opentext™ | Cybersecurity

Position Paper

Customer Satisfaction Guide for Zero Trust

As organizations work to incorporate Zero Trust principles into their environment, one of their most daunting challenges is to apply this new security model to digital interactions with their consumers. More than any other type of user, these are the ones who gravitate to a "don't make me think" mindset, which makes them extra difficult to secure. This paper reviews a few approaches to Zero Trust strategies and how NetIQ by OpenText helps you achieve them.

Introduction

Zero Trust doesn't have to limit your ability to engage your digital customers with speed and convenience.

It wasn't that long ago that there was no such thing as an online or mobile app from which you could choose your seat on a flight. You were left at the mercy of airline employees or travel agents to offer alternatives. Today, you can check your seat and upgrade status, access boarding passes, and change flights, as well as perform other tasks that were once only possible via an interaction with a person. Not only did this cost you in both time and convenience, but it created a level of overhead for the airlines as well. Now, you can experience that same level of convenience across a wide range of industries, such as banking, retail, and even healthcare. Moreover, organizations that aren't moving aggressively to this new paradigm of consumer engagement find themselves lacking or scrambling to catch up.

Zero Trust means that your mobile apps need to move away from username/password authentication and implement a multi-step/passive method.

This level of digital service isn't possible with standard identity and access management architectures. You need a more sophisticated level of management for customer identities—one that works at a dramatically larger scale. While organizations commonly have thousands or tens of thousands internal users, they might also have tens, hundreds, or millions of external users. The way user information is gathered or acquired is different now and often requires a different approach to integration. This new customer-facing identity and access management (CIAM) infrastructure needs to secure resources with less friction while protecting against a higher level of risk—all without getting in the way of access.

Zero trust imposes a higher level of security

The requirement for continuous identity verification can kill operational efficiency

If you make doing business with you difficult, your customers will go elsewhere

Figure 1. Zero Trust doesn't have to kill your ability to engage your digital customers with speed and convenience.

And as IT teams and their business owners look at how to elevate their CIAM infrastructure so they can raise the quality of their digital interactions and personalized engagements with their consumers, there's a new obstacle—Zero Trust.

Zero Trust is a security philosophy based on the default approach that organizations shouldn't automatically trust anything inside (commonly labeled the intranet) or outside their secured perimeter. Rather, security-wise, everything is treated the same and anything that is trying to connect to its systems must be verified before being granted access. In terms of protecting backend systems, this change imposes new requirements onto the organization's CIAM infrastructure.

Another consideration when implementing Zero Trust is that consumers expect their experience to follow them wherever they go. As such, it's the organization's job to keep that experience as familiar as possible. For example, customers expect their on-the-road mobile application experience to be as convenient as their web-based experience at home.

Forrester promotes a proactive architecture approach to protecting your organization from cyberthreats—Zero Trust.

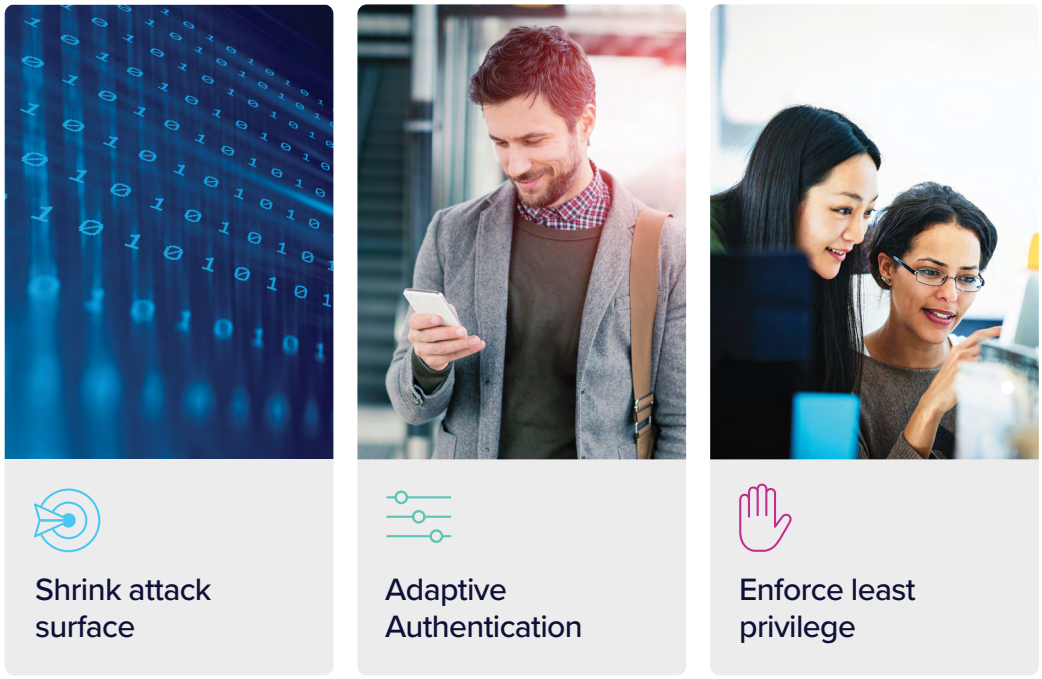

Figure 2. Essential elements of your Zero Trust strategy

The Basics of the Zero Trust Model

Moving to a Zero Trust security model means you need to assume that both the network and all of the services using it are potentially hostile. This is a major shift for any IT organization who, for decades, has depended on the intranet model. As such, this foundational transformation will likely need to happen in piecemeal—either in terms of selecting portions of your environment to upgrade or identifying portals of the Zero Trust model that give you the biggest bang for the security buck to focus on first.

Minimize Your Attack Surfaces

Although network segmentation has long been a security practice for architects, Zero Trust formalizes that approach to isolate valuable, well-protected systems. Rather than thinking in terms of traffic that flows within your intranet (versus securing traffic coming in from the outside), with this new security approach you shrink each network zone across your environment and then enable them to control access for each one. In many ways, microsegmentation is counter to the traditional VPN approach.

Beyond network segmentation, you can further section off access to applications and microservices by using gateways. When you segment and secure access to each service, you dramatically decrease the attack surface that might be public facing or within a zone that has been compromised by a malignant agent or user. This focus on shrinking attack surfaces synergizes well with the transition to microservices. As your digital environment continues to transition to microservices, you have the opportunity to apply specific security processes to each one, shrinking your exposure regardless of where they reside.

One of the best ways to build consumer trust and loyalty is to secure their interactions with an adaptive and frictionless experience.

Emphasis on Least Privilege

As part of the Zero Trust discussion, the focus is typically on limiting the lateral movement of users and processes across zones throughout the network. Given that, historically, the primary way attackers gained access to sensitive data was through compromising the network, this is indeed a significant component of Zero Trust. However, because services are now commonly scattered across a variety of remote sources, they can't always be protected with a secured zone or a dedicated network. So, while enforcing a "least privilege" security model has always been a primary Zero Trust network strategy, today's anywhere microservice paradigm gives credence to expanded use of the least privilege security model.

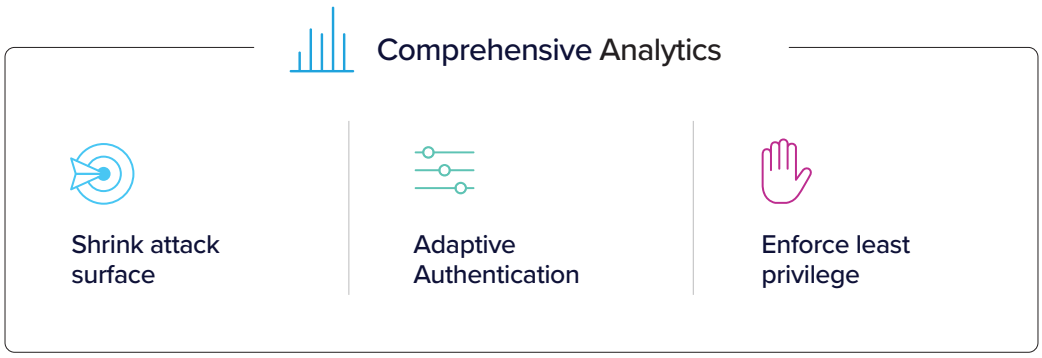

Figure 3. Zero Trust focus for CIAM

As you extend least privilege up the stack, here are some basic principles to keep in mind as you decide how far to take it in your environment:

- Root server accounts shouldn't be the foundation of your administration. If so, you are distributing too much access and have no attribution of who is accessing your systems. Instead, use a delegated model with granular controls.
- You need a privileged user lifecycle that keeps up with administrators' changing roles and responsibilities. If this isn't automated, you won't be able to stay on top of your privileged users' access rights, which represents a significant risk to your environment.
- Ensure that you employ comprehensive auditing. Having a solution that documents the roles and actions of privileged users is a powerful deterrent to rogue behavior and is a forensic treasure trove.

To stay on top of your least privilege strategy, set up an environment where you can automatically manage user access, identity information, and access policies.

Adaptive Access Management

When it comes to verifying a user's identity, IT and security groups have struggled for decades to determine how to apply the right mix of security and usability. And as their customers transition to being digital consumers, IT groups continue to revisit this give-and-take balance between the level of risk that the organization is willing to tolerate and the need to engage with these consumers effectively. And because competitors are always ready to snag dissatisfied customers, the pressure is on to allow digital customers to do more—

often spawning new security and access management initiatives. Yet, despite this massive investment, the pace of breaches has remained unacceptably high. It is due to this general access management and security failure that security teams to are taking a closer look at Zero Trust and why it is so relevant to CIAM.

One of the precursors to a Zero Trust level of access management was the adoption of risk-based authentication, which in general offers a way to adjust the authentication experience based on the risk score and context. For example:

- Device identification
- Geolocation
- IP address and IP address history
- Known cookie
- HTTP headers
- User attributes
- Last login time
- And more

Adaptive authentication has a fundamental dependency on the ability to correctly identify when a customer's identity is in question.

Depending on the policies that fit the business, higher risk scores might invoke a second-factor or multi-factor authentication experience. Or, if the score is high enough, it can be used to reject authentication altogether. In reality, the majority of organizations keep their risk-based authentication rules quite simple. In essence, they define their policies so that users accessing services from within the intranet are verified by a simple username and password, while those outside are required to authenticate using a second factor. But what about consumers who, by their very nature, are always outside? What should be the consumer experience when accessing personal, regulated, or other types of sensitive information? Often, it turns out that the risk is just as high, or even higher:

- **Customer trust**—While the types of private information that consumers are most concerned about vary depending on the kind of service they are using, a common one is their credit card information.. As we have seen in a variety of high-profile cases, when consumers lose trust in their online retailer or other types of service providers, they go elsewhere. For the healthcare industry, when electronic records or different kinds of patient information are stolen, the Office for Civil Rights gets involved and lawsuits often follow. The typical way that this type of information is lost is through outsiders who break into source repositories using the compromised credentials of a privileged user.
- **Protection against outsiders**—Virtually all organizations have private data included in their customer-facing infrastructure. A lot of this information is used across a host of specialized applications, for example, microservices. Keeping this private information secure while offering more powerful and compelling services to customers is a constant challenge.

What APIs are you customers invoking?

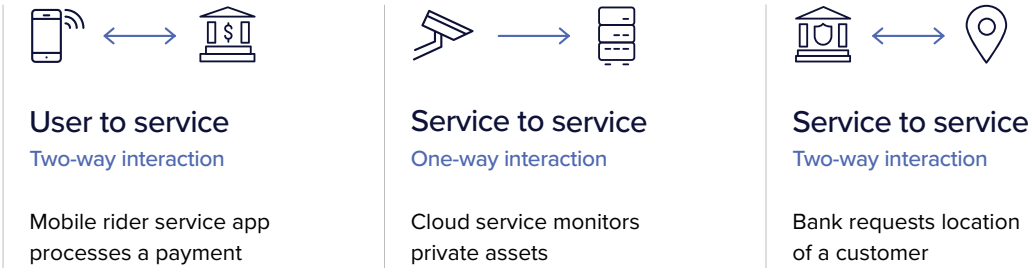

Figure 4. Zero Trust includes protecting the APIs that you customers invoke.

As Zero Trust security is applied to meet these challenges, stronger implementation of risk-based authentication is required. One of the key differences in this new model is that it has eliminated carte blanche single sign-on in favor of continuous authentication. This means whenever a customer accesses a new resource (commonly through an API underneath a mobile app), they will be required to verify their identity. Likewise, if a customer is accessing a protected resource that is outside of expected behavior, they will be required to verify their identity. Of course, if an organization wants to gain and keep customers, they can't be repeatedly harassing them to verify their identity. Instead, they need to implement some passive or at least low-friction methods for the customer to verify themselves. It also means that the risk engine needs to be much more context-aware and more effective at discerning between expected user behavior and actual higher-risk situations.

Beyond adapting authentication levels based on customer context, security groups also have the option to adapt the authorization for what the user can access. There might be situations where the best way to keep interaction with the customer as open as possible—while controlling risk—is to allow access to less sensitive information while blocking access to higher sensitive information, all in the same session. Whatever your strategy, having an adaptive environment is an essential element to achieving Zero Trust access management.

> **"... you just had a major security breach... it looks like they got into your primary customer database via the APIs you depend on for all your mobile applications... trying to figure out how this happened... it is because you have done nothing... resulting in an open door for any hacker to walk through."**
>
> **The API Evangelist**

Using NetIQ to Build out Your Zero Trust Environment

Minimize Your Attack Surfaces

For your applications that support federation protocols (such as SAML2, OAuth, or WS-Federation), NetIQ Access Manager by OpenText™ offers IdP support. However, you can also use it to add another layer of protection for your applications, services, and other resources. NetIQ Access Manager does this by offering an optional Access Gateway. With this gateway, you can shrink the attack surface by directing all access through it and then setting up centrally administered rules that control access based on your security policies. You can also configure the gateway to leverage the NetIQ Risk Service by OpenText™, which enables you to adapt authorization levels based on measured threats that protect against higher-risk situations.

Policies must be dynamic and calculated from as many sources of data as possible.

NetIQ Access Manager can also provide secure, up-to-date TLS communication for applications and systems that can't be upgraded or are in the process of being replaced. The reverse proxy enforces TLS 1.2 communication between clients and the Access Gateway on uncontrolled public networks. It can also support legacy SSL communication to origin web servers, where the communication channel can be secured by internal network security controls and firewalls. Having a single, easily updated platform exposed to the public network makes your entire system more secure. Best of all, you can use NetIQ Access Manager's gateway to protect any application, even those that don't support federation.

Provide the Right Level of Privilege

NetIQ Identity Governance by OpenText™ provides an efficient process that keeps your access permissions current, which is incredibly important to securing your environment. This is especially true for your privileged administrators and users who work with your customers' sensitive or regulated information. NetIQ Identity Governance automates both the identity and permissions lifecycle and administration. This enables you to quickly see which users should have and do have permissions to protected information and to centrally remediate access risks across your entire environment.

NetIQ Directory and Resource Administrator by OpenText™ is the perfect solution for organizations who want to use their Azure AD to implement role-based delegation for their administrators and privileged users. Powerful workflow automation enables you to enforce policies across your entire Azure platform.

NetIQ Privileged Account Manager by OpenText™ takes least privilege to the next level by providing a variety of controls targeted specifically at securing access to your systems. In addition to these comprehensive controls, privileged user activity can be monitored to provide seamless audits. NetIQ Privileged Account Manager records administrator activity that not only provides forensic information, but also helps to support compliance requirements.

Adaptive Authentication

Perhaps the most challenging element of a Zero Trust implementation is continuous authentication. This is because it breaks so many paradigms of an organization's current processes and past investments. Even with continuous authentication, IT must maintain a high usability threshold for its customers as their identity is verified at various points of interaction. And while continuous authentication is quite secure, in order to be viable it needs to be invisible to the customer or at least invoke very low friction. Because repeatedly presenting authentication requests to the user isn't customer-friendly, the NetIQ Advanced Authentication by OpenText™ framework provides the broadest range of integrations that offer passive authentication methods to choose from. And because user requirements differ, this level of choice is essential in helping organizations find the best fit. To protect against vendor lock-in, the framework is based on open standards that offer you the widest range methods today, as well as into the future.

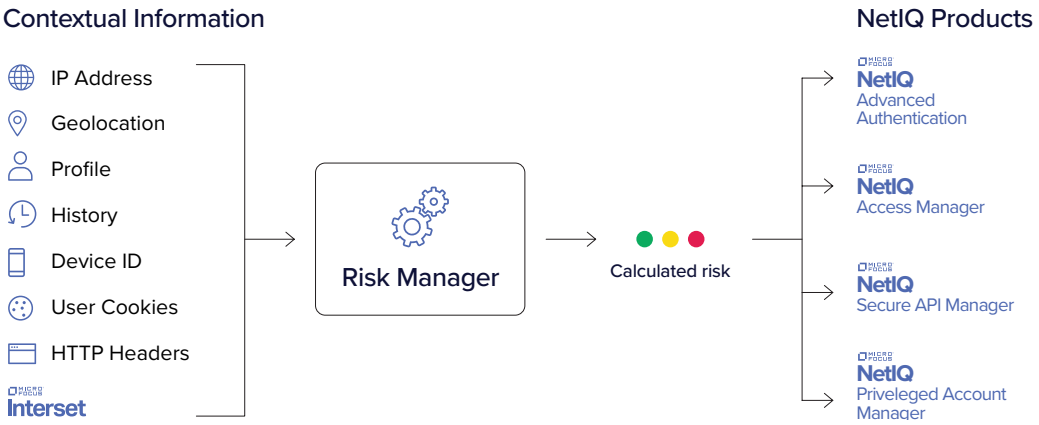

Figure 5. The NetIQ Risk Service provides context-based risk scores for the suite.

Recognizing that an adaptive authentication environment is essential to maintaining customer engagement and satisfaction, NetIQ Risk Service by OpenText™ offers advanced metrics for risk scoring. The best way to identify and protect against imposter-based attacks is to learn the unique "normal" behavior of your individual customers. This type of baseline enables the Risk Service to detect unusual and suspicious behaviors. User and entity behavior analytics (UEBA) are developed through machine learning and are the most effective way of building an effective context-based adaptive environment. The NetIQ Risk Service offers integration with the NetIQ by OpenText Interset solution. When out-of-context behavior is identified, the NetIQ Risk Service can invoke another passive authentication of the customer, using NetIQ Advanced Authentication.

"In a world where governance and further digitalization is increasingly important, we have no doubt that we have chosen the right partner in Micro Focus (now part of OpenText™). Its vast portfolio of security solutions is sure to address our needs into the future."

Stefan Winterber
Head of IT
Netstal

Conclusion

Surprisingly, a Zero Trust environment isn't any more complicated or costly than what most organizations have in place today. Often, savings and simplicity are achieved by consolidating multiple disconnected technologies. Moving to Zero Trust might very well mean leaving behind expensive legacy technologies and moving to a simpler solution that has significantly lower overhead.

To learn more about what Cybersecurity by OpenText is doing to help organizations build a Zero Trust environment, please visit **www.microfocus.com/en-us/cyberres/identity-access-management**.

To learn more about the NetIQ Advanced Authentication framework and how it works with NetIQ Risk Service, please visit **www.microfocus.com/en-us/cyberres/use-cases/risk-service**.

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.