AT&T Business

AT&T Guardicore: fight cyberbreaches with microsegmentation

The AT&T Cybersecurity Consulting team has been working with clients for **over 25 years.**

Implement software-based microsegmentation across your environment to enforce zero trust

Digital transformation helps organizations achieve greater business agility, reduces infrastructure costs, and enables remote work. It also creates a larger and more complex attack surface that does not have a well-defined perimeter. Each server, virtual machine, cloud instance, and endpoint is now a possible point of exposure. With the prevalence of ransomware and zero-day vulnerabilities, attackers are more adept at moving laterally toward high-value targets when – not if – they find a way in.

Fortunately, when it comes to fighting malware and ransomware, there's a formidable new cybersecurity "microsegmentation" solution. It's called AT&T Guardicore.

A great analogy for microsegmentation is a ship. Ships are designed using compartments so that a breach of one compartment doesn't result in a sunken ship. Similarly, networks can be divided into smaller protected segments so that a security breach can be reduced and not have a catastrophic impact on business operations. A breach can cause leaked customer data and brand and reputational damage.

Features

- Granular, AI-powered segmentation
- Multiple protection methods
- Real-time and historical visibility
- Broad platform support

Benefits

- Prevent lateral movement in ransomware attack and quickly contain damage if compromised
- Protect workloads in any environment and safeguard critical applications via segmentation
- Meet compliance requirements for microsegmentation (PCI/DSS and SWFT)
- Supports breach insurance coverage requirements
- Simplify security management across cloud, data centers, and physical assets with one platform

AT&T Guardicore is purpose-built to simplify microsegmentation. It provides easy, fast, and intuitive ways to enforce zero trust principles within your network. It stops lateral movement by visualizing activity within your IT environments, implementing precise microsegmentation policies, and detecting possible breaches quickly. In a zero-trust world, you must assume that every user, device, app, network, and cloud is at risk of compromise. All users must validate who they are and only go where they are permitted.

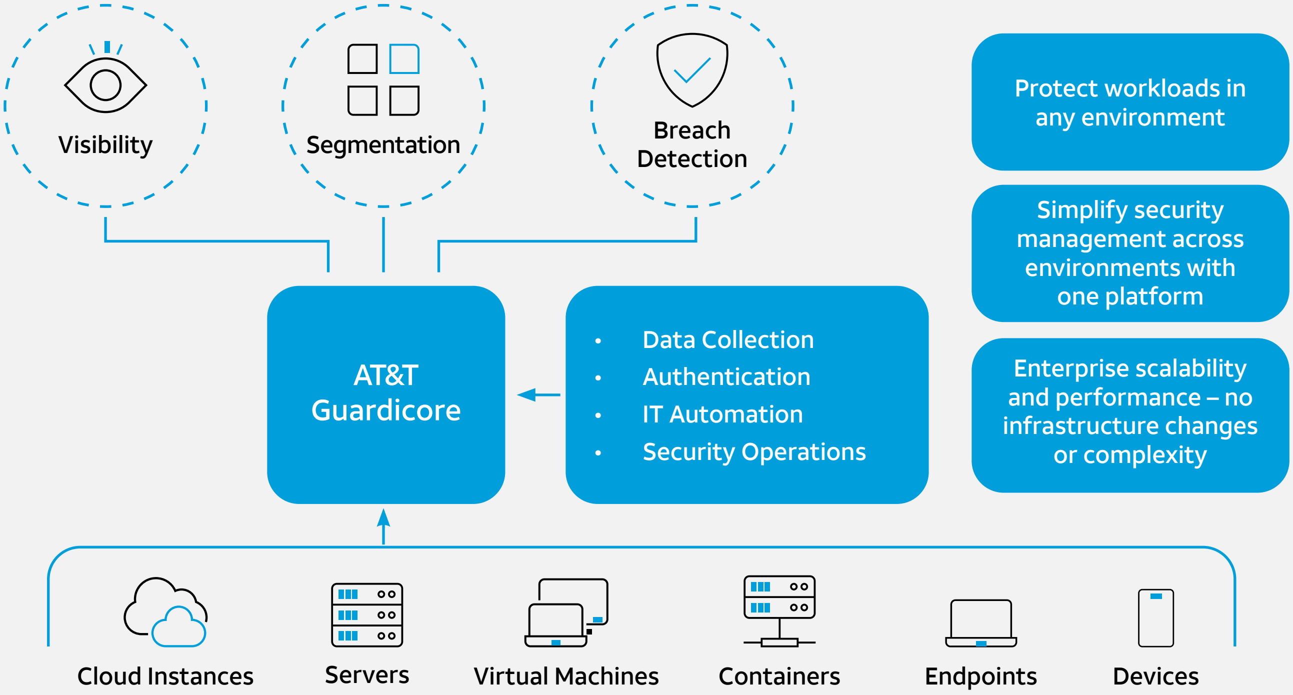
How it works

Legacy segmentation tools like firewall appliances, VLANs, and network security groups are slow to change and heavily dependent on network infrastructure, crippling IT agility and often resulting in business disruption. AT&T Guardicore is different. Rather than relying on the underlying network or cloud infrastructure for segmentation, it creates a software-based segmentation overlay that works across data centers and cloud environments.

AT&T Guardicore collects detailed information about an organization's IT infrastructure through a mix of agent-based sensors, network-based data collectors, virtual private cloud flow logs from cloud providers, and integrations that enable agentless functionality. Relevant context is added to this information through a flexible and highly automated labeling process that includes integration with existing data sources, such as orchestration systems and configuration management databases.

The output is a dynamic map of the entire IT infrastructure that allows security teams to view activity with user and process level granularity on a real-time or historical basis. These detailed insights, combined with AI-powered policy workflows, make the creation of segmentation policies fast, intuitive, and based on real workload context.

Comprehensive protection at scale



Visibility

Segmentation

Breach Detection

AT&T Guardicore

- Data Collection
- Authentication
- IT Automation
- Security Operations

Protect workloads in any environment

Simplify security management across environments with one platform

Enterprise scalability and performance – no infrastructure changes or complexity

Cloud Instances

Servers

Virtual Machines

Containers

Endpoints

Devices

Our holistic solution combines key capabilities required for achieving Zero Trust within your IT environment

Easy to implement policies

Policy creation is made easy with prebuilt templates for the most common use cases. Policy enforcement is completely decoupled from the underlying infrastructure, so security policies can be created or altered without complex network changes or downtime. In addition, policies follow the workload no matter where it resides – in on-premises data centers or public cloud environments. These segmentation capabilities are complemented by a sophisticated set of threat defense and breach detection capabilities, as well as threat hunting services.

What is Zero Trust?

Zero Trust incorporates these basic principles[1]:

- Trust no user
- Maintain total situational awareness about activities on the network
- Monitor and log what internal users are doing
- Inspect and log all incoming and outgoing traffic

AT&T Guardicore's value

- **Multiple protection methods.** Designed to integrate with your existing infrastructure. Integrate threat intelligence, defense, and breach detection capabilities to reduce incident response time.
- **Detailed, AI-powered segmentation.** Implement policies in a few clicks using AI recommendations, templates for remediating ransomware and other common use cases, and precise workload attributes like processes, users, and domain names.
- **Real-time and historical visibility.** Map application dependencies and flows down to the user and process levels on a real-time or historical basis.
- **Broad platform support.** Cover modern and legacy operating systems across bare-metal servers, virtual machines, containers, Internet of Things (IoT), and cloud instances.
- **Flexible asset labeling.** Add rich context with a customizable labeling hierarchy and integration with orchestration tools and configuration management databases.

Implement microsegmentation, stop lateral movement and security breaches with AT&T Guardicore

Why AT&T

AT&T Cybersecurity makes it safer for your business to innovate through network resiliency. We help to design, deploy, and manage the secure network that you aspire to by proactively identifying areas of cyber risk and preventive measures to protect digital connections.

To learn more, contact your AT&T Business representative or visit the AT&T Business website:
cybersecurity.att.com/products/guardicore

[1] Newton's Telecom Dictionary, 32nd edition