appgate

Today's Top Cyberthreats and How Zero Trust Network Access Defends Against Them

This whitepaper focuses on today's most common cyberattacks and how Appgate SDP, a Leader in *The Forrester New Wave™ Zero Trust Network Access, Q3 2021* report, defends against them.

Ransomware ○ DDoS Attacks ○ Insider Threats ○ MITM Attacks

ZERO TRUST NETWORK ACCESS **WHITEPAPER**

Introduction

It's a common refrain that an organization's overall cybersecurity approach—creating a strong posture, making good decisions and recognizing and responding to potential threats—is everyone's responsibility. While true, the reality is that nobody holds more responsibility than the IT, network and security professionals who architect the environment; establish policies; and select, install, configure and maintain the infrastructure and security solutions that safeguard those investments.

The need for robust security solutions has never been more important. Cybercrime is a lucrative business with high rewards and relatively low risk, perpetrated by motivated, skilled threat actors. And the monetary and reputational consequences for organizations that are breached can be devastating.

A number of factors complicate the task of safeguarding an organization's data and assets:

- **More attack vectors** are available for cybercriminals to find and exploit, including remote workers, third parties, unmanaged devices, cloud workloads, IoT devices and zero-day exploits
- **Flat network topologies** are often the product of complexity and perceived tradeoffs between security and convenience, which lead to unsanctioned lateral movement once an attacker has gained initial access
- **Complex perimeter-based solutions** are ill-equipped to secure modern enterprises characterized by work-from-anywhere policies, globally distributed workforces and hybrid workloads
- **Connect, then verify architectures** operate on the premise of a trusted network and weak authentication, introducing unnecessary risk
- **Overprivileged users** are the product of the complexity of managing legacy solutions and tradeoffs and have access to more information and systems than they require
- **Hybrid enterprise systems** include multi-cloud, on-premises and legacy infrastructure that each require different and disparate security controls

The Scope of Cybercrime

Make no mistake, cybercrime is a massive and growing problem: Cybersecurity Ventures, publishers of Cybercrime Magazine, estimates that global cybercrime costs will reach $6 trillion USD in 2021.[2]

The Human Factor

While plenty of attention is devoted to technical factors that complicate cybersecurity efforts, perhaps the most challenging factor is human error, including:

- Design flaws that create vulnerabilities in an application or gaps within a set of security solutions
- Implementation mistakes, like misconfigurations or patching oversights
- Operational errors, like clicking on a phishing email

Such errors are so ubiquitous—and the impacts so significant—that a 2021 study determined that 84% of serious incidents are caused by employees' mistakes.[1]

Unfortunately, there is no straightforward or single solution to the human factor. Consequently, cybersecurity professionals must avoid solutions that rely upon human infallibility; instead, the presumption of human error must inform solutions that limit its impact.

[1] Egress, "Insider Data Breach Survey" July 2021

[2] Cybersecurity Ventures, "Cybercrime to Cost the World $10.5 Trillion Annually by 2025" November 2020

Safeguarding modern enterprises with Zero Trust Network Access (ZTNA)

Legacy technologies haven't kept up with the pace of change within today's organizations—whether from an IT or workforce management perspective—proving inflexible in function and expensive to scale. In fact, rather than enabling necessary change, such solutions often become blockers, completely antithetical to the higher-level IT vision.

Securing access with Zero Trust principles—beginning with a foundation of ZTNA—is a vital, proven and readily attainable step toward strengthening defenses against today's threats and those that will emerge tomorrow.

The combination of proven value and flexibility is one reason why ZTNA is poised for rapid and widespread adoption, with Gartner forecasting that, *"By 2024, at least 40% of all remote access usage will be served predominantly by Zero Trust Network Access (ZTNA), up from less than 5% at the end of 2020."*[3]

White House Mandates Zero Trust

In response to many high-profile cyberattacks targeting critical infrastructure and government agencies, on May 12, 2021, the White House issued an executive order requiring federal agencies to adopt a Zero Trust architecture.

Industry-leading ZTNA: Appgate SDP

Appgate SDP delivers industry-leading ZTNA to anything from anywhere by anyone. It requires users to be fully authenticated across a range of identity-centric and context-based parameters, such as role, time, date, location and device posture, before permitting least-privilege access to enterprise resources (to prevent unsanctioned lateral movement).

Working within the existing security ecosystem to enforce the principles of Zero Trust, Appgate SDP delivers a single policy decision point that controls access across an enterprise's entire IT ecosystem. Exceptional integrations mean less rip and replace and more augment and optimize in order to strengthen and simplify access controls by putting existing systems and data to work.

Zero Trust Maturity Pays Off

According to the *Cost of a Data Breach Report 2021* by IBM Security and the Ponemon Institute, the average cost of a breach was 35% lower for organizations "in the mature stage of Zero Trust deployment" compared to those without ZT deployed.

On average, this figure equated to a difference of $1.76M USD per incident.

[3] Gartner, "Gartner Forecasts 51% of Global Knowledge Workers Will Be Remote by the End of 2021" June 2021

Ransomware

In many respects, ransomware is an ideal cybercrime business model. It has low start-up costs and high rewards that come with relatively low risk because prosecutions are rare. It should come as no surprise then that the rate of ransomware attacks has doubled year over year and ransomware now ranks as the third most common type of malware breach.[4]

Ransomware is big business—in fact, U.S. Homeland Security Secretary Alejandro Mayorkas estimated that victims collectively paid more than $350 million in ransoms in 2020.[5] Ransomware gangs make money by disrupting critical business operations and stealing (and threatening to release) valuable data—especially proprietary information, records that may trigger regulatory penalties and private/sensitive data that may be embarrassing to executives, like personal correspondence, contracts and compensation.

Headline-grabbing incidents (e.g., Colonial Pipeline, JBS Foods, Ireland's Health Service Executive, etc.) reveal the potential for disruption to business operations and the reality that even well-protected organizations are not immune to these attacks. And dealing with the impact of an incident can be costly, with the Cost of a Data Breach Report 2021 conducted by Ponemon Institute calculating the average cost of a breach at $4.62 million USD.[6]

Ransom Costs are Soaring

In the first half of 2021, the average ransom payment reached $570,000, representing an 82% year-over-year increase.[7]

Mitigating Ransomware with Appgate SDP

While Appgate SDP is not designed to protect against the initial deployment and execution of ransomware, it can nevertheless significantly reduce the impact.

Ringfencing controls a device or server's outbound connections, constraining its ability to receive data from command and control servers—severing a critical link used in manually directed (i.e., hands-on-keyboard) attacks. Ringfencing also limits the spread of ransomware with a bookended approach that prevents an infected device from initiating outbound connections to other devices and by limiting inbound connections on uninfected devices.

Microsegmentation precisely segments the network and resources to further restrict lateral movement and contain the blast radius of ransomware.

As an added defensive element, Appgate SDP's **device posture checking** can detect if a legitimate user's device has been compromised by a ransomware attacker, at which point SDP denies the device access to the network.

Combating Phishing

Phishing is one of the most prevalent and effective vectors used in the initial stages of many cyberattacks. Unfortunately, no amount of awareness training will ever entirely prevent people from clicking on malicious links, so security strategies must account for users becoming compromised.

Appgate helps to mitigate the impact of phishing using the same measures employed to combat ransomware: preventing lateral movement to mitigate an attack's reach and using dynamic device posture checking to inform what resources a user should be permitted to access.

[4] Verizon, 2021 Data Breach Investigation Report, 2021

[5] ABC News, "DHS secretary warns ransomware attacks on the rise, targets include small businesses" May 2021

[6] IBM Security and the Ponemon Institute, Cost of a Data Breach Report 2021, July 2021

[7] Dark Reading, "Average Ransomware Payment Hits $570,000 in H1 2021" August 2021

Distributed Denial of Service (DDoS) Attacks

A denial of service (DoS) attack is an attempt to make a particular device, service or network resource unavailable. The largest such attacks tend to leverage botnets as a distributed infrastructure, earning the moniker distributed denial of service (DDoS) attacks—a term often, though imprecisely, used as the general label for any DoS attack.

DDoS attacks come in many varieties, and while bandwidth floods tend to generate headlines because of their large scale, most cloud hosting services have sophisticated defenses against such attacks.

Arguably, a more significant risk for an enterprise is that an attacker will target a particular service or application by attempting to initiate or establish many concurrent connections—thereby exhausting the service's state memory or ability to process transactions—which does not require particularly high data volumes.

As cybercrime marketplaces mature, new attacks are developed and the cost of automation tooling continues to fall, the number of DoS attacks—and the risks for enterprises—continues to rise.

A Persistent Threat

Denial of Service attacks are one of the oldest threats, yet they have persisted due to their effectiveness, the ease with which they can be carried out and the difficulty of defending against them using traditional approaches.

Mitigating DoS Attacks with Appgate SDP

Attackers cannot target services that they cannot see, which is why Appgate SDP **eliminates attack surfaces** by making resources invisible until users are authorized. By "cloaking" assets, SDP disrupts the port scans that are often part of the reconnaissance phase preceding an attack.[8]

Instead of the "trust, then verify" approach of legacy solutions, Appgate SDP employs a "verify, then trust" approach using **single packet authorization (SPA)**. This tried-and-true technology makes the execution of a DoS attack more difficult, making you a much less vulnerable target.

SPA uses proven cryptographic techniques to make internet-facing assets (and the Appgate SDP solution itself) invisible to unauthorized users. Only devices that have been seeded with the cryptographic secret will be able to generate a valid SPA packet, which is used to "knock" on the receiving port—and only at this point does the asset become visible and is the user able to establish a network connection.

Importantly, SPA is embedded into Appgate SDP architecture. Outside of the regular implementation and configuration of Appgate SDP there is no bolt-on software required—it just works, as designed.

[8] IBM's X-Force Threat Intelligence Index 2021 reported that "Scan and exploit" was the initial attack vector in 35% of incidents observed by IBM Security X-Force Incident Response—edging out phishing (33%) for the top spot

Insider Threats

Insider threats come in a few forms:

1. **Negligent insider:** A careless user whose unsafe habits—like sharing passwords, leaving devices unattended or failing to recognize an impersonation scam—unwittingly aid an attacker
2. **Compromised insider:** A user whose account or device has been accessed and has fallen under the control of an attacker, whether through negligence or no fault of their own
3. **Malicious (or coerced) insider:** A user who intentionally causes harm, whether acting alone or under threat or influence from a malicious actor

Fortunately for organizations, malicious insiders are relatively uncommon and account for only 8% of data breaches.[9] Unfortunately for organizations—and as noted in the introduction—any system that involves humans is fallible.

Insider threats are particularly challenging to manage because:

- Visible activities and policies may inadvertently make employees feel judged or persecuted
- Insiders already have access privileges, so there may be fewer signals for automated security solutions to examine. This is particularly true in flat networks where lateral movement is difficult to identify and contain
- Employees are not the only insiders—contractors, vendors and other third parties may have system credentials, and managing secure access for such a diverse workforce can be cumbersome and prone to errors

Managing Third-Party Access

Legacy access solutions, like VPNs, have been at the core of data breach headlines reporting third-party overprivileged access that has led to far-reaching financial, reputation and sensitive data losses.

In contrast, ZTNA provisions secure access for third parties without introducing friction or complexity, providing granular access only to the resources each third-party user needs.

Mitigating Insider Threats with Appgate SDP

Appgate SDP allows organizations to implement safeguards against insider threats without introducing unnecessary friction that would compromise the workforce's ability to do their jobs.

Device ringfencing and **least privilege access** limit user access to only those network resources and services that are required. At the same time, Appgate SDP uses **dynamic policies** to adjust rights as the context in which they are requested changes, so it's easy to provision access as needed—overcoming many of the administrative headaches associated with more static management techniques.

And, as noted in the ransomware discussion, **device posture checking** can detect if a legitimate user's device has been compromised, at which point SDP denies the device access to the network. Similarly, Appgate SDP can receive vital context from other security solutions—like a security incident and event management (SIEM), User and Entity Behavior Analytics (UEBA) or extended detection and response (XDR) platform—that aggregate many signals to detect potentially malicious behavior.

Importantly, with Appgate SDP, management of insider threats doesn't require an all-or-nothing approach where a user either has some access or none at all. Instead, **surgical access permissions** mean that even if a user gets flagged or quarantined, administrators can still allow access to particular non-critical systems—so the user can keep doing their job even while investigation and remediation are underway.

[9] IBM Security and the Ponemon Institute, Cost of a Data Breach Report 2021, July 2021

Man-in-the-Middle (MITM) Attacks

In a man-in-the-middle (MITM) attack (also sometimes called a manipulator-in-the-middle attack), a threat actor intercepts communications—typically without the authorized users' knowledge.

Attackers can leverage MITM attacks to steal login credentials or personal information, spy on the victim, sabotage communications or corrupt data. There are many tactics, techniques and procedures (TTPs) that threat actors employ—many of which have been packaged into convenient and efficient tooling—but they all involve the attacker silently sitting in the middle, between the source and destination.

Given that they often fail to encrypt traffic, mobile devices are particularly susceptible to MITM attacks, which increases the risk for organizations with BYOD policies. Many IoT devices are similarly vulnerable, due to poor security practices.

While TLS encryption can provide a strong defense against MITM attacks, incomplete or outdated implementations and exploitable vulnerabilities mean that TLS by itself is not a failsafe solution. For example, while TLS can authenticate both parties involved in the communication, many implementations only authenticate one party. Similarly, poor certificate validation can lead to mistakenly trusting a threat actor masquerading as a legitimate party.

Mitigating MITM with Appgate SDP

Appgate SDP incorporates **dynamic rules** that enable users to access protected resources and that bind each individual device to specific users. SDP analyzes the user's identity, project/time and location and evaluates their context against pre-defined conditions before granting access.

Additionally, Appgate SDP uses **the full TLS standard to provide mutual, two-way cryptographic authentications (mTLS)**, while **validation** ensures that the device requesting access possesses a private key that isn't expired or revoked; that the device is running trusted software and is being used appropriately; and that the key is held by the proper device.

Finally, **SPA** provides another countermeasure to MITM attacks by obscuring the connection points on the network—so an attacker trying to position themselves between two parties will struggle to find or make the connections needed to execute the attack.

Conclusion

Many attack vectors expose organizations to risk from ransomware, DoS attacks, insider threats and MITM incidents. Traditional, perimeter-based security solutions are no longer adequate to handle the challenge. As exemplified by Appgate SDP, ZTNA provides effective risk mitigation and enables you to combat today's most prevalent—and potentially destructive—cyberattacks.

Appgate SDP is one of the few ZTNA solutions that gives you control over access with identity-centric micro-perimeters and that renders resources invisible with SPA. By leveraging a unique set of APIs, Appgate SDP allows you to build a well-ordered Zero Trust security ecosystem—giving you unprecedented control to automate access and increase visibility across silos, while keeping policies dynamically in sync with metadata. Your end users get a seamless experience with concurrent access to digital resources while restricting access for risky devices by using advanced posture checking.

Robust network access control is foundational to effective countermeasures. ZTNA should be a central pillar for combating today's worst threats.

Threat prevention is a significant benefit of ZTNA, but not the only one. Interested in learning more about the operational benefits that Appgate SDP provides?

Dive into industry-specific case studies and ZTNA use cases by downloading the Nemertes Real Economic Value report on Zero Trust.

Read Study

About Appgate

Appgate SDP is a leading Zero Trust Network Access (ZTNA) solution that simplifies and strengthens access controls for all users, devices and workloads. We deliver secure access for complex and hybrid enterprises by thwarting complex threats, reducing costs and boosting operational efficiency.

The full suite of Appgate solutions and services protects more than 600 organizations across government, Fortune 50 and global enterprises. Start your secure access journey, with confidence by visiting www.appgate.com/SDP.

appgate