

Preventing Breaches by Building a Zero Trust Architecture

COMODO

The cybersecurity landscape has undergone a dramatic transformation over the past decade.

And, it's all but certain that more changes are to come.



Enterprises are spending more than ever before on cybersecurity solutions.

YET, ATTACKS CONTINUE TO INCREASE IN

frequency and sophistication. Gartner Inc., a global research and advisory firm, forecasts that information security spending will exceed \$124 billion worldwide in 2019, an 8.7 percent increase over the previous year.¹ However, 64 percent of respondents in CSO's 2018 U.S. State of Cybercrime Survey had experienced monetary losses due to targeted attacks that were the same or greater than the previous year's losses.² The Ponemon Institute's 2018 Cost of Data Breach Survey also revealed that the average total cost of a data breach is \$3.86 million — the highest ever.³

These numbers are alarming, but their underlying message is clear. Current cybersecurity strategies aren't working. Businesses are spending more than ever before on solutions that aren't offering true protection—or a positive return on investment (ROI).

It was against this backdrop that Forrester Research developed the Zero Trust paradigm. In 2010, when they coined the term “Zero Trust,” it was nothing short of a revolution in network security.

Zero Trust eliminates the notion that organizations can trust users and devices inside the perimeters of their corporate networks.⁴ This is often referred to as the “castle and moat” model of network security. Instead, Zero Trust replaces the “trust-but-verify” approach with a “never trust, always verify” model. Adopting Zero Trust requires a mindset shift on the part of IT leaders and administrators and a more interrogative, suspicious approach to information security in general.

Today's IT Infrastructures and Threats Demand a New Model of Security Architecture



The primary reason companies' cybersecurity investments aren't yielding the hoped-for results is that their IT environments have changed so radically in structure and shape.

WITH THE RISE OF CLOUD-BASED SERVICES AND

increases in employees' use of personal and mobile devices, the idea of fixed network perimeters has become largely meaningless.

Nearly half of all enterprise workloads currently run in public or hybrid clouds.⁵ Industry leaders predict as many as 94 percent of workloads will be processed in cloud data centers by 2021.⁶

None of these applications, or the computer resources that run them, can be secured behind an internal firewall.

According to Forrester Research, more than half of companies in the U.S. and Europe already have bring-your-own-device (BYOD) programs in place or are developing them in response to workforce demand.⁷ A majority of these devices are unmanaged, and none operate within traditional enterprise network perimeters.

EVEN IF THESE WORKLOADS AND DEVICES—AND THE

applications and valuable data they hold—could somehow be contained within the boundaries of a trusted network, the realities of today's threat landscape render the "castle and moat" approach completely inadequate.

Twenty-eight percent of the breach incidents analyzed in the 2018 Verizon Data Breach Investigations Report was perpetrated by internal actors:⁸ even the most robust perimeter-based defenses can do nothing to prevent this type of malicious activity. The same study also reported that the most common attack action used for data exfiltration was credential theft, against which perimeter-based defenses are wholly ineffective.

**Zero Trust was designed
to combat these types
of threats.**

What is Zero Trust?



The central guiding principle in the Zero Trust model of information security is “never trust, always verify.” **Zero Trust seeks to eliminate internal “trusted” zones within networks and instead make security omnipresent throughout the digital business ecosystem.** With Zero Trust, all network traffic is untrusted, and all data is to be continuously inspected.

It’s a holistic approach that emphasizes visibility and ongoing monitoring over perimeter-based defenses and strategic goals over particular tools and technologies.

The Zero Trust model is rooted in three core concepts.



CONCEPT NO. 1

NEVER TRUST, ALWAYS VERIFY

Adopting a Zero Trust architecture means eliminating the concept of trust from your network's design. You must assume all traffic is a potential threat until proven otherwise. All traffic should be inspected, verified and secured, no matter where it resides. Data that sits in an on-premise data center is to be treated the same way as data hosted in the public cloud. No traffic is to be allowed by default.

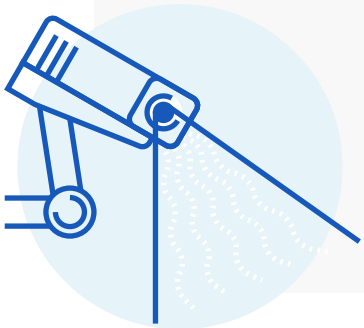


CONCEPT NO. 2
**PROTECT CUSTOMER AND
BUSINESS DATA**

A robust security strategy begins with a focus on the data. You need to understand where your data is stored, how it is used, why it is sensitive and what might put it at risk. You must implement granular access control policies to protect it and prevent employees and partners from accessing and sharing sensitive resources unless it's absolutely necessary for business functions.

CONCEPT NO. 3
**CONTINUOUSLY MONITOR YOUR
INFRASTRUCTURE AND NETWORK TRAFFIC**

Ongoing monitoring of all network traffic enables your security team to spot anomalous user behavior or suspicious activities quickly. This is the key to keeping incursions from becoming breaches. Maintaining logs of all internal and external traffic will also improve visibility into your environment.

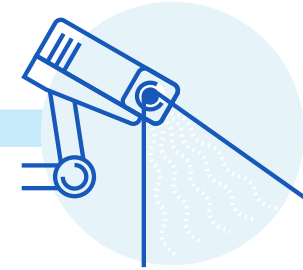




CONCEPT NO. 1
**NEVER TRUST,
ALWAYS VERIFY**



CONCEPT NO. 2
**PROTECT CUSTOMER AND
BUSINESS DATA**



CONCEPT NO. 3
**CONTINUOUSLY MONITOR
YOUR INFRASTRUCTURE
AND NETWORK TRAFFIC**

Taken together, these three principles call for organizations to adopt a data-centric approach to securing their environments. Rather than assuming that some users—or certain types of traffic—can be deemed “trustworthy,” **Zero Trust demands that every file be treated as potential malware, and every user as a possible threat agent.** Only after they’re proven themselves trustworthy should users—or the data packets they generate—be given access to the network.



To build a robust security infrastructure, you must first establish a solid foundation.

The Zero Trust model can supply that foundation, but adopting it requires stakeholders across the business to reimagine information security and change how they think about risk. Everyone within your organization tasked with creating, manipulating, analyzing, sharing or storing data has a role to play in making this shift.

Zero Trust provides an architectural blueprint for enhanced information security that can be applied in every IT environment, but implementing it isn't always simple. It requires commitment, new strategies and the right technology investments.

 To make it easier, we've outlined a simple five-step plan to help you incorporate Zero Trust principles into your organization's security infrastructure plan.

-  **STEP 1**
Change your mindset
-  **STEP 2**
Map the data and transaction flows within your organization
-  **STEP 3**
Define microperimeters around sensitive data
-  **STEP 4**
Validate every device and endpoint
-  **STEP 5**
Continuously monitor your Zero Trust ecosystem

STEP 1

Change your mindset

TAKING A ZERO TRUST APPROACH TO INFORMATION

security requires transforming the way you think about trust in your business's digital ecosystem. It's a paradigm shift; in the old model, connections and access were allowed by default. Now, access control and inspection policies are to be enforced throughout the environment.

IT leaders must change the primary questions they're considering. Instead of asking "How can I protect my organization and its internal assets?" or "How can I keep attackers off my network?," you need to ask "How can I build a set of protections that will travel with my data, no matter where it is located?" and "How can I keep security central in all our digital business processes?"

Adopting a Zero Trust strategy does not require deploying any particular tools or technologies.

It's not necessary to wait for your next major infrastructure overhaul to get started. Putting Zero Trust into practice is a strategic goal

But it does mean that traditional endpoint security or legacy signature-based antivirus/anti-malware solutions won't be adequate protection for your environment. These products don't offer robust defenses against today's emerging threats. For instance, 77 percent of ransomware victims in one recent survey were running up-to-date endpoint protection at the

time of the attack.⁹ And once attackers have devised a means of evading antivirus software's detection mechanisms, additional layers of defense are needed to prevent them from gaining a foothold within the environment.

It's not necessary to wait for your next major infrastructure overhaul to get started.

Putting Zero Trust into practice is a strategic goal. Only after you've decided to work toward it should you begin considering the technologies that could best help you get there. Progress toward Zero Trust can be made incrementally, and you'll still see significant security gains.

STEP 2

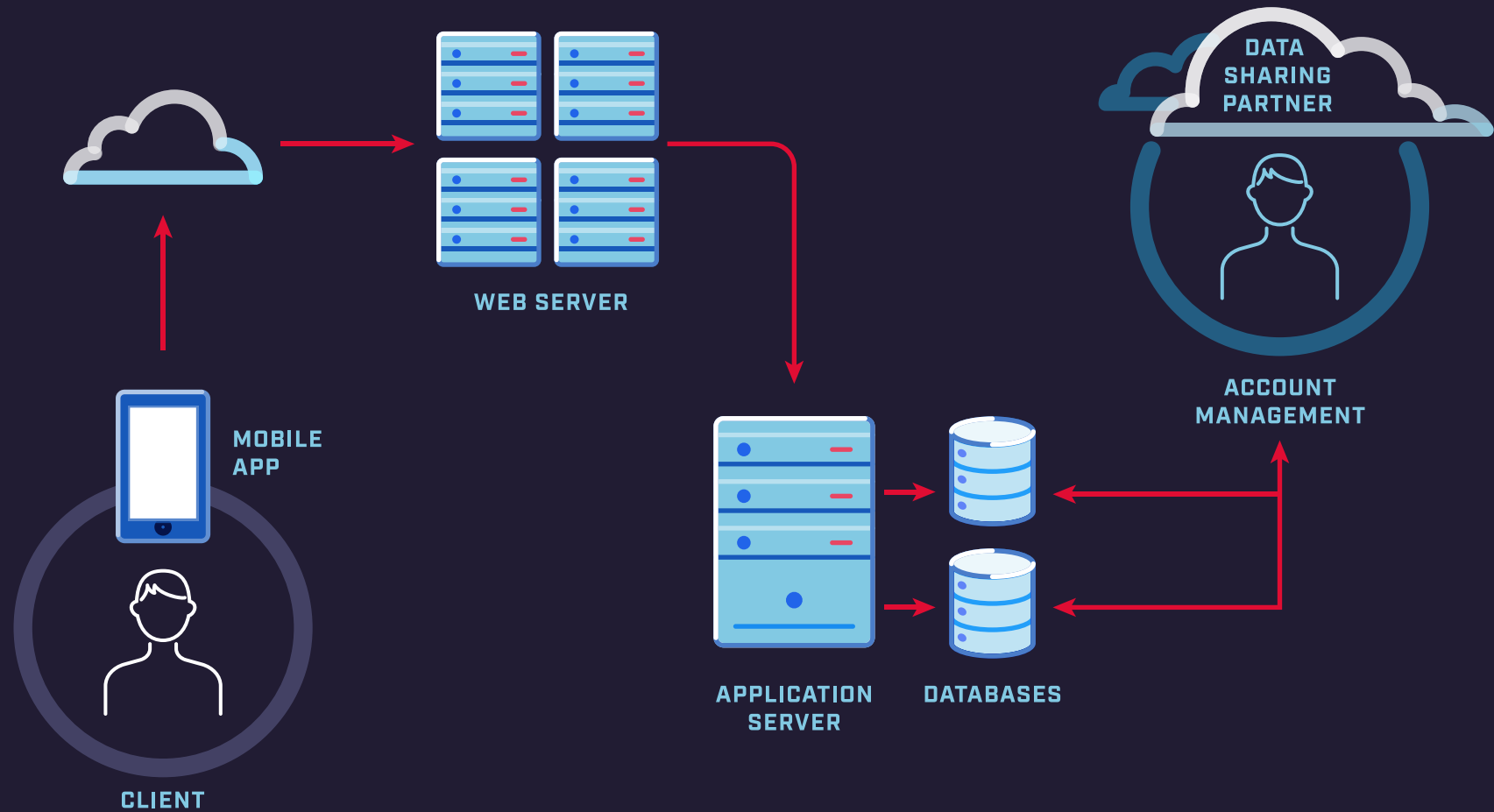
Map the data and transaction flows within your organization

BECAUSE YOUR DATA'S SECURITY AND INTEGRITY ARE

central to the Zero Trust paradigm, its implementation begins with a thorough understanding of where your data resides and how it flows between users, devices, systems and other resources in your IT environment. You'll need to engage stakeholders across the organization in this process since it usually involves network architecture, third-party services and questions about user needs and value to the business.

Your team will need to create a comprehensive inventory of your data assets that identifies where data is stored, how it is collected or created, who uses it and how it travels. You can create visual representations of these processes or flows, called data flow diagrams, at varying levels of abstraction.

If your business must adhere to compliance requirements such as the Payment Card Industry Data Security Standard (PCI-DSS)¹⁰ or the EU's General Data Protection Regulation (GDPR),¹¹ you probably already have existing data flow diagrams you created to meet these requirements.



Courtesy of Forrester

An example data flow map

STEP 3

Define microperimeters around sensitive data

RATHER THAN CREATING A TRUSTED ZONE WITHIN THE perimeters of your network, microperimeters help you set strict access control rules and policies that enforce data security regardless of where your users, their devices or the services they're running are located.

Establishing microperimeters—or microsegmentation—involves restricting access, applying robust security controls and closely monitoring traffic. The idea is to maximize the security of your most sensitive data repositories by segmenting the network and enforcing this segmentation with security controls. The goal is to isolate and contain threats, keeping them away from your sensitive data and eliminating the potential for compromise.

To set up microperimeters, you'll need technology solutions that offer granular

Establishing microperimeters—or microsegmentation—involves restricting access, applying robust security controls and closely monitoring traffic.

access controls, enabling you to define groups by traits, such as location, job function or individual user identity. This needs to protect your users even when they are outside the confines of the corporate network. Look for email and web security gateways that automatically contain unknown files and refuse them permission to install or execute until they've been inspected and deemed free of risk. High-risk file sharing sites and services should be blocked for your entire organization.

Data Loss Prevention (DLP) solutions can also serve to enforce microperimeters. They enable you to scan all outbound web and email traffic to enforce policies that prevent the exfiltration of sensitive data. They can give your security team complete visibility into where your data is traveling and which users or devices are interacting with it.

STEP 4

Validate every device and endpoint

“NEVER TRUST, ALWAYS VERIFY” IS A CORE TENET OF THE

Zero Trust model. Just as all traffic should be considered threat traffic until it has been verified, every endpoint attempting to connect to your network should be considered a source of malware until it has been identified and proven otherwise.

Unknown devices should never be allowed to access your organization’s network unless they have security controls installed that you’re able to manage and administer. Ensure that your network controls offer granular device discovery capabilities that can link every endpoint attempting to connect with your network with a unique identifier. You need real-time visibility into the full digital footprints of all employees. This also includes those who work remotely.

Look for a technical solution that can seamlessly monitor a variety of device types and operating systems and can enforce uniform policies for all of them. It’s common for multiple devices belonging to the same employee to become infected at the same time, so cross-device correlation is vital.

STEP 5

Continuously monitor your Zero Trust ecosystem

ONCE YOU'VE DEFINED THE MICROPERIMETERS AROUND your most sensitive data repositories, set up granular access control policies to protect them. Implement a solution that will prevent unverified devices from connecting to your network and offer you visibility into the process taking place on the endpoints that are connecting. You will need to monitor these systems on an ongoing basis.

A cloud-based security information and event monitoring (SIEM) platform can ingest and correlate logged data from a wide array of tools and solutions, particularly if they're all part of an integrated platform. These solutions—including email and web security gateways, secure DNS filtering, advanced endpoint protection or endpoint detection and response platforms—can produce a large volume of valuable data with the potential to reveal attacks and threats to your

environment. But, this data's value can be captured only if it's being monitored in real time.

Depending on your organization's in-house capabilities, it often makes the most sense to outsource this monitoring to a dedicated security operations center (SOC). With SOC as a Service (SOCaaS), you'll get 24-hour, year-round dedicated monitoring of your entire security infrastructure performed by a team of experts. Look for a service provider with advanced threat-hunting capabilities and the ability to contain threats and remediate incidents remotely. Packet-level traffic monitoring capabilities are also essential.

In this area, readily integrated solutions also are best. Ensure that the SOCaaS you are considering will work with the security solutions you've already deployed within your infrastructure.

CONCLUSION

PROTECTING BUSINESS IT ENVIRONMENTS FROM EVER-EVOLVING THREATS HAS NEVER POSED MORE OF A CHALLENGE THAN IT DOES TODAY.

As cybersecurity costs continue to increase, malicious activity shows no signs of slowing down. Cybercriminal operations are more carefully targeted and better funded than ever. Nationwide state-level adversaries remain active, and even relatively unsophisticated hackers have successfully compromised enterprise networks.

In this environment, a Zero Trust Architecture offers the opportunity to tilt the odds in favor of the defenders. If your organization is serious about improving its security posture in the face of today's increasingly sophisticated threats, the Zero Trust framework represents a way forward.

Implementing a Zero Trust security architecture is no easy task. It calls for decision-makers to let go of deeply-held assumptions about information security they may have maintained for years. It

demands effort and commitment from stakeholders throughout the business. And it requires investment in carefully-chosen technology assets.

Not every organization has the resources to conduct ongoing monitoring or threat-hunting in house. With cybersecurity talent in short supply and the increasing complexity of the technologies in the security stack, it often makes the most sense to outsource responsibility for protecting your network and information assets to a trusted partner.

Comodo offers a comprehensive portfolio of interlocking solutions that can provide full visibility into your environment, granular access controls and policy management for your entire IT ecosystem, on-premises and in the cloud. Comodo's solutions are engineered to work seamlessly with their Managed Detection and Response services, offering full-scale remote resource management and monitoring to enterprises of all sizes, as well as managed IT service providers.

Comodo solutions are engineered to help businesses achieve a Zero Trust Architecture to prevent breaches. And several solutions, including Comodo's Advanced Endpoint Protection, Secure Web Gateway and Secure Email Gateway, feature Comodo's unique, industry-leading Auto Containment Technology.

Comodo's Auto-Containment Technology prevents breaches by containing and analyzing 100 percent of unknown files that come in contact with a network. As an unknown file executes on an endpoint, the file is instantly contained and analyzed, while users experience no interruption in the system's performance. While the unknown file is in Auto-Containment, it is analyzed statically and dynamically in the cloud. 95 percent of the time, a "trusted" verdict is returned in under 45 seconds. 5 percent of the time, human experts further analyze unknown files to provide "trusted safe" or "malicious" verdicts. Auto-Containment never trusts unknown files and always verifies they are safe before releasing from the container.

COMODO

ABOUT COMODO

In a world where preventing all cyber attacks is impossible, Comodo provides active breach protection with its cloud-delivered, Zero Trust platform. The Comodo Dragon platform provides a Zero Trust security environment that verdicts 100 percent of unknown files. The platform renders an almost immediate verdict on the status of any unknown files, so it can be handled accordingly by software or human analysts. This shift from reactive to proactive is what makes

Comodo unique and gives them the capacity to protect your business—from network to the web to cloud—with confidence and efficacy.

Comodo has experts and analysts in 185 countries, protecting 100 million endpoints and serving 200,000 customers globally. Based in Clifton, N.J., Comodo has a 20-year history of protecting the most sensitive data for businesses and consumers worldwide.

ENDNOTES

1. www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019
2. https://images.idgesg.net/assets/2018/11/201820us20state20of20cybercrime_sample20slides_gated20for20insider.pdf
3. <https://www.ibm.com/downloads/cas/861MNWN2>
4. <http://crystaltechnologies.com/wp-content/uploads/2017/12/forrester-zero-trust-model-information-security.pdf>
5. https://www.logicmonitor.com/resources/thank-you-for-downloading/?url_content_id=300316&slug_name=ty_the-future-of-the-cloud-a-cloud-influencers-survey&content_type=Survey&content_title=Cloud%20Vision%202020:%20The%20Future%20of%20the%20Cloud%20Study&content_dl_link=https://www.logicmonitor.com/wp-content/uploads/2017/12/LogicMonitor-Cloud-2020-The-Future-of-the-Cloud.pdf
6. <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-cl1-738085.html>
7. <https://www.forrester.com/Bring-Your-Own-Device-%28BYOD%29>
8. https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf
9. <https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/endpoint-survey-report.pdf>
10. https://www.pcisecuritystandards.org/document_library
11. <https://gdpr-info.eu/art-83-gdpr/>