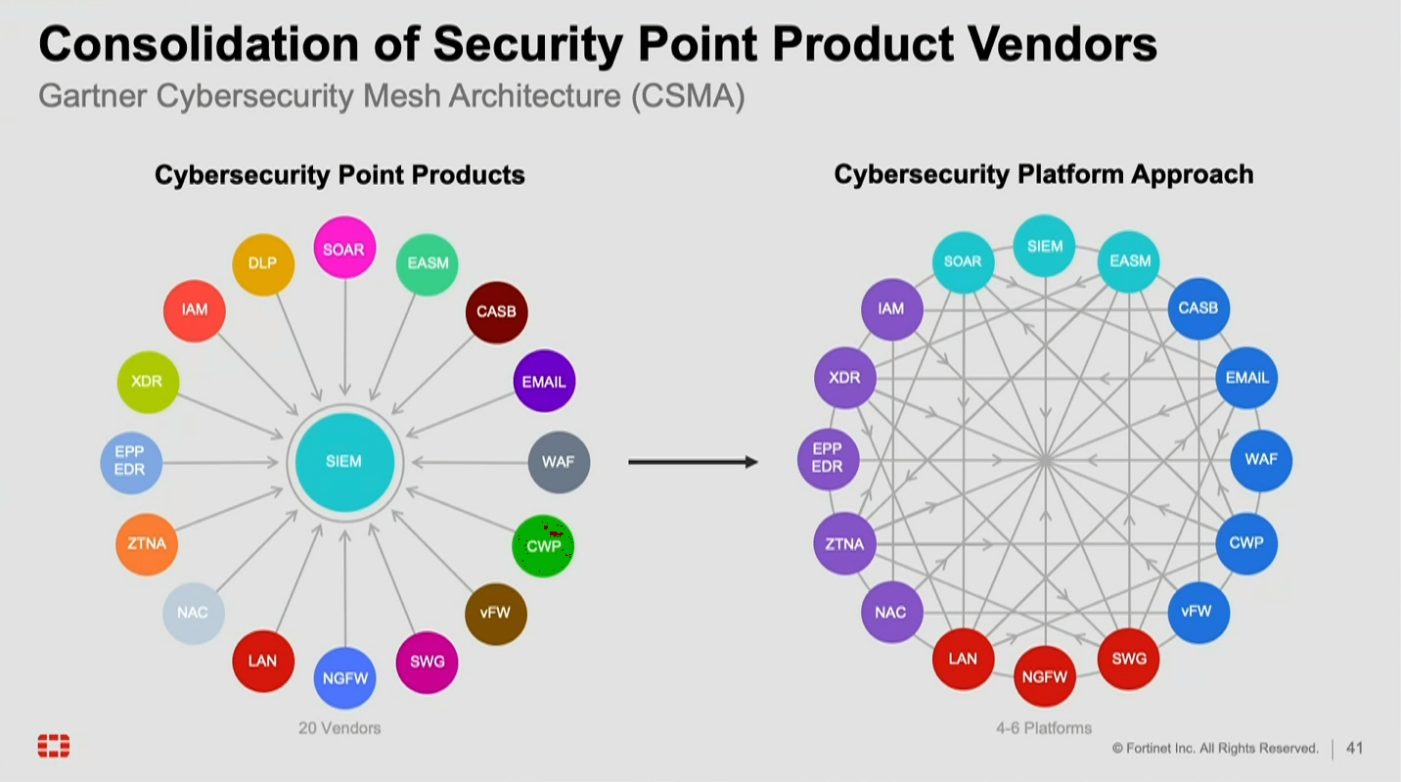
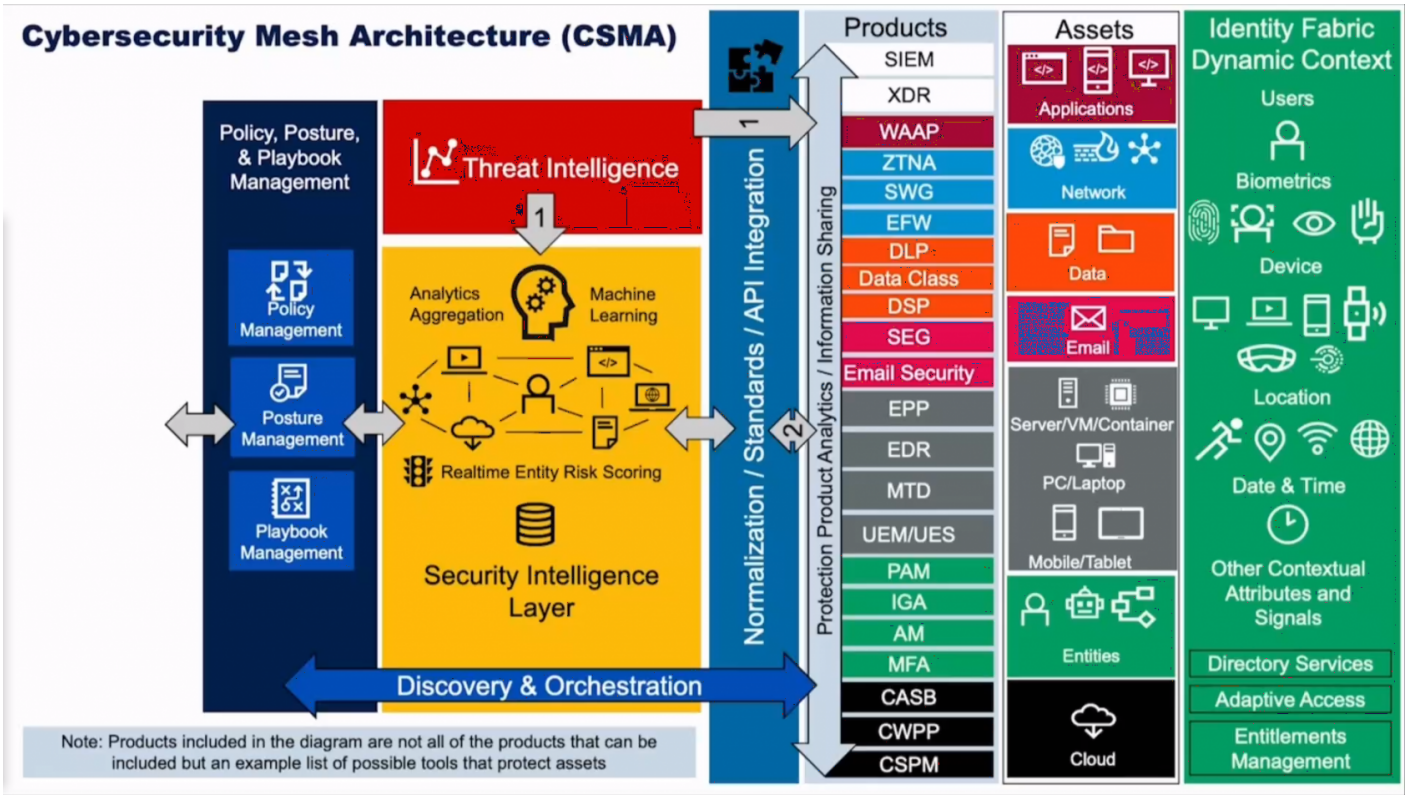
Cybersecurity Strategy

Security Topics and Theories.

- Cybersecurity Mesh Architecture
- NTLM Brute Force

Cybersecurity Mesh Architecture




Cybersecurity Mesh Architecture (CSMA)
Policy, Posture, & Playbook Management
Policy Management
Posture Management
Playbook Management
Threat Intelligence
1
Analytics Aggregation
Machine Learning
Realtime Entity Risk Scoring
Security Intelligence Layer
Discovery & Orchestration
Normalization / Standards / API Integration
1
2
Protection Product Analytics / Information Sharing
Products
SIEM
XDR
WAAP
ZTNA
SWG
EFW
DLP
Data Class
DSP
SEG
Email Security
EPP
EDR
MTD
UEM/UES
PAM
IGA
AM
MFA
CASB
CWPP
CSPM
Assets
Applications
Network
Data
Email
Server/VM/Container
PC/Laptop
Mobile/Tablet
Entities
Cloud
Identity Fabric Dynamic Context
Users
Biometrics
Device
Location
Date & Time
Other Contextual Attributes and Signals
Directory Services
Adaptive Access
Entitlements Management
Note: Products included in the diagram are not all of the products that can be included but an example list of possible tools that protect assets

NTLM Brute Force

https://www.varonis.com/blog/investigate-ntlm-brute-force

> More specifically, you will need to use Event ID 8004 in Event Viewer to identify the actual device that is on the receiving end of these NTLM brute force attack attempts. Locating the victim device will be the first step in the remediation process.

> 8004 events are typically not enabled by default and may require configuration changes in specific Domain Controller group policies to enable logging.