

CUTTING-EDGE DEFENSE TACTICS FOR NETWORK ENDPOINTS

**EXPLOSION OF CONNECTED DEVICES REQUIRES
RE-THINKING OF SECURITY PROTECTION MECHANISMS**



DEFINING THE NETWORK ENDPOINT

Data has historically been contained to the computing devices that accessed it within the enterprise campus perimeter. The traditional network endpoint was isolated to desktop PCs, laptop computers and most server components that attached to the organization's network. In recent years, a dramatic increase in mobile devices has broadened the endpoint definition. Mobile devices require access to a company's data anytime and from anywhere. With the addition of always-connected, sensor-powered Internet of Things (IoT) devices, the range of endpoints can now include everything from IP cameras to smart vending machines to biomedical devices.

The original definition still holds true to this day; however, the presence of more sophisticated devices requesting an IP address from the network, and often without a user interface, also suggests that the approach to endpoint defense must change. Bi-directional communications means the endpoint can be an entry point into a network or application. What does the device need to communicate with? Does it require internet connectivity? Does a device with an embedded OS provide some form of protection? All endpoint devices are not created equally. "The operating and security characteristics of traditional desktop devices, mobile devices, servers, and the many classes of IoT devices vary significantly, as do the threat

vectors used to attack them, leaving CISOs with an increasingly complex attack surface to defend," says Dave Gruber, Senior Analyst for industry research firm ESG.

Considering the OSI Model, the Media layers handle packets, frames and symbols (bits). On the other hand, the Host layers work in data. An endpoint can be any point that is responsible for processing Host layer data. If an attack is due to "man in the middle" or packet interception or injection, then it is not likely an attack on an endpoint.

With the advent and growth of IoT, devices are ever-increasing the layers of the OSI model that a device processes. This means that the security team is comparably ever-increasing its endpoints. This is because there is, "no longer a brightline determination on what the ingress and egress points are in an enclave," says Jamal Hartenstein, IT Security Program Manager, KAI Partners. "Defining an enclave has become more vague and ambiguous for enterprises. Endpoints are now found outside of the traditional enclave."

"The explosion of connected devices also requires re-thinking the protection mechanisms to apply to those endpoints," notes Kayne McGladrey, Director of Security and IT, Pensar Development. "Similarly, the widespread adoption of cloud-based services means that there's no single network to protect."

OSI MODEL

Layer			Protocol data unit (PDU)	Function
Host layers	7	Application	Data	High-level APIs, including resource sharing, remote file access
	6	Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption
	5	Session		Managing communication sessions, i.e. continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes
	4	Transport	Segment, Datagram	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing
Media layers	3	Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control
	2	Data link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer
	1	Physical	Symbol	Transmission and reception of raw bit streams over a physical medium

Source: Wikipedia

ENTERPRISE CONCERN OVER ENDPOINT DEFENSE

Millions – and potentially billions – of new endpoints seem like an insurmountable task for security teams to manage. However, our experts tempered that perception of endpoint chaos down to a manageable going concern. “Endpoint solutions are part of the defensive toolbox,” says Bob Turner, CISO, University of Wisconsin-Madison. “They are a steady component that are increasingly part of the defensive fabric that integrate and share cyber intelligence with other advanced threat protections like our SIEM and next-generation firewalls.”

Some of the observed risks to organizations from the growing in endpoints include:

- Allowing smartphones from the mobile workforce on the network without registering them as corporate devices
- Tardy security patches
- Third-party access

“Endpoint solutions are part of the defensive toolbox.”

— BOB TURNER, CISO, UNIVERSITY OF WISCONSIN-MADISON



“As attacks on endpoints increase and attacks mature, the defense tactics must match or exceed that,” says Dennis Leber, CISO, Cabinet for Health and Family Services (CHFS) in the Office of Administrative & Technology Services (OATS) for the Commonwealth of Kentucky.

According to the SANS Institute¹, 42% of IT professionals had recently suffered a breach on their endpoints, and only 63% of organizations that were using next-gen endpoint security solutions had deployed the full capabilities of those solutions. “Organizations need to use any reputable risk methodology to prioritize the risks to their endpoints and to develop mitigation strategies,” says Pensar Development’s McGladrey.

ENDPOINT DEFENSE: TOOLS AND ECOSYSTEM

As established endpoint security vendors branch out, leveraging their common threat analytics platforms to secure new classes of endpoints, there are new device-specific and industry-specific solution providers delivering optimized security solutions for server, mobile/enterprise mobile applications and IoT endpoints. “These specialized security solution providers often have a deeper understanding of the specific threats associated with individual device use cases, and can therefore provide more robust, specialized security solutions,” says ESG analyst Gruber.

Common across most device types are the need for detection, investigation and response, however remedia-

tion strategies often differ. While it is okay to quarantine a desktop device, “taking a business-critical server or an IoT device out of service can significantly impact business operations,” adds ESG’s Gruber.

Sufficient market maturity exists to adopt software tools to assist in endpoint defense. Some organizations have issued RFPs to attract vendors with a vision and roadmap to achieve Unified Endpoint Management (UEM). “We had a large number of responses that included the traditional endpoint providers as well as

¹ <https://www.sans.org/reading-room/whitepapers/analyst/endpoint-protection-response-survey-38460>



new tools and approaches,” says higher-education CISO Bob Turner.

The vendor and supplier ecosystem for endpoint defense is expanding, which is viewed as a benefit for organizations that seek a variety of approaches and functions. However, the ecosystem growth also increases the complexity of tool selection for the organization. Nearly every endpoint security vendor is selling a “single pane of glass”, which was noted by both security leaders Michael Welch, CISO, OSI Group and Pensar Development’s Kayne McGladrey, unfortunately doesn’t integrate with the “single pane of glass” for cloud security, for insider threat detection, or any other system. The noise associated with multiple systems make it very hard for defenders to effectively triage and respond to threats.

For some industry verticals, managing the endpoint security controls can be delegated to the desktop teams. However, this functionality must go hand-in-hand with more advanced Incident Response capability. “We must have the capability to quickly identify potential threats, quickly build that threat intelligence package and respond through our security controls and processes, to eliminate the threat and go through an after-action report,” says Randall Frieztzsche, CISO & Privacy Officer, Denver Health.

Software automation and tools that require less human interaction are a growing security trend. Similarly, organi-

zations desire tools that integrate into a broader security solution, such as the need for a potential software tool to be able to communicate with the enterprise SIEM tool and ticketing system. “It is desirable to have the capacity to have a dashboard and SIEM tool that can automate not only notifications to humans, but can automatically open a trouble-ticket and assign it to the appropriate department or technician, says IT Security Program Manager Hartenstein. “The market is ready with tools and compatibility, but not every enterprise has a mature enough security posture to adopt such automation.”

While most CISOs crave consolidation and simplification, “it will be some time before larger endpoint security vendors will be able to incorporate these best-of-breed solutions into broad platform or suite offerings,” says ESG research analyst Dave Gruber. Until then, CISOs should look to work with specialized solution providers, especially in emerging areas like IoT, where security challenges are sufficiently different enough that new approaches are required.



ENDPOINT DEFENSE: PEOPLE

The tools for endpoint defense are improving and integrate more and more with other management tools and processes for the organization's security program. Initially requiring additional staff, increased levels of automation will alleviate any people-intensive tasks as the tools go online. "The greatest benefit is the visibility our first responders are given," says CISO Bob Turner.

The role of security personnel in endpoint defense depends on the type of function the endpoint software is performing and the size of the team that a company employs. "If teams are lean, it usually requires additional staff to manage and support," says OSI Group CISO Welch. "Many of the endpoint products are providing a managed service, which works well for companies that don't have the staff to support."

Large enterprises, such as healthcare providers, financial institutions or education systems, rely on dedicated human support staff to manage endpoint defense in addition to a Defense in Depth (DiD) solution to manage risk with diverse defensive strategies and a level of redundancy around the clock. In contrast, smaller enterprises (depending on their compliance and risk exposure) rely on automated products to protect endpoints, which initiate alerts and workflows for incidents that require a response.

Overall, business awareness is growing. Organizations understand that a simple click on a link or browsing a website negates endpoint protection. For CISO Dennis Leber, "mixing behavioral analytics, real-time monitoring and protecting is the growing approach to address this."

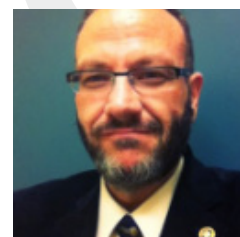
ENDPOINT DEFENSE TACTICS

Science fiction writer Gene Wolfe wrote in *The Urth of the New Sun*, “The best offense is a good defense, but a bad defense is offensive.” Avoid offending executives and end-users alike by developing endpoint defense tactics. We asked our security leaders to give us three insights that every organization should consider in an effective endpoint defense. Since industries vary in compliance obligations and individual businesses have unique requirements, we received almost no overlap in responses from our subject-matter experts. Here are 18 endpoint defense tactics for you to consider.



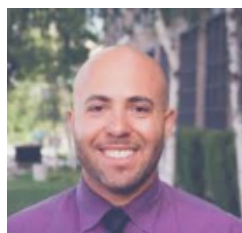
BOB TURNER
CISO, UNIVERSITY OF WISCONSIN-MADISON:

- Know who is accessing the data through robust identity and access management
- Know what data belongs on or can be accessed through the endpoint
- Use tools that report indications of compromise to a central console or reporting point



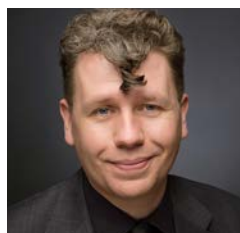
RANDALL FRIETZSCHE
CISO & PRIVACY OFFICER, DENVER HEALTH:

- Utilize malware detection but don't rely 100% on those signature-based detection methods
- Use an additional threat detection/response tool to ensure that any malware or suspicious activity is both detected and alerted
- Find the right response mechanism – either 24/7/365 staffing or MSSP to make sure these detections are addressed with priority



JAMAL HARTENSTEIN
IT SECURITY PROGRAM MANAGER, KAI PARTNERS:

- Make authenticating to the endpoint more difficult with multi-factor authentication (MFA)
- Protect the endpoint with an anti-virus solution product
- Control your Image: This includes OS hardening, continuous patch management, and Mobile Device Management (MDM) solution. This usually only occurs when enterprises limit their permutations of endpoint images.



KAYNE MCGLADREY
DIRECTOR OF SECURITY AND IT, PENSAR DEVELOPMENT:

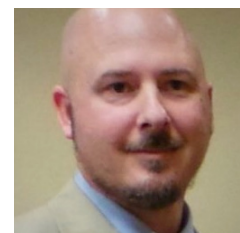
- Have an inventory of every endpoint; aspire for both an active and a passive IT asset management system
- Patch all the endpoints that support patching. Get rid of devices that cannot be patched.
- Segment network endpoints by the sensitivity of the data collected, processed, and/or stored making it incrementally harder for a threat actor to move laterally into a different type of device



MICHAEL WELCH
CISO, OSI GROUP:
The core areas of defense of network endpoints are:

- Vulnerability Management (OS and Applications)
- Malware protection
- Data-Loss Prevention

All of them should have detection and response capabilities and privilege management



DENNIS LEBER
CISO, CABINET FOR HEALTH AND FAMILY SERVICES (CHFS) IN THE OFFICE OF ADMINISTRATIVE & TECHNOLOGY SERVICES (OATS) FOR THE COMMONWEALTH OF KENTUCKY:

- Continuous detection and mitigation (CDM)
- Approach beyond technology
- Address people

ENTERPRISE ALLIES FOR ENDPOINT DEFENSE

To achieve adoption of endpoint defense across the organization, start with a tops-down approach. Begin by identifying executives responsible for owning risk. "Without engaged leaders, the cost and complexity required will not be supported to the technologist level," says CISO Bob Turner. "Get them on board and the rest are straightforward."

IT leadership and executive leadership focused on IT are also very important, says Denver Health CISO & Privacy Officer Frietzsche, "to understand the threats, the current controls, and the next vision of controls, people, processes and technology to defend against realistic threats." DevSecOps is becoming a bigger stakeholder than before regarding effective endpoint defense.

IT managers and front line technical staff are also invested in managing the additional work that comes from increased visibility. Developers and architects

"We can never have all the controls needed to stop 100% of attacks."

— RANDALL FRIETZSCHE, CISO & PRIVACY OFFICER, DENVER HEALTH

must engage in more than just fielding systems that have utility and effectiveness built in. They need security as a primary feature. And, finally, the user who operates the endpoint in a secure manner rounds out the stakeholder team that are invested in securing the data.

All stakeholders should be an ally for endpoint defenses, says CISO Welch. "It is our job as security professionals to educate the stakeholders on the risks presented to the business and the tools that are used to reduce those risks."

SECURITY AWARENESS TRAINING

Awareness is an important component in any cyber defense strategy and security control. More aware users tend to engage early and give helpful suggestions for utility and important operating features in endpoint defense.

"We can never have all the controls needed to stop 100% of attacks," says Denver Health's Frietzsche. "We must train our users in the use of email and websites, to ensure they understand what a threat looks like, and when to exercise caution." Many of the cyber-attacks launched against organizations require human interaction, such as clicking a link or opening an attachment.

Users should not only be aware of security risks but the security team at organizations should persistently engage with their end-user community via simulated phishing attacks. "People ignore the mandatory one-hour cybersecurity drop-ceiling training in the break room, but they don't forget the first time they get phished," says Security and IT Director Kayne McGladrey. Remember that the goal here is not to demonstrate how smart the security team is. Rather, the desired outcome is to sensitively inform and educate users on how to avoid attacks on their endpoints.



ENDPOINT DEFENSE STRATEGY ASSESSMENT

The changing threat landscape and the sophistication of cyber-attacks necessitates that organizations should assess endpoint defense strategies on a regular basis. Our experts converged on an annual review as an adequate timeframe to learn from any events or assessments and identify potential gaps. There will be variations on the frequency based on the size and objectives of the organization. CISO Dennis Leber suggests that an ongoing assessment as part of a continuous monitoring program reduces the risk

of a strategy assessment falling out of cycle with the needs of the organization. “Large, centrally-managed organizations need to resist the urge to change frequently,” adds university CISO Bob Turner.

The leadership of an organization should also consider derivative liability in a data breach lawsuit, says security legal expert Jamal Hartenstein. Derivative liability is based on a two-factor test. “They must make (1) regularly informed decisions and (2) act in good faith,” Hartenstein says it may be easier for courts to attack the frequency and regularity of reporting and communication with the decision-makers, which is an activity entirely under the control of the organization.

As part of your overall strategy, organizations “must know what is important to your brand and how to prioritize the goals based on the biggest risk to that brand; addressing your risks today but also risks that may be presented in the future,” remarks CISO Michael Welch. The endpoint defense tools that are deployed should scale to match your environment.



ABOUT CYBER SECURITY HUB

The Cyber Security Hub is an online news source for global cyber security professionals and business leaders who leverage technology and services to secure the entire perimeter in their enterprise.

We're dedicated to providing the latest industry news, thought leadership and analysis in the cyber security space. Cyber Security Hub's expert commentary, tools and resources are developed through obtaining data and interviewing end users and analysts throughout the industry to deliver practical and strategic advice.

Our editorial team surveys and monitors the latest trends in cyber security and creates news articles, market reports, case studies and in-depth analysis for a captive audience consisting of C-Level executives, VPs and directors of cyber security and information technology.

CYBER SECURITY HUB

Dorene Rettas

Managing Director,
Cyber Security Hub
Dorene.Rettas@CSHub.com

Jeff Orr

Editor,
Cyber Security Hub
Jeff.Orr@CSHub.com

Patrick Gallagher

Marketing Manager,
Cyber Security Hub
Patrick.Gallagher@iqpc.co.uk

Rosecley Morishita

Editorial Director,
Cyber Security Hub
Rosecley.Morishita@iqpc.com

Michael Roberts

Sales Director,
Cyber Security Hub
Mike.Roberts@CSHub.com



UPCOMING MARKET REPORTS

OCTOBER: A Centralized Point Of View: SIEM For Better Efficiency And Compliance

NOVEMBER: Fiscal Trajectory: Cyber-Spend Allocation For 2020

DECEMBER: Cautionary Tales of 2019 Enterprise Cyber Security Breaches

SOCIAL MEDIA INFORMATION:



TWITTER: CSHubUSA



FACEBOOK: CSHubIQPC



LINKEDIN: Cyber Security Hub - Enterprise Security Professionals