SOLUTION BRIEF

Reevaluate your Endpoint Strategy

The Key Security Battleground – The Endpoint

The endpoint device is the key cybersecurity battleground. It's where the data, users, and the Internet meet, and where attackers focus their efforts. Organizations know this and invest in endpoint security solutions to mitigate the risk. Since attacks like phishing and ransomware still succeed, a different approach is clearly needed.

Why do endpoint attacks keep succeeding?

Most endpoint security architecture depend on two solutions. First, Next Generation Antivirus (NGAV) is used to counter known threats, and to some degree variants of those threats. Second, Endpoint Detect and Response (EDR) solutions are often installed. EDR attempts to detect evidence of attacks that have evaded NGAV, but can do little to stop them. EDR can provide forensic data to help defend against similar attacks in future, but doesn't prevent the initial infection.

ENDPOINT PROTECTION PLATFORMS (EPP)

- Known as Antivirus (AV) or Next Gen Antivirus (NGAV)
- Good for stopping known threats or file behavior anomalies

ENDPOINT DETECTION & RESPONSE (EDR)

- Detects suspicious activity and provides remediation suggestions
- Good for providing visibility to new threats or variants of existing threats

With this baseline, it's fairly easy to see why attacks still succeed. They use obfuscation techniques that bypass NGAV and EDR, and leverage social engineering to fool users into supporting the attack by clicking on links and opening docs. So, what's needed is a more "inherently protective" approach: one that ringfences the operating system and data so that no matter how an attack gets on a PC, it can't steal information or establish a permanent foothold.

Threat Containment – “Inherent Protection” at the Endpoint

HP has developed a unique approach to endpoint protection succeeding where NGAV and EDR fail. The approach, called “Threat Containment”, uses isolation technology to run each potentially risky action (like opening an email attachment) in an isolated space. The isolation is enforced by CPU hardware, so any malware that might be present can’t get around it. And when the task is completed, the isolated space is destroyed, taking the malware instance with it.

THREAT CONTAINMENT

- Uses micro-virtualized machine (μVM) to protect each task
- Stops malware regardless of behavior or identification and provides forensic visibility into the malware helping close the endpoint security gap

The isolation concept in Threat Containment is similar to that used by data center hypervisors. These allow multiple applications to run on common hardware, and prevent each application from directly accessing the hardware, hypervisor kernel or other applications. HP has taken this proven architecture and extended it to the endpoint PC with performance and resource optimizations necessary to ensure consistent user experience. Our “micro-virtualization” approach avoids the CPU and memory requirements of traditional hypervisors, and is specifically optimized for the most common attack vectors: Office documents, PDFs, and web links.

Threat Containment compliments NGAV and EDR to provide a comprehensive endpoint protection architecture. NGAV filters out the more obvious known threats, while EDR provides strong forensics to support security operations researchers. Threat Containment delivers the final element: a zero-trust per-task protective shield that assumes that untrusted documents and links may be compromised, and should therefore be isolated during execution.

Solution Benefits for All Stakeholders

Threat Containment is unique not only in its technical approach, but in the broad range of benefits it confers to the organization.

RISK MANAGEMENT

- Zero-trust approach
- Protects personal and corporate usage
- Inherently protects

VISIBILITY

- Safe space for malware observation
- Mimics environment for superior threat intelligence
- Cloud analytics for historical analysis

USER EXPERIENCE

- No changes to user workflows
- No remediation needed
- Work with confidence
- Performance maintained

OPERATIONAL EFFICIENCY

- Minimize security tools
- Reduce support tickets
- Fewer false positives
- Less endpoint remediation

COMPLIANCE AND AUDIT

- Meet control objectives
- Compensating control for patching

HP THREAT CONTAINMENT SOLUTIONS: SURE CLICK ENTERPRISE[1] AND WOLF PRO SECURITY[2]

Sure Click Enterprise is HP’s Threat Containment solution for larger organizations. It supports the flexible policies and broad integrations enterprises demand. Centralized management can be deployed either on-premises or in the cloud, and Credential Protection is included at no additional cost. Smaller organizations should consider Wolf Pro Security: it provides Threat Containment with simplified management and optional NGAV.

Summary

When building your endpoint strategy, you need to choose efficient solutions to minimize risks and security solution management. Using traditional EPP and EDR solutions are not enough. Threats are bypassing these solutions causing increased alerts taking up IT security team resources. Adding Threat Containment allows your organization to deliver greater operational efficiency through a zero-trust security approach maximizing endpoint protection while lowering costs without impacting employee productivity. It fills the security gap left by EPP and EDR alone.

[1] HP Sure Click Enterprise is sold separately. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed. For full system requirements, please visit System Requirements for HP Sure Click Enterprise for details.

[2] HP Wolf Pro Security is available preloaded on select HP devices, is available as a subscription and in term licenses. Contact your HP sales representative for more details.