Reduce response time with automation and orchestration

AlienApp for Secure Web Gateway, powered by Zscaler enables expedited cybersecurity incident response

Defend, detect, and respond

For an organization to protect itself from cyber attacks, detecting and responding to threats quickly is critical. The sooner action is taken to mitigate threats, the less likely it is to cause a major disruption.

AT&T Managed Threat Detection and Response (MTDR), helps detect and respond to threats before they impact business. The AT&T Security Operations Center (SOC) provides 24/7 proactive security monitoring, security orchestration, automation, and more in one turnkey service, to enhance security posture quickly and cost effectively. With MTDR, organizations benefit from the powerful security orchestration and automation capabilities of the Unified Security Management (USM) platform and its pre-built integrations with other security and IT tools through the AlienApp framework. These integrations enable the ability to push and automate incident response actions through other security tools, including AT&T Secure Web Gateway, powered by Zscaler, providing broad threat coverage for highly effective early detection and rapid response.

AT&T Secure Web Gateway, powered by Zscaler offers organizations a way to apply unified protection against web-based threats for all of their users by restricting what sites they can access. But this solution goes far beyond simple URL filtering. AT&T Secure Web Gateway, powered by Zscaler utilizes dozens of threat intelligence sources to help protect users against the latest viruses, spyware, and other types of malware. Some editions also offer the ability to perform granular inspection on encrypted web traffic or protection against zero-day threats with sandboxing technology.

Potential benefits:

- Enhances efficiency of IT teams with 24/7 monitoring, including daily security operations of monitoring and reviewing alarms
- Equips organizations with flexible, cloud-based solutions that adapt to changing IT environments
- Provides centralized visibility across an entire environment: in the cloud, on premises, and across endpoints
- Enhances cyber defenses with easily implemented and unilaterally enforced single policy base for internet browsing occurring on-premises or by remote users
- Empowers administrators to quickly evolve and improve policy directly from the USM platform
- Modify or remove policies automatically to respond to threats dynamically

With AT&T Secure Web Gateway, powered by Zscaler, administrators can help provide that the websites their users interact with are both safe and appropriate for the workplace.

AlienApp for Secure Web Gateway, powered by Zscaler integrates AT&T Managed Threat Detection and Response and AT&T Secure Web Gateway, powered by Zscaler, providing a more comprehensive view of an environment and helping enable faster time to response through security orchestration and automation.

Ability to scale across a changing environment

As organizations accelerate their adoption of public cloud and SaaS applications for business productivity, IT environments are evolving quickly and attack surfaces are growing. Traditional security controls often lack the adaptability needed to support newer IT environments, meaning that business transformation is either slowed down by security concerns or, worse, charges ahead without proper security controls in place. Security monitoring programs must be able to keep up with changes in business, whether migrating services and workloads to the cloud, shifting to a more remote workforce, or opening new satellite offices or retail locations.

MTDR and AT&T Secure Web Gateway, powered by Zscaler offers flexibility that readily adapts to changing IT landscapes and provides a centralized view into an entire environment, making it easy to bring an additional location or environment online without having to install an appliance on site. When an anomaly is detected in the USM platform, the MTDR SOC analyst team can utilize the AlienApp for Secure Web Gateway, powered by Zscaler to implement and unilaterally enforce a single policy base for internet browsing occurring on-premises or by remote users. Together, the cloud-based solutions can help evolve security posture in response to any material change or expansion of environments.

Protecting today's shattered perimeter

There's a new reality when it comes to network security, driven by the idea that the "perimeter" is vanishing. Traditional protection and prevention controls, like firewalls, intrusion-detection systems, and malware protection, are no longer enough. Today's new, challenging environment warrants a re-examination of the tools and technologies used to protect organizations from cyber attacks.

Cyber criminals are constantly shifting their tactics, so in addition to protection and prevention controls, businesses need a way to continuously monitor what's happening on their networks, cloud environments, and critical endpoints, and to quickly identify and respond to potential threats.

AT&T Secure Web Gateway, powered by Zscaler represents the evolution of effective protection. Its technology "elevates" the security analyst so they can categorize events versus needing a deep understanding of networking. It humanizes policy enforcement, making policy applications easier. AT&T no longer speaks in IP's, but rather in users, groups, and categories of content and how customers think about permissions.

Using the AlienApp for Secure Web Gateway, powered by Zscaler, the MTDR SOC analyst team can quickly evolve and improve policy directly from the USM platform. By continually monitoring the customer's environment, detecting and validating threats, and then coordinating across AT&T Cybersecurity for remediation, MTDR analysts can work with the SWG team to add, modify, or remove policies to respond to threats dynamically.

Bridging the cybersecurity skills shortage

It's no secret that the cybersecurity industry is facing major talent shortage with little relief in sight. In fact, 59% of organizations report that they are at extreme or moderate risk due to cybersecurity staff shortage. Skilled security professionals are in high demand, making it a challenge for organizations to hire and retain top talent. To make matters worse, already understaffed security teams often struggle to focus on strategic security projects as they're busy dealing with the daily operations and maintenance of their security tools, reviewing and investigating noisy SIEM alarms, and manually updating security policies across their systems in response to incidents or vulnerabilities.

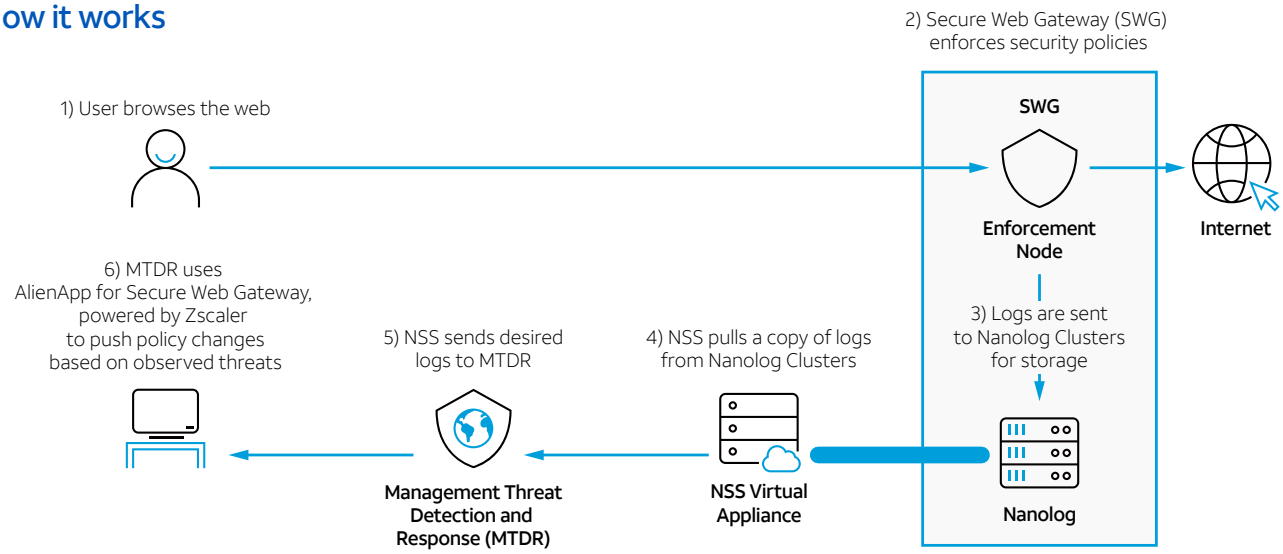
With AT&T Secure Web Gateway, powered by Zscaler and MTDR, technology teams will no longer need to continually monitor and tune firewall policy or a complicated SIEM deployment. AT&T SOC analyst teams are responsible for monitoring customer environments and critical IT assets 24/7 and handling the daily security operations of reviewing alarms and reducing false positives, so administrators can focus on responding to actual threats, rather than sifting through noise.

Reducing the impact of human error

People are the weakest link when it comes to security. Mistakes will be made, and every organization dealing with sensitive data or is worried about how a security threat can affect business continuity needs to have a strategy for rapidly evolving their access policies and monitoring their infrastructure. Early, effective threat detection that helps to enable a fast, coordinated response before the attacker has a chance to cover their tracks and move laterally throughout the network gives companies a considerable advantage in the fight for effective cybersecurity.

When a security incident occurs, the AT&T SOC analyst team works side-by-side with customers' incident responders to help them respond quickly and effectively. AT&T analysts conduct in-depth incident investigations on actionable alarms and escalate incidents based on severity, in accordance with United States Computer Emergency Readiness Team (US-CERT) Incident Reporting Guidelines. Investigations provide rich threat context on the incident, which may include additional threat intelligence, related alarms and events, conclusions, relevant files, an audit trail of activities, and response recommendations. This gives incident response teams a consolidated view of the situation, helping them act without delay. Throughout the incident response process, AT&T analysts are available 24/7 to provide support.

How it works



About AT&T Cybersecurity

AT&T Cybersecurity helps to reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our SaaS-based solutions with advanced technologies including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange™, and our relationship with more than 40 best-of-breed vendors, accelerate your response to cybersecurity threats. Our experienced consultants and SOC analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. With experience across all industries, we understand your business demands, and deliver the right insights, guidance, and solutions for you.