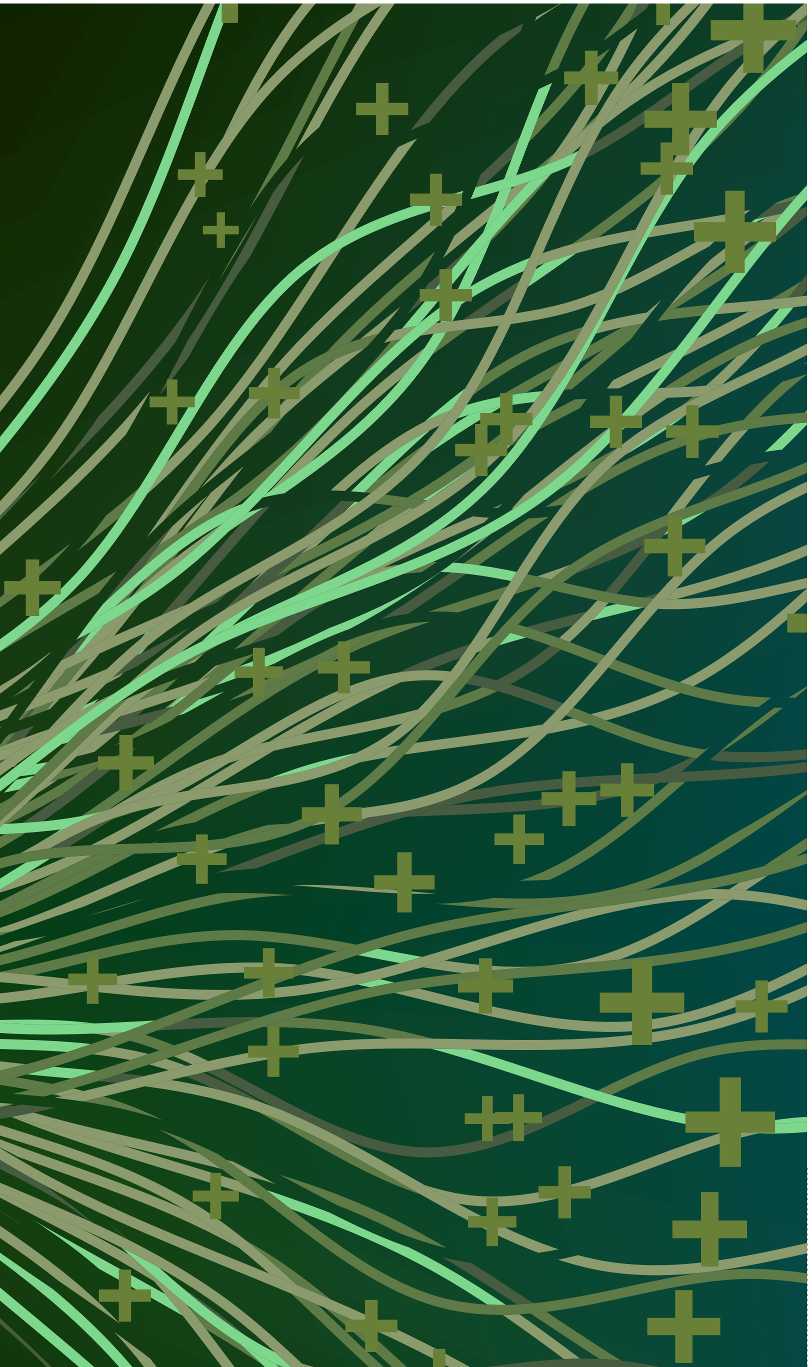

E-Guide

SUPPLEMENTARY DEFENSES FOR ENDPOINT SECURITY

TechTarget | SearchSecurity

Home

Supplementary defenses for endpoint security

LEARN HOW NETWORK access control, data loss prevention (DLP) and robust data destruction can secure endpoints and protect enterprise data.

Home

Supplementary defenses for endpoint security

SUPPLEMENTARY DEFENSES FOR ENDPOINT SECURITY

Mike Cobb

Given the diversity of devices, combined with the wide assortment of users that now connect to an enterprise network, absolute endpoint protection is virtually impossible. There are various technologies, though, that can help safeguard data stored on endpoints while protecting the network from devices that may be vulnerable to attack or already compromised. This technical tip looks at how network access control (NAC), data loss prevention (DLP) and robust data destruction can help secure endpoints and prevent them from putting enterprise data at risk.

WHAT NAC DOES

NAC is a key technology for admission control based on the overall security posture of a user and his or her device. Pre-admission security policy checks, and the ability to automatically remediate non-compliant devices, ensures each endpoint meets a minimum level of compliance before it can connect fully connect to the network. This not only ensures that endpoints are capable

Home

Supplementary defenses for endpoint security

of protecting themselves from attack by malware, but stops them from putting the rest of the network at risk. NAC can leverage user and device profiles in backend data stores, such as LDAP, RSA and Active Directory. This enables routers, switches and firewalls to work together to determine who and what is trying to connect to the network, and assign the appropriate access. This provides greater coordinated defense-in-depth with security controls able to share their knowledge of network and device behavior.

NAC products can provide quite detailed information about the status of an endpoint's security: Are all necessary patches applied? Is hard-drive encryption enabled? Is the host-based firewall running? Which ports are open? While answering these concerns, and more, context-aware capabilities provide ongoing protection during each network session. Support for more specialized equipment -- such as point-of-sale systems, kiosks, supervisory control and data acquisition systems that may connect to the network -- is also important, as is integrating NAC with mobile device management technologies so that the security status of mobile devices can also be checked.

Home

Supplementary defenses for endpoint security

WHERE DLP FITS IN

While NAC can keep endpoints compliant and control their access to resources, DLP technologies can protect data on endpoints from unauthorized attempts by careless or malicious users to copy or share it. DLP tools use deep content filtering to inspect and control the data a user or device is trying to download, copy, print, share, or transfer to both prevent unauthorized use and stop sensitive data from leaving the network. This provides real-time data protection as user accounts can be automatically disabled, or devices quarantined as soon as a suspicious data (i.e. large uploads or downloads, odd login times, etc.) transfer begins.

They can either be standalone or cloud-based tools, or integrated into existing endpoint security suites. Extending data loss prevention to mobile devices, whether corporate- or user-owned, usually requires some form of mobile device management product. Many of these can also ensure data on mobile devices is always encrypted.

REQUIRED: DATA DESTRUCTION POLICY

Encryption should of course be used on all endpoints, but the less sensitive data left on endpoints, the better. The turnover of network endpoints has never been

Home

Supplementary defenses for endpoint security

higher, and data destruction polices need to be applied to all devices that have the ability to store data. Correctly sanitizing an endpoint's drive or flash storage when it is reassigned or decommissioned is essential in order to destroy all the electronic data on it; normal file deletion commands only remove pointers to the data, which means it takes only a trivial effort, using common software tools, to recover the actual data.

Reducing the number of endpoints holding forgotten copies of classified information reduces the chances of them leaking or exposing enterprise data. Combining robust data destruction with NAC and DLP technologies will greatly improve the overall security of endpoints and the data they store or process.

Michael Cobb, CISSP-ISSAP, is a renowned security author with over 20 years of experience in the IT industry. He co-authored the book IIS Security and has written numerous technical articles for leading IT publications. He has also been a Microsoft Certified Database Manager and registered consultant with the CESG Listed Advisor Scheme (CLAS). Cobb has a passion for making IT security best practices easier to understand and achievable. His website www.hairyitdog.com offers free security posters to raise employee awareness of the importance of safeguarding company and client data, and of following good practices.

Home

Supplementary defenses for endpoint security

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.