keatron Evans, principal security researcher and an instructor at Infosec Institute. "Companies are now struggling to even define where or what their perimeter is. … It's very hard to secure something you can't identify or define."

With so many people working from home, virtual private network (VPN) usage at an all-time high and the rapid migration to cloud services, the word 'perimeter' has an entirely different meaning than it did 10 years ago, Evans says.

"We used to have a clear definition of what our network perimeter was, and the task was to protect the data and technology within our borders," echoes Dawn Cappelli, vice president, global security and CISO at Rockwell Automation, with corporate headquarters in Milwaukee, Wis. "Today, a clear line of delineation doesn't exist, and protection has to extend to where the work is done and the data is stored."

When the pandemic hit, only the most mature companies were implementing cloud access security brokers (CASB) to minimize cloud shadow IT and control access, as well as enabling VPN access for remote and third-party suppliers who needed access to the internal corporate network, Procopio

Our Experts: Data-centric security

Will Ackerly, Co-founder and CTO, Virtru
Eric Adams, CISO, Kyriba Corp.
Dawn Cappelli, CISO, Rockwell Automation
Robert Elworthy, assistant IT director, Langdale Industries
Keatron Evans, principal security researcher, instructor & author, Infosec Institute
Trey Keifer, regional director, NCC Group
Mario Procopio, founder, Pro CISO

Data-centric

60%

Gartner, which coined the term SASE, predicts that by 2025, 60% of all enterprises will adopt a SASE convergence strategy, up from 10% in 2020

— Gartner

says. Suddenly, everyone had to extend their network perimeter for remote workers.

"It's evident that the network perimeter has become less physical and especially needs to be more adaptable to the dynamics and location of the users and the data that they need to access," he says.

Procopio believes security should be less about perimeters and more about identifying and protecting the user, resources and data being accessed.

Keatron Evans, principal security researcher, instructor & author, Infosec Institute

Hybrid on-premises and multi-cloud environments, in addition to remote workforce and third parties, require new approaches to protect the dynamic attack surface of the modern organization, he says. Secure access service edge (SASE) technologies "help to dynamically and securely extend the perimeter end to end, from the user access point to across the cloud perimeter, while access is determined by identity policies."

All security features that would normally be implemented inside the office network perimeter should now be implemented from the endpoint itself seamlessly and in replacement of trust-bound VPNs, Procopio says. This includes anti-malware, encryption inspection, firewalling, URL filtering, sandboxing and data loss prevention being made available to all connected network edges, wherever they might be located.

Digital business created a new ecosystem in which partners are adding business capabilities and security complexities, Gartner says. CISOs need to enable trust and resilience as they map their vision for risk and security.

"The objective is to provide an ecosystem that balances the imperative to protect the enterprise with the need to adopt innovative, risky new technology approaches to remain competitive," wrote Tom Scholtz, distinguished vice president and distinguished analyst, in a recent Gartner report.

Data-centric defenses

Yet, with so much data now beyond a corporate network's physical reach, knowing where to begin building or strengthening a data-centric defense can be difficult.

Securing data at rest and in transit are concepts security teams have understood for years, so there are mature processes in place, but data at rest remains a challenge, observes Trey Keifer, a regional director at NCC Group, a Manchester, U.K.-based information security consultancy.

CISOs are grappling with how to encrypt data that still requires computation. Keifer points to secure enclaves as one approach: a secure area of a processor that uses encrypted memory so data can be processed while completely isolated from any applications on a server or system.

> "What we used to view as a perimeter no longer exists, Companies are now struggling to even define where or what their perimeter is .... It's very hard to secure something you can't identify or define."
>
> *– Keatron Evans, principal security researcher, instructor & author, Infosec Institute*

The technology has been around for approximately five years, he says, "but it's been very slow to be adopted by software developers, because they've been stuck in the model of 'If I can keep access from a machine, my data will be secure,'" he says. "They've left it to sysadmins to figure that

Data-centric

24%

Percentage IoT spending is expected to grow in 2021

— IoT Analytics

out while they concentrate on building software."

Secure enclaves let IT define separate roles and draw a distinction between user data and admin data, creating another layer in an application or operating system. The technology is "definitely not utilized to its fullest potential yet," Keifer says. Microservices and containerization are two other similar strategies.

Trey Keifer, regional director of the Southeast/Mid-Atlantic territory, NCC Group

Whitelisting is a huge part of the strategy at Langdale Industries, a Valdosta, Ga.-based holding company and parent company of 25 subsidiary companies, says Assistant IT Director Robert Elworthy.

"One of the main things about whitelisting is if a threat actor comes through one of the whitelisted sites, the problem is at their end, not ours," he said. "That's the problem with perimeter security — when you hand a piece of mail to your postman, you don't know how many hands touch it. You want to get it as securely to the mailman as you can."

> "We ensure that what we procure meets our standards, and there's lots of give and take with legal involved sometimes, and [with] security and finance. We have a thorough third-party risk manager who uses third-party tooling to monitor systems so if there's a security issue, we know instantly."
>
> – *Eric Adams, CISO, Kyriba Corp.*

Defining zero trust

Zero trust has been generating a lot of buzz, but when your organization has multiple business partners, how do you ensure your definition of zero trust is the same as theirs?

That is a question Eric Adams, CISO of treasury management software company Kyriba Corp. of San Diego, Calif, has been thinking about as the company is preparing to move into the federal space.

Kyriba works with multiple banks in several countries that use different formats, and that requires setting up lots of connections. The mantra used to be "trust, but verify, and now it's zero trust," Adams says.

Kyriba's challenge is to ensure it trusts its third-party partners. "When we're using our own third parties, we do a thorough evaluation of them" and make sure they have compliance certifications such as Service Organization Controls (SOC) 1, SOC 2 and ISO, he says. Kyriba also uses multifactor authentication and single sign-on.

"We have an interview process to ensure they're meeting the right security" based on Kyriba's standards, he says. But when you are a multitenant SaaS provider, you cannot necessarily meet all the various security policies because business units use different policies, Adams says.

"We ensure that what we procure meets our standards, and there's lots of give and take with legal involved sometimes, and [with] security and finance," he says. "We have a thorough third-party risk manager who uses third-party tooling to monitor systems so if there's a security issue, we know instantly."

The company also requires third-party annual reviews to ensure its business partners are still following agreed-upon policies and procedures, Adams says.

With upwards of 50 third-party vendors helping Langdale's subsidiaries run their businesses, Elworthy faces a similar conundrum.

Data-centric

$6.2B

Annual investment in 2020 for financial services cybersecurity

— FinTech Global

"Our philosophy on zero trust is, we'll give you access to something we know you need access to in the most secure way possible, but if a [subsidiary] can't give us a valid or logical reason for why someone needs access, that's where we press back and say no, or we work with them" to see what their security practices are and how they align with those of Langdale, he says.

His staff assesses each individual vendor and asks questions such as how are they securing data at rest and in transit? "If we're uneasy, we'll say, 'We'll host the data and you can come get it from us via FTP."

For example, if a health provider needs to ingest some of their data, IT will create

The case for data-centric security

Data-centric protection has never been more critical, with data more typically extending well beyond the corporate network. Mature data ownership requires thinking about data throughout its lifecycle, said Will Ackerly, co-founder and chief technology officer of Virtru, during a recent SC Media webcast entitled Unlocking data-centric security.

Ackerly outlined steps to achieve that, including properly characterizing and tagging data as it is discovered, "and treating it as you need to from a protection standpoint."

It is also important to ensure that as data is stored by third-party partners, it is appropriately protected. It is up to security teams to manage the policies around those protections and through the use and analysis of that data, "making sure you're monitoring and auditing and potentially taking remedial action as necessary," Ackerly said. "Those are all core principles for the mature implementation of data-centric security."

Think about data as the center of your security strategy, he said. The objectives should be persistent protection, strong confidentiality, share with anyone, full control and visibility and audit.

When sharing data to other environments, "it's one thing to encrypt data," but you must also provide consistent controls, he said. "Visibility and audit mechanisms should be required anywhere the data goes. "As you think about implementing a data-centric strategy, take inventory on whether and how your approach can amplify these particular capabilities," Ackerly advised.

In a mature implementation, security teams can worry less about where data is stored and take the stance of an assumed breach — that the adversary is already inside the network.

"That's a very valuable approach to take, particularly as we're sharing data outside," Ackerly said. Being able to identify someone trying to get access to data and what they are doing, are key.

IT should also be explicit about categories of compliance-related attributes to make policy decisions, he said.

"Strong encryption and strong identity done right are extremely empowering," he said. "If I do it right and invest in self-protecting data and data centricity I can take it anywhere, and the investments I've made in that data can follow me anywhere and I'm not losing control."

Ackerly also discussed how a data-centric security model compares to network security when it comes to third-party risk.

"One of the powers of data-centric security is as you're transferring data to another environment, at a minimum, you can categorize and tag the data, so the recipient is in a position to know the obligations of the data to inform the downstream processes," he said. "Trust, but verify, is where you can really unlock incredible power."

—ES

Data-centric

20%

Percentage of companies that never require their employees to change passwords

— PC Matic

a report and upload it to a secure FTP environment and provide access with privileged controls, Elworthy says. IT also whitelists the provider's IP address.

"We know where the data is when it leaves our repository and you hold your breath and hope they're using it in a [legitimate] way," he says.

Dawn Cappelli, CISO, Rockwell Automation

The secure FTP (SFTP) server is also in a demilitarized zone off the corporate LAN so, if hackers get in, they cannot get to the rest of Langdale's network, Elworthy says.

"You want to keep business continuity, but at the same time, you don't want to leave holes — especially because ransomware a lot of times comes through third-party vendors," he notes.

"CISOs should not assume their partners' zero trust definition is the same as theirs," says Cappelli. "Foundationally, you should assume there will be differences in philosophy and configuration, because even your closest partners will likely have a different risk tolerance and operating model," she says.

Internally, a security program needs to continuously monitor and validate the appropriateness of access. Externally, control requirements should be clearly defined, communicated and proven, Cappelli says.

"For now, strong encryption is still a solution for data at rest and in transit. The concept is basic, but effective," she says. Like Keifer, Cappelli says data in use is a challenge. "Limiting access using the principle of least privilege is a starting point. Data masking and privilege escalation are good strategies for extremely sensitive information."

If zero trust were a product and not a principle, it would contradict its own definition, says Procopio, because the idea is that you do not rely on assumptions. However, at any point in time a "trusted" device, user or partner could, for whatever reason, become hostile, he notes.

"Who or what will check that the specific product itself hasn't been compromised?" Procopio says.

"It's an extreme scenario, but that's conceptually what happened with the SolarWinds attack," he adds. "One trusted infrastructure management platform was compromised, allowing access to thousands of trusting devices."

Most zero trust metrics are defined by the business roles and not by IT or the security teams, Procopio adds.

For example, an employee or business partner might be granted access to a specific system or application within a specified time frame and from an identified geographical location, he says.

> "CISOs should not assume their partners' zero trust definition is the same as theirs. Foundationally, you should assume there will be differences in philosophy and configuration, because even your closest partners will likely have a different risk tolerance and operating model,"
>
> *– Dawn Cappelli, CISO, Rockwell Automation*

"These logics are derived from the business role that a user has been assigned for accomplishing his job. Any deviation from the standard profile would trigger an elevation of security" such as a second authentication factor, to ensure that the device or user has not been compromised, he says.

Data-centric

72%

Percentage of vulnerabilities disclosed in Q1 2021 that had no patches available

— NCC Group

Other techniques, other headaches

Encryption everywhere is another option security teams have, but it also has its challenges.


Mario Procopio, founder, Pro CISO

"Encryption everywhere impacts performance, regardless of your industry," says Cappelli. "Manufacturing environments, especially those with legacy operation technology infrastructure, have an even greater challenge because encryption might not be supported in a traditional manner. While the concept sounds great, there's a balance to be made between encryption and practicality."

Evans agrees, saying that the primary challenge with encryption everywhere is it starts to impede or prevent other security functions from doing what they are supposed to be doing.

> "Who or what will check that the specific product itself hasn't been compromised? It's an extreme scenario, but that's conceptually what happened with the SolarWinds attack. One trusted infrastructure management platform was compromised, allowing access to thousands of trusting devices."
>
> *– Mario Procopio, founder, Pro CISO*

"For example, if all traffic is encrypted then it's going to be harder for intrusion detection systems, firewalls, data loss prevention and other technologies to inspect that traffic," he says. "So now you need more expensive and more capable versions of these functions to be able to decrypt and re-encrypt on the fly. It can get very, very messy."

On the defensive side, security teams often struggle with trying to pull exfiltration intelligence from encrypted traffic, Evans says. "Encryption everywhere can compound that challenge if done in an overzealous tone."

He is far more bullish on multifactor authentication (MFA), calling the technology "a great game changer that has instant impact on raising the level of authentication security, when done properly."

The way Cappelli sees it, MFA can be well implemented, or it can cause confusion and potentially impact both security posture and operations expedience. Applying MFA on systems and data that are not important, "can cause bad behaviors, like users approving unexpected authorizations out of habit," she says. "Finding a balance can be a challenge."

Strategies for data-centric defense

When planning a defensive strategy, gone are the days of just thinking how to protect the castle, says Cappelli. "Instead, we're looking at the entire ecosystem of vendors, solutions and work locations, considering how to isolate and manage threats," she says. While she does not discount the technical challenges, "the new opportunity is obtaining sufficient information about your third and fourth parties to make informed risk decisions."

As potential threats evolve, you must keep aware of technology constantly, says Adams. "Prioritization is key, and you look at encryption and access controls and perimeter boundaries and assess it based on your business."

This requires constantly staying aware of what technologies are available to keep each functional security domain safe. "There are evolving sets of tooling and processes involving humans and machines to be able to do this. CISOs have budgets and this is where prioritization is important," he says.

75%

Percentage of victims of pandemic-related fraud who said their cases were still unresolved

— Identity Theft Resource Center

Kyriba uses the National Institute of Standards and Technology (NIST) framework as its standard for vulnerability remediation, Adams adds. The company is focused on "really securing our code repositories and understanding changes to them." Keeping track of those, along with security code analysis and other processes like dynamic code analysis and runtime analysis are "now, more than ever … super important with the attacks we're seeing."

Robert Elworthy, assistant IT director, Langdale Industries

For Elworthy, defending against tomorrow's threats requires multiple layers of security.

"Don't put all your faith in just the edge," he says. "You have to look at endpoint security and monitoring and ingesting information coming from all your different data points and the transportation of data."

Software alone is not a panacea; it is a people issue as well. "You have to look at the human aspect from the end user clicking a mouse from the endpoint they are using and how secure your controls are," Elworthy says. This requires the use of different security layers that allow IT to see if someone is accessing something they are not supposed to and where data is going.

"It's spider webs after that. It's a big shotgun blast and how much of that you can watch," he admits.

A proactive security posture requires teams of people passionate about different domains, Cappelli says. "Security personnel tend to focus on technologies but having good visibility and a deep understanding of risk management, third-party relationships, new regulatory requirements and the changing threat landscape are all important elements in maintaining a proactive culture," she says. "If everyone in your program thinks and acts the same, they likely have the same blind spots, and that's dangerous." ■

For more information about ebooks from SC Media, *please contact Bill Brenner, VP, Content Strategy, at bill.brenner@cyberriskalliance.com.*

If your company is interested in sponsoring an ebook, please contact Dave Kaye, chief revenue officer, at (917) 613-8460, or via email at dave.kaye@cyberriskalliance.com.

Data-centric

69%

Percentage of companies using backup-as-a-service

— ESG

A global leader in data protection and privacy, Virtru equips organizations to implement a Zero Trust strategy through data-centric security. By wrapping each data object in its own layer of encryption, organizations are able to meet privacy and compliance requirements.

Visit http://www.virtru.com or follow us on Twitter at @virtruprivacy.

Masthead

EDITORIAL
EDITORIAL DIRECTOR CONTENT STUDIO
Bill Brenner
VP, Content Strategy
bill.brenner@cyberriskalliance.com
SPECIAL PROJECTS MANAGER
Victor Thomas
victor.thomas@cyberriskalliance.com

SALES
CHIEF REVENUE OFFICER
Dave Kaye
(917) 613-8460 *dave.kaye@cyberriskalliance.com*
VP, SALES
Matthew Allington
(707) 651-9367 *matthew.allington@cyberriskalliance.com*

I (Zero) Trust You.

A strong Zero Trust strategy means that, when it comes to people or systems accessing your network, "**Never trust, and always verify**."

At Virtru, we believe that Zero Trust doesn't have to make things difficult.

Safeguard your most sensitive data while still empowering collaboration. Protect your data at the object level and maintain control at all times.

See how Virtru's data-centric encryption can protect your most sensitive information everywhere it's shared, equipping you to maintain compliance with even the most stringent security standards.

Start the conversation today: **virtru.com/contact-us**

virtru