TO E5 and Beyond!

Making the most of E5 licenses with Microsoft and the various Defender 365, Purview, and Office 365 Protections that come with it.

Kyle Goode
Acadia Healthcare

Defender For Endpoint

Native Windows Application for Endpoints and Servers

Full Windows, MacOS, and Linux Support

EDR - ✓

NDR - ✗

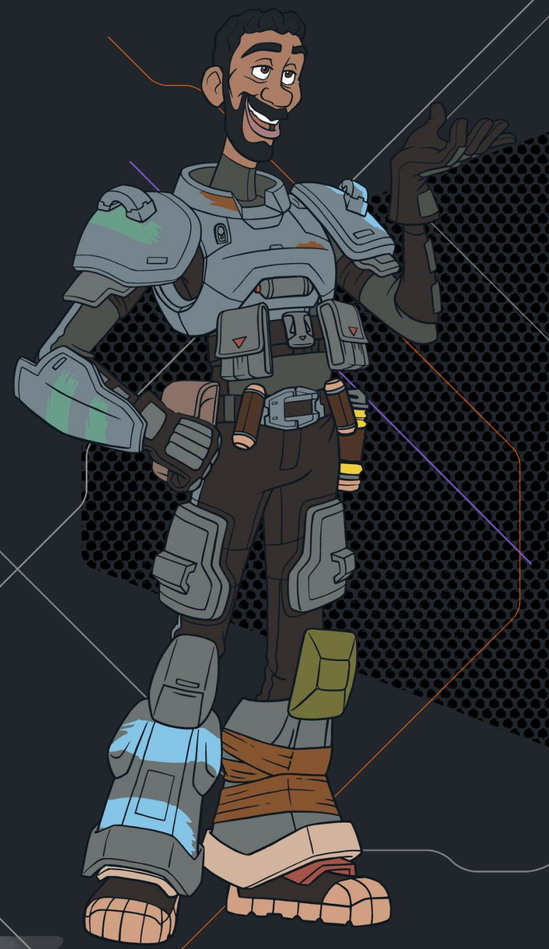
IDR - ✓

XDR - ✓

Defender for Servers

Native Support for Windows Servers 2012 and Up

Linux support for RHEL, Ubuntu, SLES, Debian, and Oracle



Defender for 365

Outlook/Exchange

Teams

Sharepoint

Word, Excel, Powerpoint, etc 365 apps

Safe Attachments, Documents, and Links

Zero-hour auto purge(ZAP)

Priority account protection

Intune Endpoint Security Protections

Advanced Antivirus Settings

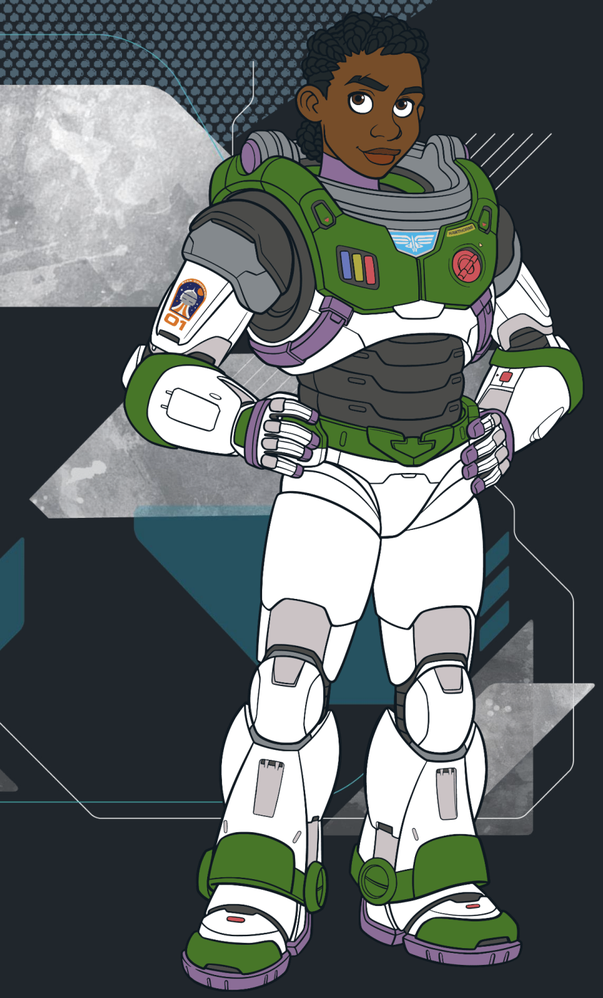
Tamper Protection

Disk Encryption

Host Based Firewall

Attack Surface Reduction Rules

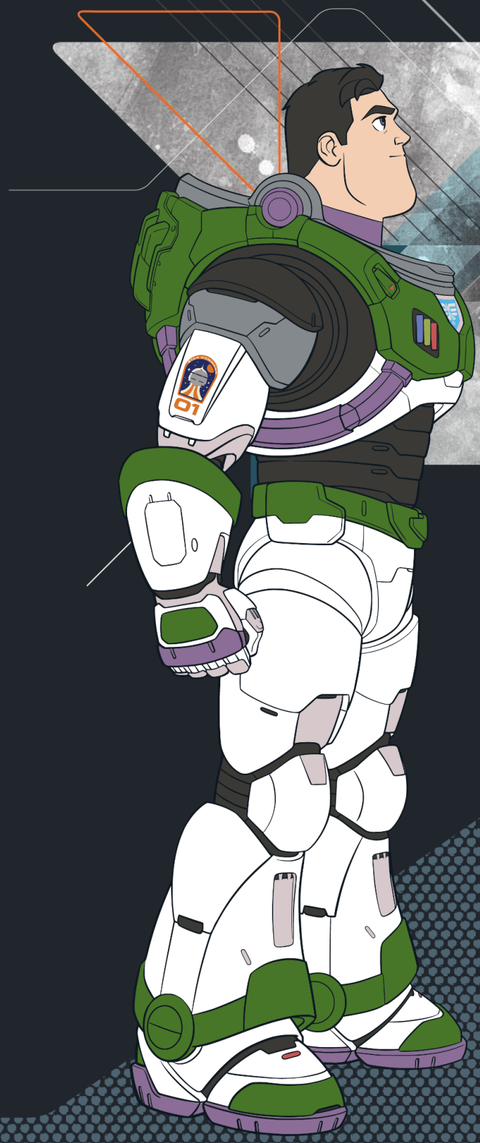
Defender for Identity



User and Entity Behavior Analytics

Identifies and ranks risky users, sign-ins, and insider threats

Risk Scored Authentication + Conditional Access = IDR automation



Conditonal Access

Session Limits

Geofencing

MFA Policies

Risk Based MFA Prompts

Blocking Legacy Authentication

Risk Based Password Reset

Purple Knight

Insider Threat

Vulnerability Management

Firmware

Cloud Apps

Software

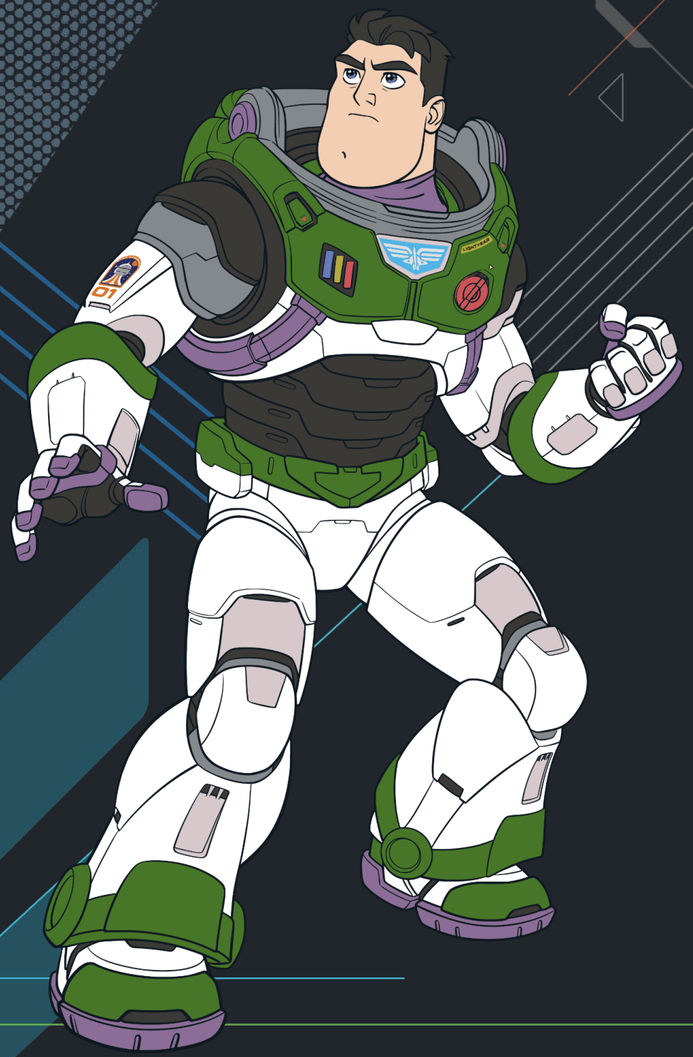
Shadow IT

OS Patches

Browser Extensions

IoT Devices

Certificates



Purview

eDiscovery

Trainable Classifiers(HIPAA and SOX are pre-canned classifiers)

Sensitivity labels

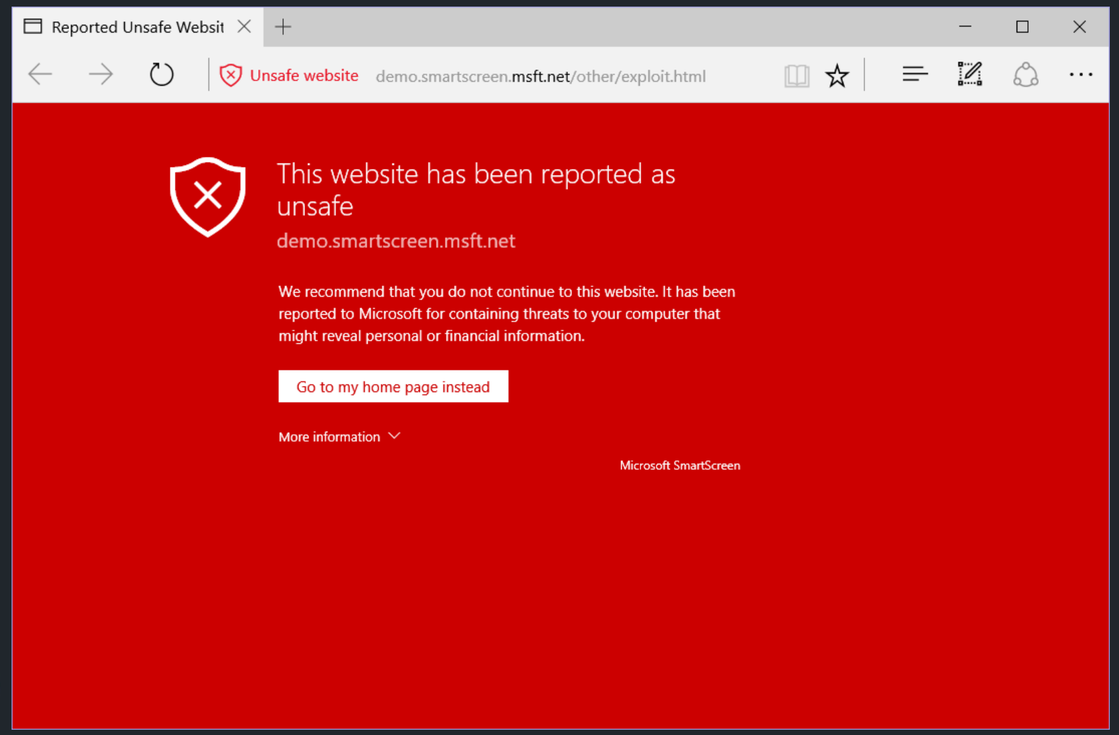
Data Loss Prevention

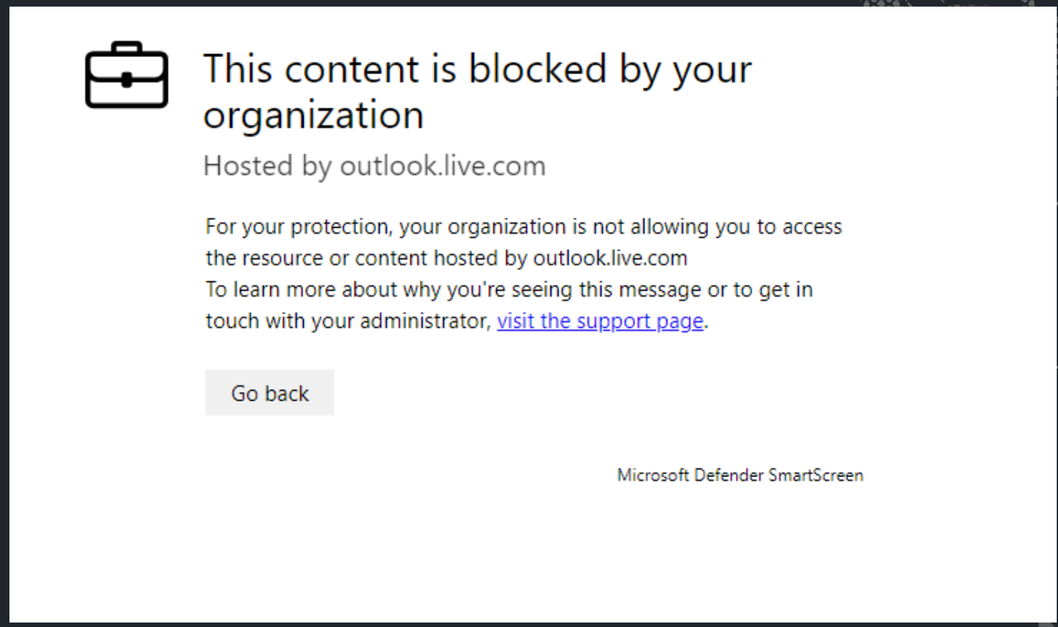
Web Content Filtering

Adult content	- **Cults:** Sites related to groups or movements whose members demonstrate passion for a belief system that is different from those that are socially accepted. - **Gambling:** Online gambling and sites that promote gambling skills and practice. - **Nudity:** Sites that provide full-frontal and semi-nude images or videos, typically in artistic form, and might allow the download or sale of such materials. - **Pornography / Sexually explicit:** Sites containing sexually explicit content in an image-based or textual form. Any form of sexually oriented material is also listed here. - **Sex education:** Sites that discuss sex and sexuality in an informative and nonvoyeuristic way, including sites that provide education about human reproduction and contraception, sites that offer advice on preventing infection from sexual diseases, and sites that offer advice on sexual health matters. - **Tasteless:** Sites oriented towards content unsuitable for school children to view or that an employer would be uncomfortable with their staff accessing, but not necessarily violent or pornographic. - **Violence:** Sites that display or promote content related to violence against humans or animals.
High bandwidth	- **Download sites:** Sites whose primary function is to allow users to download media content or programs, such as computer programs. - **Image sharing:** Sites that are used primarily for searching or sharing photos, including those that have social aspects. - **Peer-to-peer:** Sites that host peer-to-peer (P2P) software or facilitate the sharing of files using P2P software. - **Streaming media & downloads:** Sites whose primary function is the distribution of streaming media, or sites that allow users to search, watch, or listen to streaming media.

Legal liability	- **Child abuse images:** Sites that include child abuse images or pornography. - **Criminal activity:** Sites that give instruction on, advice about, or promotion of illegal activities. - **Hacking:** Sites that provide resources for illegal or questionable use of computer software or hardware, including sites that distribute copyrighted material that has been cracked. - **Hate & intolerance:** Sites promoting aggressive, degrading, or abusive opinions about any section of the population that could be identified by race, religion, gender, age, nationality, physical disability, economic situation, sexual orientations or any other lifestyle choice. - **Illegal drug:** Sites that sell illegal/controlled substances, promote substance abuse, or sell related paraphernalia. - **Illegal software:** Sites that contain or promote the use of malware, spyware, botnets, phishing scams, or piracy & copyright theft. - **School cheating:** Sites related to plagiarism or school cheating. - **Self-harm:** Sites that promote self-harm, including cyberbullying sites that contain abusive and/or threatening messages towards users. - **Weapons:** Any site that sells weapons or advocates the use of weapons, including but not limited to guns, knives, and ammunition.
Leisure	- **Chat:** Sites that are primarily web-based chat rooms. - **Games:** Sites relating to video or computer games, including sites that promote gaming through hosting online services or information related to gaming. - **Instant messaging:** Sites that can be used to download instant messaging software or client based instant messaging. - **Professional network:** Sites that provide professional networking services. - **Social networking:** Sites that provide social networking services. - **Web-based email:** Sites offering web-based mail services.
Uncategorized	- **Newly registered domains:** Sites that are newly registered in the past 30 days and haven't yet been moved to another category. - **Parked domains:** Sites that have no content or are parked for later use.

Smartscreen

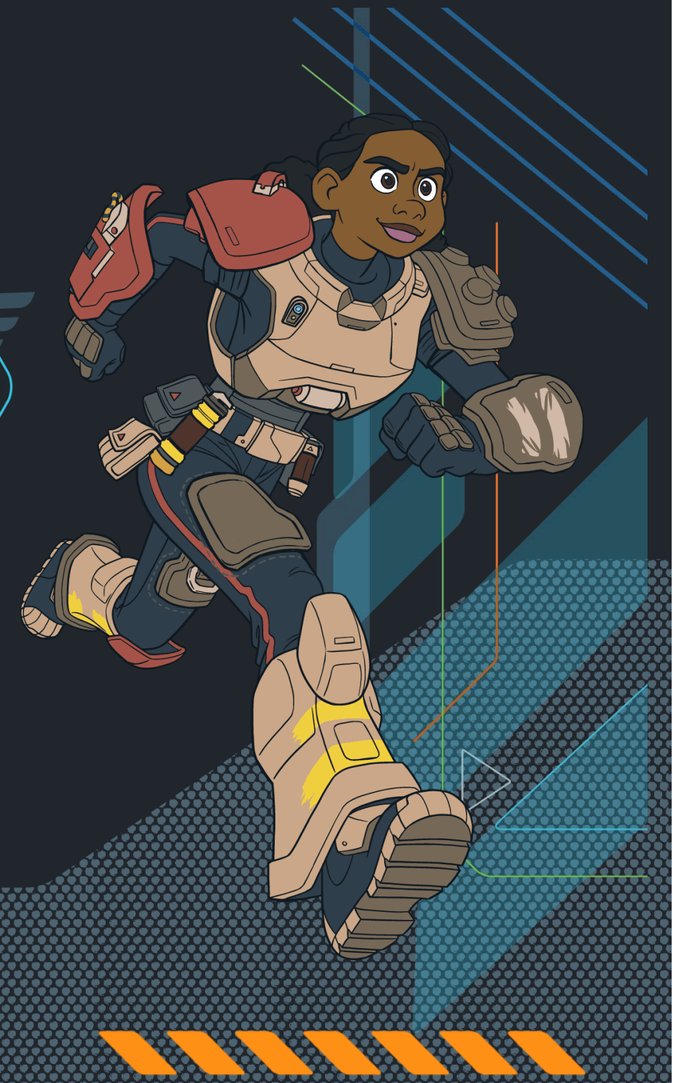


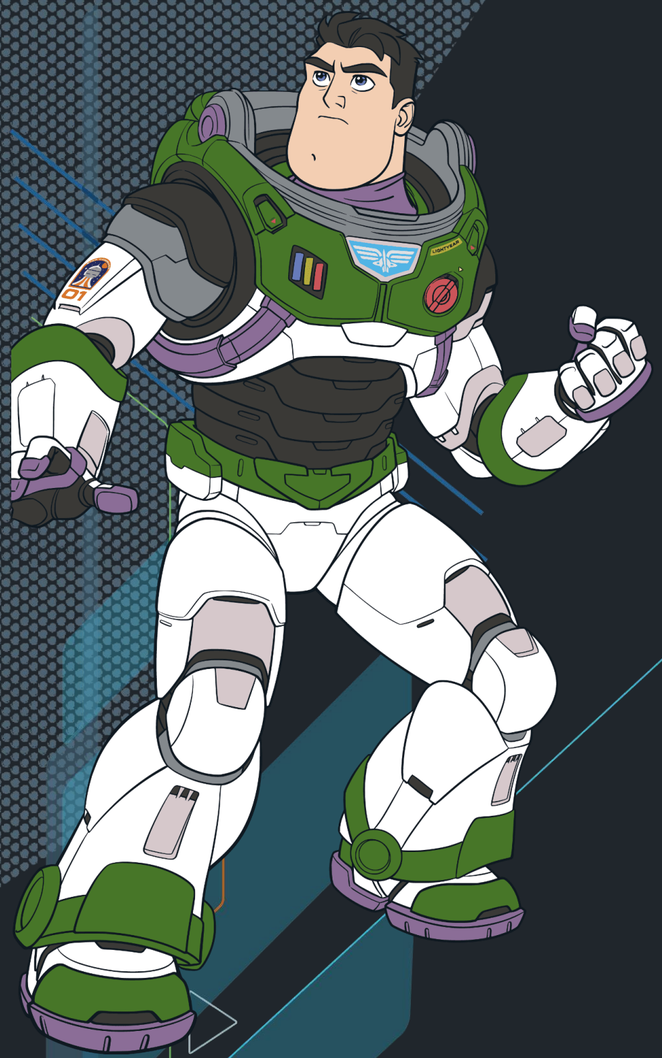


Defender for Cloud Apps

Cloud Application Security Broker

Cloud Application Security Broker





Advanced Hunting With Kusto Queries

CISA Know Exploited vulnerabilities

Metasploit

MFA manipulation

Feodo Tracker

Reports and Metrics

Web Protections

Device control

Attack surface reduction rules

Firewall

Power BI

Email

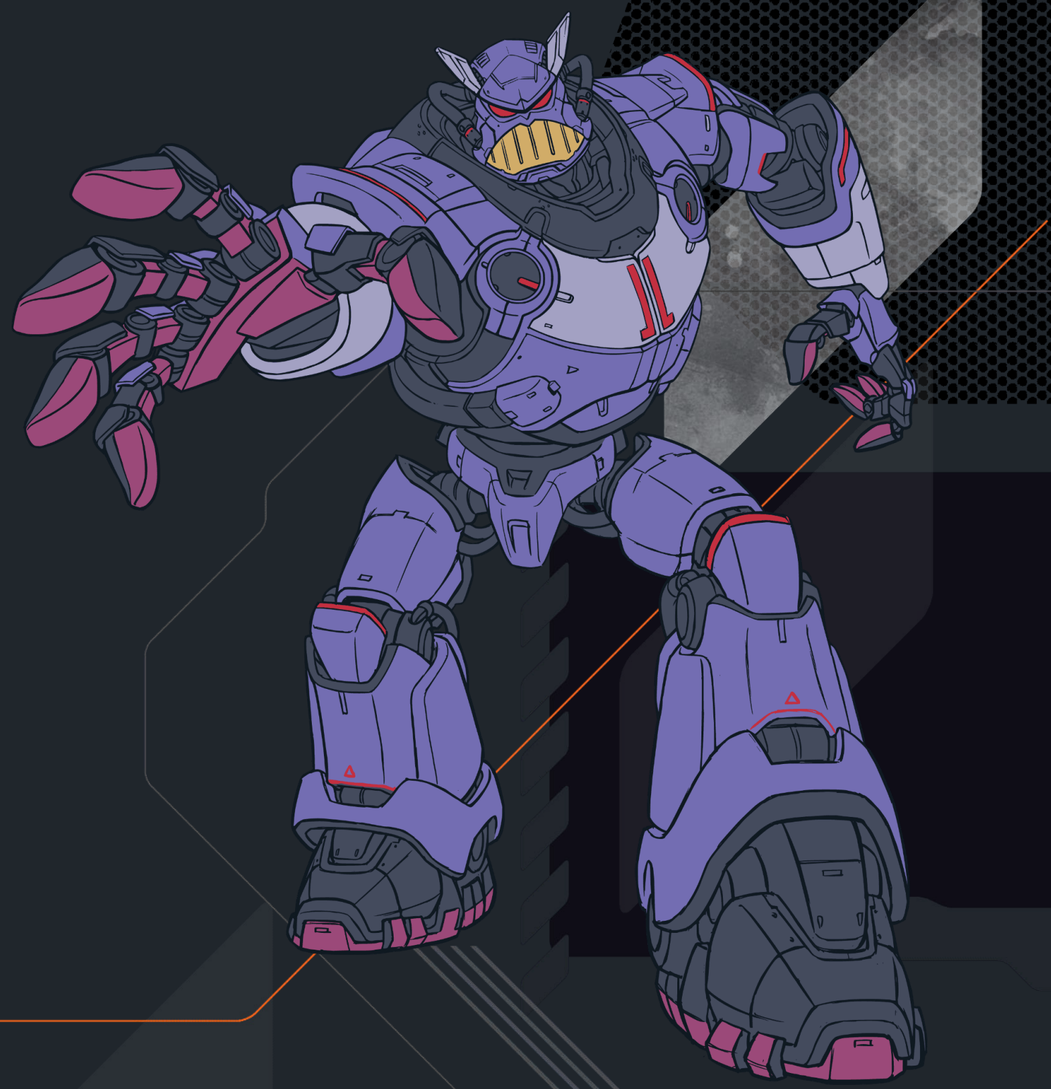
Firewall

Endpoint Vulnerabilities

Automatic Attack Disruption

Contain User

Intel Threat Detection Technology



Limitations

30 day limits on all logs

Sentinel has free…alerts

“Microsoft Time”

Device groups not by Identity AD or Entra ID groups

XDR without the NDR

Alert Tuning is painful

Support Limitations

Tips

Disable End User Notifications

Audit well first then block

Create Custom Detections

Bing is your friend

Manage IOCS

THANKS!

Questions?

Kyle Goode
Acadia Healthcare