Otterize

Zero Trust / Microsegmentation

DATASHEET

Zero Trust / Microsegmentation

Requirements

- Zero trust is a security framework that eliminates implicit trust and continuously validates every stage of digital interaction. It's a fundamental shift from traditional perimeter-based security to a model that assumes breach and verifies each request, regardless of its origin.
- Security perimeter has moved to a fine-grained isolation architecture that is aligned with zero-trust security.
- Zero trust is the default security posture for modern applications for multiple reasons.
- Microsegmentation is a key component of zero trust, dividing the network into smaller zones to limit the blast radius of attacks and enforce granular access controls.

Devs

- Build security into applications from the start, ensuring secure coding practices and access controls in alignment with SecOps directives.
- Integrate IAM and micro segmentation configuration with existing workflows and deliver secure, compliant applications faster.
- Reduce cognitive load associated with security configuration, especially in areas like identity and access management (IAM), where specialized knowledge is often required.

CISOs

- Manage risk effectively, protect sensitive data, and meet regulatory requirements.
- Proactive security posture that minimizes the impact of breaches and strengthens the organization's overall security stance.
- Communicate security risks and the business value of proactive security measures to development, DevOps, and other stakeholders to ensure buy-in and successful implementation.
- With limited resources and a growing digital attack surface, CISOs need solutions that automate security processes and enable efficient management of security controls across the organization.

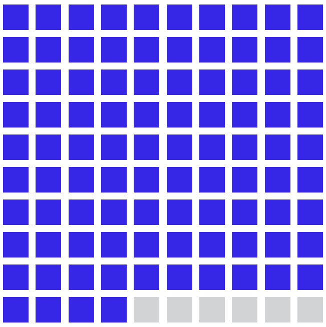
Platform Admins

- Simplify the management of complex environments by automating security policy enforcement and providing granular access controls.
- Reduce the risk of misconfigurations and improve operational efficiency.

Drivers

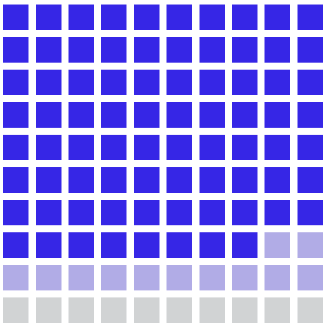
- **Erosion of the Perimeter:** Traditional perimeter-based security is no longer effective in today's distributed environments.
- **Sophistication of Attacks:** Cyber threats are constantly evolving, requiring a more robust and adaptive security model.
- **Rise of Cloud & Hybrid Environments:** Organizations are increasingly adopting cloud and hybrid infrastructures, which demand new approaches to security.
- **Regulatory Compliance:** Regulations like PCI-DSS, HIPAA, and GDPR mandate stricter security measures to protect sensitive data.

Key Figures and Data



94%

of organizations have experienced a business-impacting cyberattack in the past 12 months (Cybersecurity Venture)



78%

of companies worldwide say zero trust has increased in priority, and nearly 90% are currently working on a zero trust initiative (Okta's State of Zero Trust Security 2021).

7.6 trillion

Ransomware is still a concern and overall intrusion attempts continued to climb in 2023, rising to 7.6 trillion, a 20% increase over 2022's total (SonicWall).

$4.45 million

The average cost of a data breach is now $4.45 million (IBM).

Benefits

Automated Microsegmentation

- **Devs:** Otterize integrates with CI/CD pipelines, automatically generating and enforcing microsegmentation policies based on application dependencies. This ensures that security is built into the development process. By abstracting away complex security domains and domain-specific languages (DSLs), Otterize enables developers to focus on their core tasks without sacrificing security.

- **CISOs:** Otterize simplifies compliance by automatically generating audit-ready reports and ensuring that access controls are consistently enforced.

- **Platform Admins:** Otterize reduces the operational overhead of managing microsegmentation policies, freeing up the platform team to focus on other priorities.

Zero-Trust Policy Enforcement

- **Devs:** Otterize strengthens application security by ensuring that only authorized services can communicate with each other, preventing unauthorized access attempts.

- **CISOs:** Otterize not only provides granular visibility into access patterns across your environment but also enables proactive threat response by automatically remediating policy violations based on predefined global rules.

- **Platform Admins:** Otterize integrates with your existing IAM systems, making it easy to manage and enforce zero-trust policies across your entire environment.

Competitive Advantage

Application-Aware Microsegmentation

- **Devs:** Otterize is “developer-aware” in its understanding of how applications work, enabling more precise and effective microsegmentation policies than traditional network-based solutions.

- **CISOs:** Otterize’s application-centric approach is “process-aware” and reduces the risk of over-segmentation, combining the right balance between security and functionality, while optimizing performance.

- **Platform Admins:** Otterize’s dynamic policy generation adapts to changes within any cloud-native or on-prem environment, ensuring that microsegmentation policies remain effective even as applications evolve over time.

Ease of Use & Integration

- **Devs:** Otterize simplifies access management, enabling you to control application communication directly through familiar tools like Slack and GitHub. No need to involve DevOps or navigate complex configurations – maintain your workflow while ensuring secure access.

- **CISOs:** Otterize simplifies your compliance journey. Its built-in guidance accelerates your microsegmentation project, prioritizing tasks, facilitating collaboration between teams, and guiding DevOps in implementing zero trust policies effectively within your production environment.

- **Platform Admins:** Otterize integrates seamlessly with your existing infrastructure, including cloud platforms, Kubernetes, and IAM solutions.

Key Features

- **IBAC:** Otterize automatically translates high-level security intent (e.g., “allow web servers to access databases”) into detailed, granular access policies, abstracting away the complexities of network and application configurations.

- **Application Dependency Mapping:** Otterize automatically discovers and visualizes the relationships between applications and their components, including microservices, APIs, and data flows. This provides a comprehensive understanding of your application architecture and helps you identify potential security risks and dependencies.

- **Network Policy Automation:** Based on application dependency mapping, Otterize automatically generates and enforces fine-grained network policies (e.g., Kubernetes NetworkPolicies) to restrict traffic flow between application components. This ensures that only authorized communication is allowed, reducing the attack surface and preventing lateral movement in case of a breach.

- **API & Microservices Authorization Policy Automation:** Otterize extends microsegmentation to Layer 7 by generating and enforcing authorization policies (e.g., Istio authorization policies) based on application roles and permissions. This provides more granular control over which workloads can access specific application features or sensitive data, enhancing security and compliance in both on-premises and cloud environments. Additionally, Otterize automates the configuration of cloud IAM roles and permissions directly within Kubernetes, as defined by developers, ensuring that policies align with the intended access requirements for optimal application functionality. This streamlines policy management and reduces the risk of misconfigurations.

- **Multi-Cluster Visibility:** Otterize provides a unified view of security policies and application traffic across multiple Kubernetes clusters, ensuring consistent security and compliance in complex environments.

- **Multi-Cloud Support:** Otterize works seamlessly across major cloud providers (AWS, Azure, GCP), ensuring consistent security and compliance policies for hybrid and multi-cloud deployments.

- **GitHub Integration (for DevSecOps):** Otterize continuously compares your defined security policies (ClientIntents) with actual application traffic. If discrepancies are detected, Otterize automatically creates a pull request in GitHub to update the ClientIntents, aligning them with the observed traffic patterns.

- **Agentless Deployment:** Otterize operates without requiring the installation of agents on individual workloads, simplifying deployment and minimizing performance overhead. It leverages existing Kubernetes infrastructure (e.g., service mesh) for visibility and policy enforcement.