ADVANCED THREAT PREVENTION (ATP)

The threat landscape exponentially expands with our ever-increasing digital adoption, presenting a shifting set of challenges for cybersecurity professionals. Unknown threats, disconnected mobile devices and shadow IT require a change from protection to prevention. Companies can combat these advanced threats with a layered defense approach at each attack vector. Combined with active threat monitoring and management, organizations are prepared for when - not if - an attack occurs.

WHY ADVANCED THREAT PREVENTION?

Proactive Defense vs Reactive Recovery

Get ahead of complex, advanced threats by creating a strong and adaptable defense. It is much easier and more cost effective to prevent an attack than to recover from one.

Defend the Attack Surface

Defend the organization's attack surface by identifying and mitigating vulnerabilities, reducing the risk of security incidents, and increasing the organization's ability to respond to and recover from attacks.

Centralized Context & Correlation

Cyber attacks are complex with many aspects. ATP enables centralization, cross-source context and correlation of information for better defense and quicker response.

NextGen Perimeter Defense

Protect the network against a wider range of cyber attacks using advanced features like deep packet inspection, application awareness, and machine learning to identify and stop cyber threats in real-time.

Advanced Endpoint Protection

Use machine learning, behavioral analysis, and threat intelligence to detect and prevent a wide range of cyber attacks, including malware, ransomware, and zero-day exploits on individual endpoints.

Email Security

Protect against email delivered cyber attacks like phishing and ransomware by utilizing AI to scan, block or quarantine suspicious messages.

Cloud Security

Gain visibility into cloud resources, secure cloud infrastructure and applications, detect and respond to cloud-based threats to prevent cyber attacks and minimize their impact.

User Awareness Training

Significantly reduce the number of successful attacks by training and testing users to be a vigilant line of defense.

Identity Protection

Protect user credentials with a complete identity program to reduce the risk of unauthorized access to sensitive systems and data, prevent account takeover and mitigate the impact of security incidents.

Incident Detection & Response

Identify and respond to security incidents quickly, minimize the impact of an attack, and prevent similar incidents from occurring in the future.

Brite

Brite.com
1.800.333.0498
SalesInfo@Brite.com