Brite's Cybersecurity Methodology

A Simplified and Thorough Approach to Cybersecurity

Brite

Brite's Cybersecurity Methodology

A Simplified and Thorough Approach to Cybersecurity

Modeled from industry best practices, and decades of working with organizations of all sizes in various industries, Brite's Cybersecurity Methodology outlines five tenets which logically group solutions to implement a strategic cybersecurity program. These tenets are not a new methodology, but a consolidation of the existing standard frameworks with a focus on confidentiality, integrity and availability. Our customers find that conversations and projects easily align when utilizing Brite's Cybersecurity Methodology.

Detect and Protect | You can’t protect what you can’t see

63% of organizations lack asset accounting.[1]

The explosion in the number of devices (IoT, OT, endpoints, servers, etc.) and increasing sophistication of attack methods creates a multitude of visibility challenges. By continuously identifying devices, capturing detailed information and understanding the normal network traffic flow, we can begin to automate the detection of anomalous behavior and improve both automated and manual remediation. Breaches are inevitable, and stopping the spread is critical to limiting the damage. Without true, real-time, granular visibility unauthorized users, unmanaged devices and unexpected data flow go undetected and can wreak havoc an on environment.

The objective of Detect and Protect is to collect solutions that build a foundation of security insights to guide informed decisions. In today’s environments, ***how do you identify and remediate threats on and off your network?***

To satisfy the needs in Detect and Protect, the five key components are:

- Complete Visibility Into All Software on Managed and Unmanaged Connected Devices
- Complete Visibility Into All Traffic on the Network
- Known Vulnerability Assessment and Remediation
- Incident Notification and Automated Response
- Real-Time Threat Detection

Complete Visibility Into All Software on Managed and Unmanaged Connected Devices

Discover, classify and assess devices and what is installed on them the instant they connect to the network. Additionally, maintain that visibility while working remotely or off traditional networks. Utilized gained insights to drive remediate of potentially problematic devices.

Complete Visibility Into All Traffic on the Network

Visibility doesn’t stop with the device. Controlling network traffic through visibility and network segmentation reduces the internal attack surface. Limiting lateral movement across the network contains an attack to one section, decreasing the overall impact of a breach while increasing detection chances as the attacker attempts to move laterally. By understanding the level of risk and cost of protection, segmentation enables cost-effective, risk-based cyber-security programs.

Known Vulnerability Assessment and Remediation

Out of date systems are easy targets. Luckily, patching can be an easy process if resources are available and a reliable, proactive approach is in place. Vulnerability assessment tools identify systems with known vulnerabilities and help prioritize its remediation.

Incident Notification and Automated Response

Quick, effective incident notification is essential for containing the scope of an attack. Pre-determined steps and policies help to notify resources or trigger an automated response. The continuously gathered information prompts a domino effect of decisions within security tools that can then automate remediation and secure the environment. Additionally, syncing tools allows for integrated logs and improve time to incident identification and resolution.

Real-Time Threat Detection

Threats come from multiple directions. Undetected users, devices and traffic allow for attackers to move through the network. Eliminate the risk with real-time threat detection and stop hackers in their tracks

The biggest advantage against attackers is knowing who, with what device and where on the network they are in real-time. Control unauthorized users and unmanaged devices instantly for heightened security through wholesome visibility across toolsets.

Remember, you can't protect what you can't see.

Secure Access | Ensure people are who they say they are

Secure Access has become more important than ever with the overnight change in our work environment due to the response to COVID-19. As the physical perimeter has dissolved, we have encountered the challenges of delivering secure, stable and reliable access on a variety of unknown networks and devices. In addition, the verification of what users have access to and should have access to has pole-vaulted Secure Access to the top of the priority list.

Over 80% of hacking breaches stole or used credentials.[2]

The solutions within the Secure Access tenet deliver secure, appropriate and audited access to critical systems, applications and data. The objective is two-fold - First, it is to prevent unauthorized, undetected system access. Secondly, it ensures authorized users have secure and reliable access to required systems, applications and data. Evaluate your current secure access approach by asking: *How do you audit, monitor and control access for users, systems and privileged accounts?*

Secure Access is achieved by utilizing solutions for:

- Privileged Account Access, Control and Monitoring
- Shared Folder Access, Control and Monitoring
- Multi-Factor Authentication
- Secure Remote Access
- Identity Access Management
- Mobile Devices Management

Privileged Account Access, Control and Monitoring

Privileged account users hold the keys to the kingdom. Their roles require access to sensitive information, typically with administrative rights. These accounts have come under attack due to their elevated privileges and access to systems. Detailed auditing, dynamic password changes and password vaults aid in securing these vulnerable accounts.

Shared Folder Access, Control and Monitoring

Critical data lives within files and folders no matter where they are stored - on premise or in the cloud. Discover, monitor and manage access with the proper tools and controls to understand and receive alerts when unusual activity is detected.

Multi-Factor Authentication

Verify a user's identity with a combination of two more credentials as an initial line of defense to protect against unauthorized access. Credentials include *something you know* - username and password, *something you have* – hardware token or mobile device, or *something you are* – fingerprint, retinal scan and facial recognition.

[i]

Secure Remote Access

Gaining control of remote access is the initial step in controlling access to the corporate network and systems as IoT devices enable the shift away from traditional workspace to remote working. Remote access can also exist in direct-to-cloud applications, such as O365, Salesforce, etc. Whether accessing your private data center, cloud services or a hybrid, ensure you have visibility into the users, level of access and activity monitor activities.

Mobile Devices Management

The era of BYOD and IoT instigates the need for insight and control into non-traditional managed devices and the security of data on non-company devices. MDM solutions are relatively easy to deploy and provide device inventory, application control and remote wiping capabilities necessary to allow resource access.

Identity Access Management

Deploy a full identity access management (IAM) program across the organization to ensure secure and appropriate access through an individual's digital identity. Ultimately, protecting business-critical data with a comprehensive IAM program that integrates IT departments and HR systems is essential for establishing a dynamic role-based access methodology.

Secure Access's approach can be simplified into three steps: verifying the identity of users, managing and containing access to only the necessary areas, and finally monitoring for unusual activity to detect potential breach in real-time. These steps ensure the security of critical assets.

Advanced Threat Prevention | Protect against advanced, evolving threats

70% of breaches still originate at the endpoint.[3]

The expansion of mobile and fluid corporate environments has prompted an evolution of endpoints. These devices are beyond the coverage of perimeter gateway solutions. As the way we work continues to change, so do the targets. As evidence, there was a 667% increase in phishing attacks in March 2020 alone.[4] Security professionals are forced to evaluate advanced threat prevention capabilities, especially with the majority of staff physically out of the office working on endpoints connected to potentially unprotected networks.

The objective of Advanced Threat Prevention is to provide proactive measures against today's most advanced threats. Assess your current approach by asking: ***How do we prevent advanced threats on or off your network?***

The key components of Advanced Threat Protection include:

- Next-Gen Perimeter Defense
- Extending the Perimeter
- Advanced Endpoint Protection
- Email Security
- Anomaly Detection (Anti-Bot)
- Incident Response and Remediation
- Advanced Forensics and Event Analysis

Next-Gen Perimeter Defense

Traditional perimeter security is no longer a viable defense for today's complex attack portfolio. The Next-gen approach utilizes technology, AI and human expertise to protect, detect and remediate against both known and unknown threats. For advanced prevention, orchestration and automation technologies paired together deliver faster detection and response capabilities.

Extending the Perimeter

With today's cloud transformation, the perimeter does not have a definitive line. The same level of protection is necessary for applications and resources that reside in public, private and hybrid cloud environments.

Advanced Endpoint Protection

The increase of IoT devices and remote work have significantly increased endpoint security risks. Advanced endpoint protection leverages artificial intelligence against known signatures to detect abnormalities, protect against fileless attacks and learn to detect similar threats.

Email Security

As email continues to be the dominant form of business communication, it has become a reservoir of business data, making it an attractive target for spam and phishing attacks. Comprehensive email security suites address both inbound and outbound concerns. Inbound, protect against unwanted and fraudulent emails as well as providing business continuity and archiving. While outbound emails are analyzed to prevent data loss.

Anomaly Detection (User Behavior Analytics)

Humans are random and unpredictable in their use of applications and accessing data. Fortunately, bots are systematic. Through machine learning, we are able to detect anomalies and set off a series of steps to ensure bad actors are not at play. By combining user behavior analytics with anti-bot defenses, command and control of system can be stopped before the damage is done.

Incident Response and Remediation

Real time response is critical in quick remediation of attacks. The first step in incident response is to detect and identify the cause of the attack. After understanding the context, block the breach and remediate the areas affected. Finally, critically assess and analyze the breach.

Advanced Forensics and Event Analysis

Learn from past incidents by thoroughly investigating events to gain a deeper understanding of the incident. This information can inform the evolution of security measures to increase future protection.

A strong, AI-powered offense prevents against the latest threats, while automated remediation mitigates the effects of an intrusion. Together both prevention and response create a strong Advanced Threat Prevention strategy and secure organization.

Data Protection | Proactively protect your crown jewels

Data - the crown jewels, golden ticket and treasure chest for attackers. The importance of data varies by industry and the impact of data loss with it. Due to its' significance to business operations and potential value on the black market, it is an incredibly lucrative target for attacks. Because of this, security professionals need to evaluate their data and appropriately protect it.

> 53% of companies found over 1,000 sensitive files accessible to every employee.[4]

The objective of Data Protection is to automate the assessment and prioritization of data. The daunting nature of this task is offset with a set of tools and rule sets. To evaluate your current position with data, ask yourself: ***How do you protect your organization's critical data?***

To mitigate the risk of attacks, this tenet emphasizes the protection of:

- Data at Rest
- Data in Motion
- Data in Use
- Data in the Cloud

Data at Rest

The most basic form of data protection, protecting inactive data where it is stored. Protection in this phase includes ensuring that data typically located on a file share, within a laptop or server, is not being accessed without authorization. Encrypting data at rest has become a standard, especially for those devices not protected by physical security.

Data in Motion

Data is constantly being shared. Keeping that data safe when traveling from point A to B is critical for a data protection strategy. Data in motion looks to protect the transfer of data through encryption of email, removable media or secure transfers.

Data in Use

Protect data in non-persistent digital states by utilizing role-based access to ensure people can access the data they need for their role, and nothing else. Then, utilize identity management tools to ensure those accessing and using the data are who they say they are at the time they are accessing the data.

Data in the Cloud

As cloud adaptation becomes increasingly necessary, a cloud data strategy is also needed since the cloud is not inherently safe. First, be sure you understand your cloud storage agreements and considering using an encrypted cloud for sensitive data. Next, be serious about identity verification through multifactor authentication. Finally, gain visibility of all east-west cloud traffic to ensure there is no unauthorized access.

Protect data from all angles to ensure your crown jewels and sensitive data is safe. By addresses each stage of data, you can create a comprehensive data protection program.

Governance, Risk and Compliance | Ease the burden and make more informed decisions

Only 18% of organizations leverage automated processes for IT risk data collection and reporting.[5]

Compliance, audit reporting and vendor risk management are time consuming tasks. The increase in cybersecurity regulation awareness has fueled the need for continuous monitoring, consistent reporting and regular auditing. The driving force may be an industry or government regulation like GDPR, SOX, HIPAA, etc. or driven by the client/vendor relationship. In other cases, the requirements are driving the internal demands of the organization's need to manage third-party vendors.

The objective of Governance, Risk and Compliance is to provide industry standard suites to shorten time to compliance both for regulation and third-party vendors, easing the reporting demands and enabling more insightful decisions. Start your journey by asking: ***How do you continuously measure compliance and mitigate risk?***

Together, the three areas of Governance, Risk and Compliance influence the framework and requirements of a security program. Key components include:

- Compliance scanning and monitoring
- Vulnerability scanning and management
- File integrity management
- Vendor risk monitoring and management
- Security check-ups and assessments

Compliance Scanning and Monitoring

Properly evaluate if specific areas of the environment are compliant based on either the standards set by the organization or external regulations, without the need for a highly manual process.

Vulnerability Scanning and Management

Non-remediated known vulnerabilities leave organizations at risk for attacks, unnecessarily! Vulnerability scans identify any known vulnerabilities and provides additional information on the proper remediation steps. Go one step further and implement tools and processes for automated scanning and remediation.

File Integrity Management (FIM)

Automatically identify abnormal files changes and suspicious activity on critical files with a proactive FIM tool. Easily detect and contain corrupted systems before they wreak havoc on your environment.

Vendor Risk Monitoring and Management

An essential program to limit risk and liability when working with third parties to eliminate backdoor vulnerabilities. Vendor risk platforms help score the cybersecurity programs of vendors as well as facilitate the necessary questionnaires to ensure third-party compliance.

Security Check-ups and Assessments

Security is a continuous, on-going process. Regular check-ups and assessments help organizations stay on-track and improve its security plan.

Governance, Risk and Compliance sets both state and company standards to assess and evaluate against to ensure that proper security measures and deployed and successful to mitigate risk.

In Conclusion

These five tenets provide a comprehensive approach to today's cybersecurity landscape. Each tenet builds on the previous, enabling organizations to strategically implement a complete program. However, security doesn't stop at initial implementation. It is a continuous, on-going journey where a few things need to be remembered:

A tool is only part of the solution

With the constant state of evolving attacks and regulations, it's understandable to be overwhelmed with where to start. While Brite's five tenets outline the necessary tools to help, it's only part of the solution. There is no "magic bullet" to save you. It's a continuous process to achieve a proactive security approach.

Ensuring long-term improvement and success

To orchestrate tools and improve security, utilize tools to measure and demonstrate continuous improvement. A few key insights help to measure improvements are:

KPI's: Show how the business is performing based on goals and objectives set by the organization's leadership. Ideally, this showcases a positive trend over time.

KRI's: Understand the risk based on the current state and the future desired state. These should be based on established standards and contain severity and probability of occurring.

KCI's: Understand the controls that are in place and how effectively they are at meeting the desired objective.

Overall, strategic management, evaluation and improvements will lead to a longstanding, secure organization. Ease the long-term commitment to continuous security by partnering with Brite. Combine years of experience, a team of advisors and engineers with a suite of services and partners to implement a strategic, secure plan.

1. Forescout/ ESG, Forescout: Ensuring Business-centric Device Visibility Across the Extended Enterprise, 2019
2. Verizon, 2020 Data Breach Investigations Report, 2020
3. CrowdStrike, 2019 CrowdStrike Global Security Attitude Survey, 2019
4. Varonis, 2019 Global Data Risk Report, 2019
5. KPMG/ Forbes Insights, Disruption in the New Norm: Tech Risk Management Survey Report, 2018