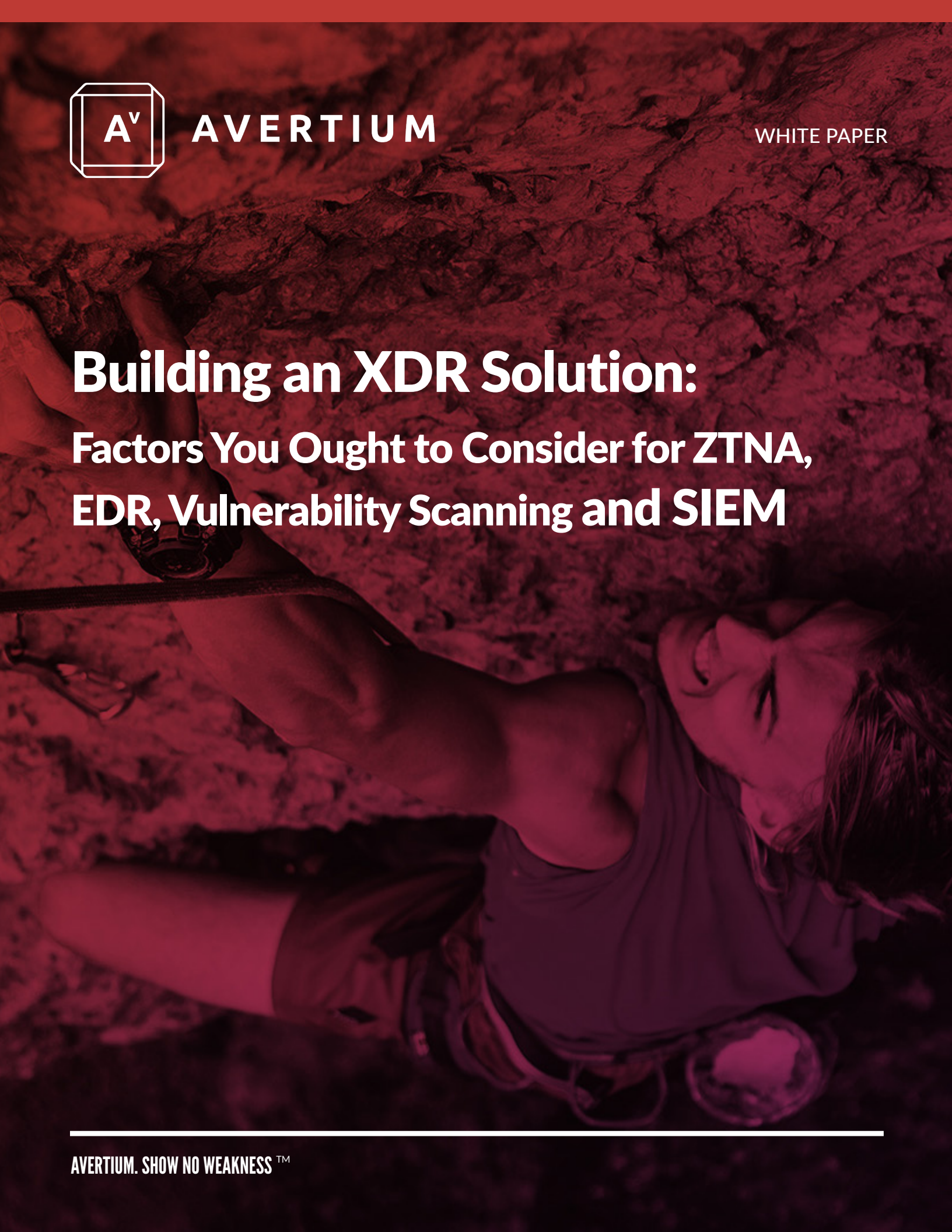

AVERTIUM

WHITE PAPER

Building an XDR Solution:

Factors You Ought to Consider for ZTNA, EDR, Vulnerability Scanning and SIEM

AVERTIUM. SHOW NO WEAKNESS ™

Table of Contents

Introduction

Over the last few years, CISOs have constantly battled evolving and more sophisticated spear phishing, CEO fraud and ransomware threats. Then Covid-19 struck, further complicating the threat landscape. The pandemic forced businesses to institute mass work-from-home policies, often without time to fully vet or test them.

> Zoom's daily meeting participants rose from 10 million prior to the pandemic to 300 million per day in April 2020. A massive rise in Zoom-themed phishing attacks followed, leading to the theft of Outlook, Office 365 and other credentials.
>
> - INKY

Loss of control of the perimeter combined with exploding usage of videoconferencing platforms have unleashed a wave of enterprise breaches according to Inky researchers. Zoom saw its daily meeting participants rise from 10 million prior to the pandemic to 300 million per day in April 2020. A massive rise in Zoom-themed phishing attacks followed, leading to the theft of Outlook, Office 365 and other credentials.

Endpoint detection and response (EDR), vulnerability scanning, and security information and event management (SIEM) tools detected many of these incursions – but not all. Hence the emergence of the zero-trust framework as an overarching security strategy to work in tandem with EDR, vulnerability scanning and SIEM to add rigor to security governance, strengthen organizational defenses and establish contextually aware access policies.

The resulting inflection point forces CISOs to decide the organization's future: Proactively adopt a comprehensive approach to secure the environment or remain at a heightened state of risk vulnerable to the expanding landscape, ever addressing incidents in reactive mode.

In this white paper we will discuss the ecosystem created by integrating these four technologies and their supporting processes around which CISOs must build a more rigorous, relevant and responsive cybersecurity program.

Zero Trust Minimizes Risk

Zero trust has emerged as a solution to the traditional castle-and-moat security posture. In conventional thinking, once you have successfully passed over the moat and been permitted entry into the castle, you are trusted to operate freely within its walls. But history teaches us time and again that sieges were often won swiftly once devious insiders gained entry and lowered the drawbridge.

It is the same in modern IT. Firewalls, passwords and two-factor authentication present a formidable barrier. But the bad guys are relentless in their efforts to circumnavigate these enterprise safeguards. Sooner or later, they will worm their way inside.

> Firewalls, single sign-on, endpoint management and VPNs have their place, but when they comprise a patchwork of products, blind spots are inevitable.

Hence the concept of zero trust: No longer are employees trusted simply because they operate on the corporate network. Instead of unrestricted access to the network simply because they are admitted, a zero-trust security posture harnesses contextual awareness to grant access to authorized users based upon patterns related to their identity, device security posture, time signature and network location. Unusual IP addresses, unfamiliar endpoints, device security posture problems, new applications or strange patterns of user behavior are flagged. Alternatively, within zero trust, access is dynamically allocated, and can similarly be dynamically withdrawn until the security team can triage and remediate the problem.

Applying this approach to users both on and off the network shores up the inherent shortcomings in the traditional approach of reliance on the controls at the network edge. Firewalls, single sign-on, endpoint management and VPNs for secure access have their place, but when they comprise a patchwork of point products, blind spots are inevitable. Advanced threat actors specifically target remote access products like Pulse Secure VPN, and it is only a matter of time before hackers discover their weaknesses and exploit them mercilessly to gain free rein to the network.

Zero trust, then, is a game changer. Its contextual security framework reinforces the lack of enterprise defenses in a bring-your-own-device (BYOD), work-from-home and cloud-enabled world.

But buyer beware. Some vendors misrepresent zero trust as a product. It is not.

Instead, it is an over-arching philosophy that underpins and enables an organization's security and technology strategy. Therefore, CISO's should pay attention to the following best practices when embarking on a zero-trust initiative:

- ✓ Conduct a comprehensive assessment of organizational technology environments and security controls to include the network, and all devices, applications and access points, to determine strengths, weaknesses and potential threats. This should include a thorough threat assessment to determine who is most likely to access the different types of data and applications, and to understand what safeguards are currently in place if the first line of defense is breached.

- ✓ Evaluate the capabilities of current security tools, processes, and staff to unearth weaknesses, vulnerabilities, gaps and blind spots.

- ✓ Evaluate additional technologies and services that may provide the functionality required to move closer to a zero-trust enterprise. Favor those products and services that not only fill the gaps, but also integrate well with existing tools and forward the goal of achieving a zero-trust architecture.

- ✓ Demo candidates to determine how well they align with your strategy. Inspect the technology's ability to granularly verify the identity of authorized users against criteria such as time of access, location, IP address, device security posture and more. This should include how well a potential new approach helps the organization develop scalable directories, institute micro-segmentation of data, and restrict access to privileged accounts and sensitive information.
- ✓ Conduct a detailed study of organizational workflows and data classification to define entitlements and access. This is a vital step on the zero-trust journey that cannot be overlooked.

Re-Evaluate EDR

Endpoint protection solutions have been around for some time. Older versions are no longer adequate for modern threat vectors. Even newer systems may be found lacking when it comes to adopting a zero-trust posture. Nevertheless, no zero-trust strategy is complete without a full-featured and well-integrated EDR element.

After all, the number and distribution of potential endpoints has ballooned in recent months as more workers operate from home. Core EDR capabilities such as cloud-based centralization, real-time monitoring, endpoint analysis and live incident response make it possible to achieve visibility to each endpoint regardless of their location.

EDR seeks to detect new as well as unknown threats and existing infections that come in via endpoints and servers. Its ability to identify unusual patterns and behavior, therefore, play an important part in any zero-trust strategy.

Detection technologies such as YARA, sandboxing, malicious process identification, threat intelligence integration and scanning are all part of the EDR arsenal. In addition, some EDR tools include retrospective analysis, event correlation and machine learning. Traditional endpoint tools are too reliant on rules, restrictions and signatures, and lack the muscle to combat targeted, multi-level incursions.

Selection of EDR solutions should be done systematically based on steps such as:

- ✓ Evaluate existing endpoint protection functionality across the enterprise. If a patchwork of tools from different vendors exists, determine which EDR platform is the best candidate for enterprise standardization.
- ✓ Additionally, evaluate any proposed standardization platform against core EDR capabilities such as:
    - Detection and prevention of hidden exploit processes that are more complex than a simple signature/pattern and often evade traditional AV.

- Integration within your existing security ecosystem should be a high priority requirement. Look for tools that work well with your SIEM, and if you do not yet have a SIEM, plan to add one to your security program.
- Threat intelligence capabilities that corral data about the various threats and threat actors that exist as a means of mitigating potentially harmful events. This augments overall security data collection efforts to establish a repository of attack and vulnerability data that can be harnessed for advanced analytics.
- Visibility into all endpoints including the applications, processes and communications in play to detect malicious activities and simplify security incident response.
- Automated alerting, and defensive response capabilities such as turning off specific processes when an attack is detected.
- Forensics to track how attackers managed to successfully negotiate enterprise defenses to gain access to critical systems and data. EDR should offer the ability to take a deep dive into the activities of bad actors to better understand their movements and minimize the impact of any breach.

✓ While the above criteria play an important role, product selection should also include an evaluation of potential solutions in terms of how closely they align with zero trust, digital transformation and other ongoing IT or security initiatives.

Vulnerability Scanning

> 60% of breaches linked to a vulnerability where a patch was available, but not applied
>
> - Ponemon Institute

Vulnerability management is a fundamental of a well-governed security program because getting the practice right dramatically reduces the potential for exposure. According to one study, 60 percent of breaches were linked to exploits against unpatched vulnerabilities.

Such alarming numbers highlight the importance of vulnerability scanning.

A variety of scan types can be used to inspect points of potential exploit, and to detect and classify system weaknesses. Some tools also predict the effectiveness of countermeasures. Others compare attack surface details to a database of information about known security holes in services and ports, as well as anomalies in packet construction, and paths that may exist to exploitable programs or scripts. Methodologies differ, too. Some log in as an authorized user and then scan. Others are conducted from an entirely external perspective. They scan the network and systems, seeking to find exploitable gaps.

Additionally, it is important to note the different between vulnerability scanning and penetration testing. Both practices seek to identify holes in security: The former indicates where potential vulnerabilities may lie. The latter is about actually exploiting vulnerabilities to see where they may lead, using the skills of a highly trained professional to identify attack vectors. And there are gray areas with tools performing both functions, or at least elements of each.

CISOs evaluating vulnerability scanning offerings are faced with several key decisions:

- ✓ Managed service or in-house operated? There are many managed service providers out there offering vulnerability scanning, and there are plenty of tools that IT can download to run in-house. It is a matter of balancing the time required, resources available, technical capabilities and cost.
- ✓ Proprietary or freeware? Vulnerability scanning tools come in all shapes, sizes and packages. Proprietary packages are often set up to be easy to use. But with the right skill set in-house, IT may be able to cobble together a series of complementary freeware tools to take care of the various aspects of vulnerability scanning. Proprietary tools obviously come at a price, but in some cases, the extra features and simplicity of operation may be worth it.
- ✓ Internal, external or both? Some scanners operate from beyond the firewall to see what holes can be exploited. Others work inside the firewall and find vulnerabilities from there. Probably, a balance of both types is required.
- ✓ With or without penetration testing? Vulnerability scanning and penetration testing are different animals. Those evaluating vulnerability scanning should determine whether they need to add pen testing capabilities as well. If so, they should consider solutions that encompass both.
- ✓ Specific or broad scanning: Some vulnerability scanners target website, Wi-Fi, specific platforms (such as AWS) or other vulnerabilities. Others scan more broadly across many different areas. If a definite area of weakness is being addressed, it may be wise to also consider scanners targeting that sector. enterprises and SMBs running mainly on the Amazon cloud.

SIEM's Holistic View

Security information and event management (SIEM) cuts through the noise generated by endless alerts and potential events by providing real-time monitoring, analysis and prioritization of data gathered from the many logs related to systems, network devices, applications and users.

A properly configured SIEM offers a holistic view of the technical infrastructure that is essential in spotting security threats, detecting and preventing breaches, and providing forensic information to learn how a security incident occurred and what its effect may have been. Further, it brings unity to the many disparate security technologies present in the enterprise. Firewalls, intrusion prevention, EDR, vulnerability data, IAM solutions, zero trust networking solutions, threat intelligence and other tools can be tied together under the SIEM umbrella.

How? SIEM platforms ingest log data from network hardware and software systems to analyze it in real time. This provides the ability to correlate events, spot anomalies and isolate unusual patterns of behavior that may indicate a security breach. Instead of IT having to deal with thousands of alerts, SIEM brings manageability to security monitoring, and makes it easier for personnel to correctly interpret ongoing events and zero in on hot spots. Many SIEM tools also generate reports for compliance purposes.

In many ways, SIEM helps to pull zero trust, vulnerability management, and EDR together into an all-encompassing security ecosystem. The benefits include faster detection and response, more efficient security operations, greater threat visibility and a reduction in security breaches.

CISO's looking to adopt or upgrade their SIEM platforms, therefore, should consider the following:

- ✓ SIEM is a discipline unto itself which requires technical and analytical processes built around it to produce the desired outcome of visibility into threats. Plan for more than just a product purchase as a SIEM requires ongoing care and feeding, as well as analysis of escalated events.
- ✓ SIEM tools have different feature sets, strengths and weaknesses. Evaluate solutions based on their ability to gather log data from existing systems, the availability of threat intelligence feeds, analytics capabilities, advanced profiling, automation capabilities, and artificial intelligence (AI)/machine learning functionality.
- ✓ Cloud-based SIEM platforms are generally more flexible and adaptable to modern hybrid cloud environments, and they simplify the management and monitoring of a remote workforce.
- ✓ SIEM tools differ in the number and variety of log sources they can connect to out of the box. Building connectors to additional devices and applications can be costly and time consuming. Choose the vendor that best supports the most relevant log sources for the enterprise.
- ✓ In addition to features, pay attention to how SIEM integrates with EDR and other key security systems, as well as how it facilitates zero-trust initiatives.
- ✓ SIEM tools continue to evolve. Decide whether you really need the latest and greatest in automation, AI and machine learning, or only need the basics. This not only reduces cost; it may avoid the need for an expensive and time-consuming rip and replace of existing tools.

Effective Risk Management

The days of on-premise IT are gone forever. Widespread cloud adoption, including the usage of SaaS platforms like Office 365 have broadened the enterprise perimeter along with the overall attack surface. The necessity to work from home during the pandemic has shifted the paradigm completely and a permanent return to the office is unlikely for many. Over time, the virtual workplace is inexorably becoming the norm. Traditional access management, user authentication and perimeter protection technologies, therefore, can no longer be relied upon.

Adoption of a zero-trust strategy is the best way to rise to the challenge. It assists CISO's in instituting a new era of user identity and privilege. It also brings clarity to the product selection process and provides a pathway towards digital transformation while staying firmly in control of risk.

However, zero trust should not be looked upon in isolation. It is best viewed as a package that includes EDR, vulnerability scanning and SIEM. Together, these four elements help the CISO to establish a solid foundation for a comprehensive security program.

In an increasingly digital environment, CISO's must come to terms with the proliferation of threat vectors without inhibiting flexibility and agility. This is only possible by shifting to an approach that does not assume that anything or anyone inside the perimeter is safe and can be trusted.

Managed security by Avertium offers a unifying ecosystem approach including tightly coupled zero trust, EDR and Managed Detection and Response (MDR), vulnerability scanning and SIEM that is strong enough for this brave new world of security. In addition, Avertium provides the structure, expertise and services to ensure a smooth transition from a castle-and-moat architecture to one that fits the amorphous nature of the modern enterprise.

There is no escaping the fact the security exposure has grown significantly in recent months. Coupled with control fragmentation, a firmer level of security governance is required. Avertium offers the discipline and best-practices-based framework needed to rise to this challenge and re-establish a resilient security posture.

About Avertium

Avertium brings enterprise-level security to mid-sized and larger organizations challenged by the cybersecurity talent shortage, rapidly evolving threat landscape and budgetary constraints. The company's acclaimed show-no-weakness approach to extended detection and response (XDR), governance and compliance, and strategic advisory services is redefining the managed security services category. From financial services and manufacturing, to technology and healthcare, more than 2,500 companies rely on Avertium's more rigorous, more relevant, and more responsive delivery of cybersecurity services. Backed by growth equity firm Sunstone Partners, Avertium operates CyberOps Centers of Excellence in Arizona, Colorado, and Tennessee. For more information, visit www.avertium.com.

Avertium. Show No Weakness.™

AVERTIUM

+1 (877)-707-7997
hello@avertium.com
www.avertium.com