opentext™ | Cybersecurity

White Paper

Zero Trust: Rethinking Security

Traditional cybersecurity has been laser-focused on keeping intruders off the company network, a goal accomplished mainly through firewalls to monitor incoming traffic and bar suspicious data packets. Today's next-generation firewalls have evolved to offer more advanced capabilities, like Secure Sockets Layer (SSL) for protecting transactions and deep packet inspection as data is delivered to the company doorstep.

While firewalls continue to be a vital part of cyber defense, it's important to remember that they were designed to protect a single network. In the age of the cloud, information flies at warp speed to and from a host of applications, partner networks, and hundreds of remote devices connecting to your network through thousands of access points. Some of these devices and apps have subpar security controls. A shocking number have none at all.

Today's multi-cloud, multi-device environment is bonanza for hackers, who have exponentially more entry points to choose from and are armed with sophisticated software tools to sniff out vulnerabilities across the internet.

Today's multi-cloud, multi-device environment is bonanza for hackers, who have exponentially more entry points to choose from and are armed with sophisticated software tools to sniff out vulnerabilities across the internet. Once they break in, they're often free to move about until they gain access to your protected customer data, your intellectual property, or your network controls.

This internal movement is possible because traditional defenses have concentrated on fortifying the barrier between your network and the outside world—the hard shell—while pretty much ignoring the "gooey center." This is not a bug, but a feature, designed to make it easier for company insiders to get around and find what they need. Once someone enters a password, and perhaps a second authentication factor, they're in like Flynn.

But multifactor authentication alone won't keep intruders out in today's world. And employees with unlimited access to company data—a common feature of legacy apps—make hackers' work even easier, as well as offering temptations to disgruntled insiders.

According to Verizon's 2019 Data Breach Investigations Report, 34 percent of data breaches come from insiders. The proportion rises to 60 percent in healthcare and 36 percent in financial services—sectors containing information especially valuable to thieves. The average cost of a breach has risen to $3.92 million, according to the Ponemon Institute.

With the stakes higher than ever, it's time for a new approach to cybersecurity, an approach based on today's reality of multiple clouds and anytime/anywhere access. That approach is called zero trust.

What Is Zero Trust?

You've probably heard the term "zero trust," but you may be confused about its meaning. That's because it's not a single technology (though it's sometimes described that way), but a collection of activities working together to give you the best protection possible as your information travels across devices, apps, and locations around the world.

Here's a summary of some of the most important features of a zero trust system. You don't have to have all these technologies or adopt them all at once. Just keep in mind that they function best in concert, so it's important to sync everything up as you go along.

Fine-Grained Access Controls

Perhaps the most fundamental concept of zero trust is controlling access, not on the blanket basis of insider vs. outsider, but according to users' specific needs. It's called the principle of least privilege: Give employees, partners, contractors, and anyone else who uses your network access only to the tools they need to do their work—nothing more and nothing less. The access system must be centrally managed and dynamic, because people and organizations change.

If Greg starts as an accountant, he will need access to company transactions. If he's promoted to controller, he will need deeper financial access and the ability to see the work of people he supervises. If he moves to the London office, he will need different information, and much of his former access will need to be terminated. When he retires, he'll still need to see his benefits, but all other access should be cut off immediately.

With zero trust, all of these actions are rule-based and automated to ensure that they are enforced right away. That's because unauthorized access can cause mayhem.

Just ask Target, which lost $162 million after the credentials of an HVAC contractor were used to steal credit card numbers and personal information of 41 million customers. Or Home Depot, where a vendor's credentials were used to extract 56 million customer credit and debit card numbers, costing the company $180 million.

It's not just contractors who are to blame. In a study by Dell, an astonishing 72 percent of employees admitted they would share sensitive, confidential, or regulated company information with outsiders if a manager asked them to, if they thought it would help them do their job, or for some other excuse. While some felt they had a duty to protect confidential information, their company's changing security guidelines made them uncertain of how to do it.

Another catastrophe waiting to happen at many companies is former employee access. A recent study found that a third of ex-employees still have access to files and documents from their former workplace. Without centralized control and automation, it's all too easy for an overburdened IT department to overlook this problem.

A single bad apple can wreak havoc, stealing intellectual property or deleting administrative accounts and protected records.

You've probably heard the term "zero trust," but you may be confused about its meaning. That's because it's not a single technology (though it's sometimes described that way), but a collection of activities working together to give you the best protection possible as your information travels across devices, apps, and locations around the world.

To add insult to injury, your company may be held responsible. In the UK, after an ex-worker posted payroll information for nearly 100,000 employees on a file-sharing website, a judge ruled that even though the firm had not mishandled the data itself, it was vicariously liable for the breach.

Protecting vital information is a company's responsibility, and with all the channels your data flows through today, no one can keep track of it manually. A finely tailored, automated identity and access management system is the foundation of all security and one of the precepts at the heart of zero trust.

Protecting vital information is a company's responsibility, and with all the channels your data flows through today, no one can keep track of it manually. A finely tailored, automated identity and access management system is the foundation of all security and one of the precepts at the heart of zero trust.

Closely Managed Privilege

Another crucial zero trust component is the close management of privileged accounts—those that can access your most sensitive information or make changes to important systems and data.

Because these accounts handle the keys to the kingdom, they're especially attractive to cyber criminals. Eighty percent of percent of security breaches involve the use of privileged credentials, according to Forrester.

Of course, attackers may not be lucky enough to compromise one of these valuable accounts initially. But if internal access controls are lax, they can work their way up.

That's why a privileged account should require additional authentication factors as the importance of information it accesses progresses. When a privileged account is dealing with sensitive customer data, fixing a network problem, or otherwise engaged in potentially dangerous activity, the user should be monitored in real time, and should never be given blanket permissions. In some cases, passwords for a specific task should be revoked as soon as it is completed.

These extra precautions not only ensure that privileged account holders are behaving properly, they also stop hackers from moving through the organization. Most criminals are looking for easy targets, and if they're thwarted at every turn, they'll get frustrated and move on.

Activity Monitoring

By coordinating with your identity and access management system, your security center can detect suspicious activity based not just on network traffic, but on internal user identity, device, location, and behavior, issuing alerts or cutting off access if, say, a New York worker unexpectedly logs in from Moscow.

Today's machine learning tools go even further, noticing if employees visit strange websites at odd hours, start downloading sensitive information they don't normally use, or type in a pattern different from their normal rhythm. Creating automated alerts for abnormal events allows you to respond to them much faster, preventing a breach or limiting its reach.

The sooner a breach is detected, the less damage it creates, according to the Ponemon Institute. The average amount of time needed to identify and contain a breach is 279 days, but those stopped in less than 200 days cost 37 percent less than others.

Security software with automated controls is particularly effective, Ponemon says. Breach costs for organizations without security automation were 95 percent higher than those with fully deployed automated systems.

In addition to monitoring user behavior, a zero trust security center continuously guards against the latest threats and provides alerts for patching vulnerabilities, helping organizations avoid the horror of assaults like the WannaCry ransomware attack.

AI software is improving constantly, and some of the latest products can protect you almost in real time.

Meaningful Data Classification

Comprehensive data classification is fundamental to zero trust. Only when you know what you have and where it is can you develop the right policies for protecting it.

To truly understand your information, you can't just rely on metatags—especially for unstructured data like videos, emails, audio recordings, images, and PowerPoint presentations.

Tags are simply shorthand created by individuals to help them find what they need, but they may not work for others searching the same data for another purpose. For example, a marketing manager might tag a presentation "Road Warrior Campaign," leaving no clue for anyone else about the company product information it contains.

Artificial intelligence and machine learning software can view unstructured data's content, make sense of it, and classify it according to both its meaning and its security value. In addition to helping everyone find what they need, it unearths unprotected sensitive data lurking in unexpected places and transfers it to a safer location.

Software-based tagging also makes compliance much easier, instantly revealing to auditors information they would otherwise spend hours searching for.

AI software is improving constantly, and some of the latest products can protect you almost in real time. As an experiment, a store set up a video camera outside its entrance, filming curious onlookers as they walked by. The camera contained facial recognition technology, but the store could only use it on those who consented. As people approached, they were asked for permission to use their images, with voice recognition technology responding to their answers. As a result, the camera successfully blurred the images of the 99 percent who didn't give consent as soon as the footage was broadcast.

Image recognition software has real time business value, too. It can be used to monitor a construction site for dangerous activity and violations, or warn a chemical factory if an unauthorized truck approaches.

Trust in the Age of the Cloud

Cloud services are immensely valuable, but they also open the door to a new set of vulnerabilities. Uploading your data to a cloud-based app means trusting it another company. No matter how reliable and ethical the provider may be, they could get hacked—and your valuable private information could be a casualty.

A zero trust approach offers a way to take full advantage of cloud services without giving up your most sensitive information. Using format-preserved encryption, you can substitute fake information for customer or employee names, addresses, credit card numbers, and other sensitive data. Then you send it along to the app for analysis. As long as the information is entered into the right fields in the right format, the app doesn't know the difference. You get all the detailed number crunching and analysis you want without turning over your personally identifiable information to the app—though you can still see this information in the results.

As security technology evolves, researchers are developing other sophisticated techniques, such as creating fake applications and servers to lure attackers, study their methods, and catch them in the act.

As use of the cloud expands and technology breakthroughs create new vulnerabilities on a massive scale, security based on protecting a single network no longer makes sense. Zero trust is a forward-looking set of procedures designed to identify your users and information with the utmost precision, helping you conserve your resources while protecting your most valuable assets automatically and in real time.

The Brave New World of IoT

The internet of things is upon us, and with it comes a dizzying array of new launching points for cyberattacks. Manufacturers of common consumer IoT products—smart TVs, webcams, and thermostats, among many others—have been notoriously lax about security, making these devices easy to hack. It didn't take long for hackers to catch on.

In the early days, their most common exploit was to amass armies of home devices to create botnets and stage distributed denial-of-service attacks on corporate websites. The most infamous is the Mirai botnet, which took down several high-volume websites at once, including CNN, Twitter, and Netflix.

DDoS attacks were just the beginning. Hackers have broken into and taken control of everything from cars to insulin pumps, pacemakers and defibrillators, baby monitors, and even toys.

The next item on their agenda could be corporate data. In 2020, there will be 5.8 billion enterprise and automotive internet-connected products in circulation, Gartner predicts.

Researchers last year created a scenario showing how hackers could execute a corporate lateral IoT attack by compromising security cameras and a router—a fairly easy task. Using software tools, they could then theoretically zoom in over workers' shoulders to see and record their login information. Other researchers have discovered vulnerabilities in office printers that could allow thieves to steal documents and passwords.

The IoT creates a new universe of security problems, and not just because of the vast number of new connecting devices. Another issue is the technology that makes their operation possible. Though 5G offers better encryption and network verification than 4G, its lightning-fast speed means that hackers who do get through will be able to move across your network in no time—unless you have automated access controls in place to stop them.

As use of the cloud expands and technology breakthroughs create new vulnerabilities on a massive scale, security based on protecting a single network no longer makes sense. Zero trust is a forward-looking set of procedures designed to identify your users and information with the utmost precision, helping you conserve your resources while protecting your most valuable assets automatically and in real time.

The OpenText Cybersecurity Advantage

With decades of experience in corporate security, OpenText™ has deep knowledge of every aspect of zero trust. We can shine a new light on your people and data, showing you the best ways to protect them while working with your existing solutions to make them a part of a coherent, up-to-date, well-functioning whole.

Learn more at
www.microfocus.com/en-us/cyberres

About NetIQ by OpenText

NetIQ by OpenText provides security solutions that help organizations with workforce and consumer identity and access management at enterprise-scale. By providing secure access, effective governance, scalable automation, and actionable insight, OpenText customers can achieve greater confidence in their IT security posture across cloud, mobile, and data platforms.

Visit the NetIQ by OpenText homepage at **www.cyberres.com/netiq** to learn more. Watch video demos on our NetIQ Unplugged YouTube channel at **www.youtube.com/c/NetIQUnplugged**.

NetIQ is part of Cybersecurity, an OpenText line of business.

Connect with Us
www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.